Uwierzytelnianie wieloskładnikowe MFA

1 Zarządzanie uwierzytelnianiem wieloskładnikowym

W celu lepszego zabezpieczenia procesu logowania, Portal SZOI i Portal SNRL 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 Portalu SZOI 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.

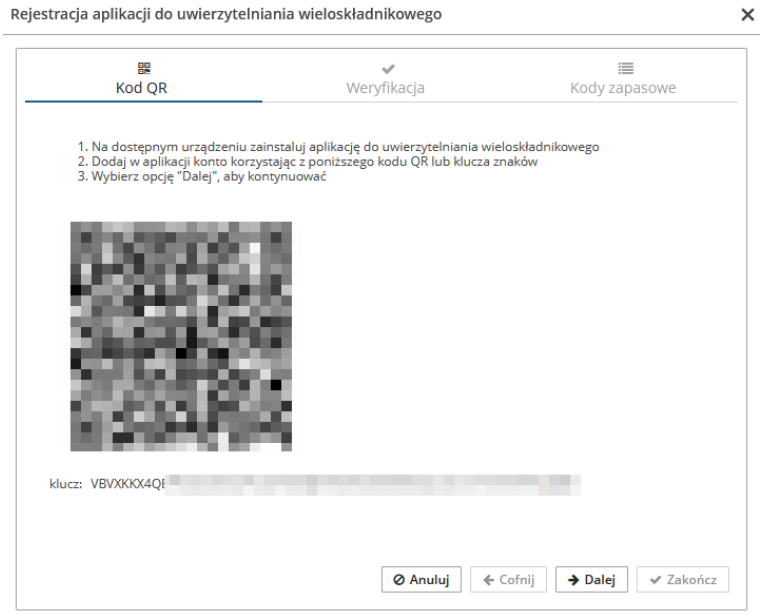
Aby móc skorzystać z powyższego mechanizmu konieczne jest posiadanie aplikacji, która obsługuje otwarty standard TOTP. Liczba aplikacji generujących tokeny TOTP jest bardzo duża i są to zarówno produkty darmowe jak i komercyjne. Poniżej kilka przykładów:

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

2 Rejestracja aplikacji

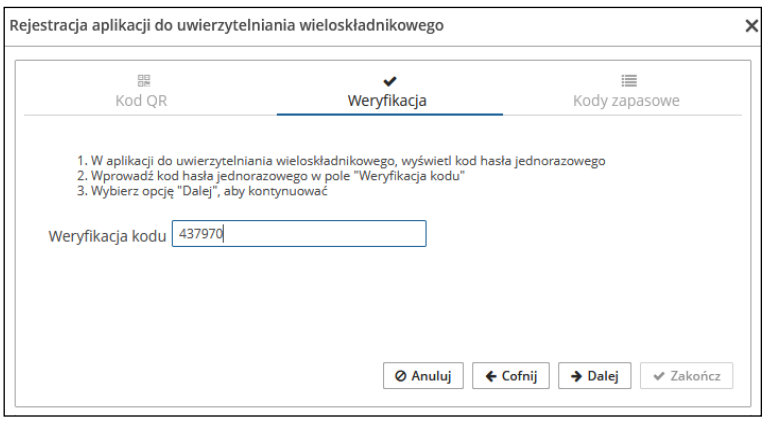
Rozpoczęcie korzystania z mechanizmu MFA wymaga jednorazowego wykonania czynności powiązania konta w portalu z aplikacją do uwierzytelniania.
Pierwszym krokiem włączenia logowania MFA jest rejestracja aplikacji, która będzie wykorzystywana do uwierzytelniania wieloskładnikowego na dostępnym urządzeniu. **Musisz pamiętać, że aplikacja (urządzenie) będzie wykorzystywane w przyszłości przy każdym logowaniu się operatora do systemu**.

Aby powiązać aplikację z kontem dostępowym wybierz z głównego menu *System -> Uwierzytelnianie wieloskładnikowe,* a następnie opcję + Rejestracja aplikacji. Wykorzystując wyświetlony na ekranie kod QR lub klucz znaków dodaj nowe konto w aplikacji.



