Instrukcja dla użytkowników SIMP i SMPT

- logowanie dwuskładnikowe

W celu podniesienia poziomu bezpieczeństwa systemów informatycznych stosuje się logowanie dwuskładnikowe MFA, czyli podwójną weryfikacje tożsamości użytkownika. Rozwiązanie to znacząco ogranicza nieautoryzowany dostęp do systemu przez osoby nieuprawnione.

Logowanie dwuskładnikowe wprowadza dodatkowy etap w logowaniu użytkownika do systemu. Oznacza to, że procedura logowania wygląda następująco:

 wprowadzenie nazwy użytkownika oraz hasła (jak dotychczas), a po pomyślnym przejściu tego etapu,

UWAGA: zostały zmienione wymagania dotyczace hasła:

- Długość 14 do 20 znaków system rozróżnia wielkie i małe litery
- W haśle musi występować co najmniej jedna litera "duża" (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
- W haśle musi występować co najmniej jedna litera "mała" (abcdefghijklmnopqrstuvwxyz)
- W haśle musi występować co najmniej jedna cyfra
- Hasło może zawierać znaki specjalne ze zbioru: !@-_#\$&*
- uwierzytelnianie za pomocą zewnętrznego mechanizmu, tj. wprowadzenie jednorazowego kodu wygenerowanego w aplikacji zewnętrznej, np. na telefonie lub tablecie.

W wyznaczonym przez NFZ terminie, tj. od 1 lipca 2025 r., ten sposób logowania (dwuskładnikowy) stanie się obowiązkowy.

Zgodnie z wytycznymi NFZ, od 1 lipca 2025 r. każdy użytkownik musi korzystać z tego mechanizmu logowania.

Aby zachować ciągłość pracy w systemie, niezbędne jest korzystanie z logowania dwuskładnikowego.

Jak włączyć logowanie dwuskładnikowe MFA:

Pierwszym krokiem włączenia logowania dwuskładnikowego 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.

Zatem wcześniej należy przygotować urządzenie mobilne – należy pobrać odpowiednią aplikację z **Google Play** dla androida na smarfony lub **App Store** dla iOS na iPhone.

Na urządzenie mobilne (smartfon lub tablet) są dostępne aplikacje typu Authenticator, np.:

• Google Authenticator

• Microsoft Authenticator

Wybraną aplikację należy pobrać i zainstalować.

W następnym kroku należy zalogować się systemu i przejść do menu **POMOC**, a następnie wybrać zakładkę **Moje dane** (niezależnie od modułu SIMP czy SMPT):



Na ekranie wyświetli się formularz, gdzie pojawi się opcja włączenia usługi:

Moje dane - edycja		М
		[©] 29 min. do zakończenia sesji
	E-mail	moje@mail.pl
	Pytanie kontrolne