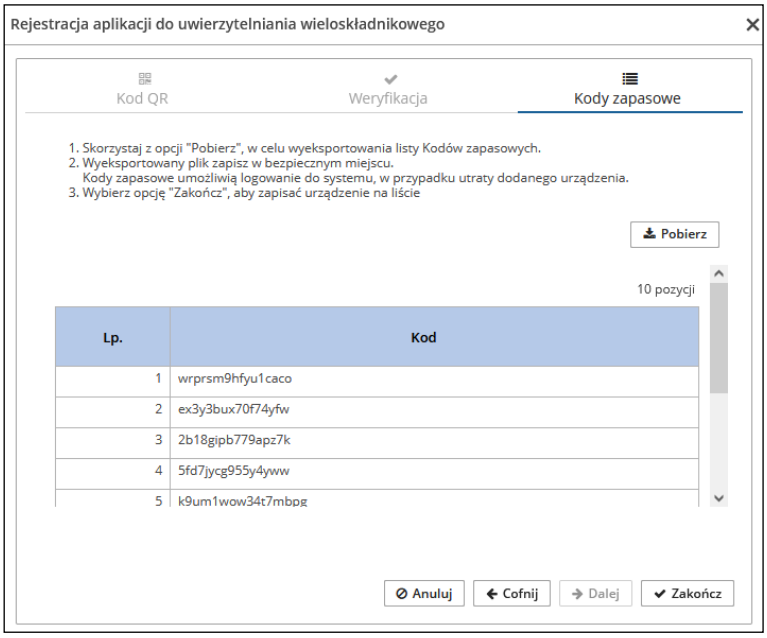
Rys. 1 Rejestracja aplikacji do uwierzytelniania wieloskładnikowego

Po zarejestrowaniu wybierz opcję → Dalej. W kolejnym oknie musisz uzupełnić kod hasła jednorazowego (jego ważność to 30 sekund), który wygenerujesz w aplikacji do uwierzytelniania wieloskładnikowego. Po uzupełnieniu kodu wybierz opcję → Dalej, aby kontynuować.



Rys. 2 Rejestracja aplikacji do uwierzytelniania wieloskładnikowego - weryfikacja

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



Rys. 3 Rejestracja aplikacji do uwierzytelniania wieloskładnikowego – kody zapasowe

Po wybraniu opcji ✔ Zakończ urządzenie zostanie dodane do listy. Od tego momentu podczas logowania do Portalu SZOI oprócz loginu oraz hasła będziesz musiał podać kod weryfikacyjny wygenerowany w zarejestrowanej aplikacji. **Pamiętaj, że jednocześnie konto może mieć zarejestrowaną tylko jedną aktywną aplikację.**

Jeżeli zaistnieje konieczność wyłączenia logowania MFA, musisz przejść do okna *Uwierzytelnianie wieloskładnikowe* i za pomoca opcji **Usuń** dostępnej w kolumnie *Obsługa* wyrejestrować aplikację uwierzytelniającą.

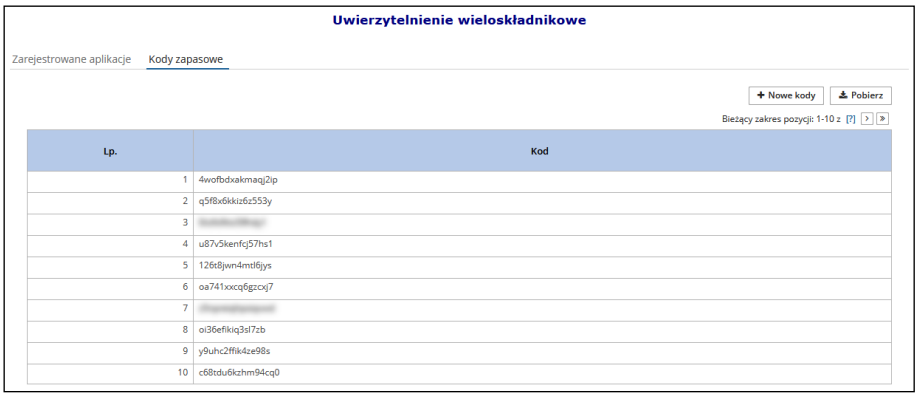
Rys. 4 Uwierzytelnianie wieloskładnikowe

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 oznaczone będą jako zamglone.

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



Rys. 5 Kody zapasowe do uwierzytelniania wieloskładnikowego

4 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 uzupełnij login oraz hasło.
2. Podaj kod weryfikujący wygenerowany w zewnętrznej aplikacji uwierzytelniającej.

Rys. 6 Logowanie do SZOI za pomocą kodu weryfikacyjnego

3. Jeżeli nie masz dostępu do aplikacji uwierzytelniającej, możesz skorzystać z kodu zapasowego zawartego w pliku TXT jaki pobrałeś podczas rejestracji aplikacji (opcja ***Zaloguj się za pomocą kodu zapasowego***).

Rys. 7 Logowanie do SZOI za pomocą kodu zapasowego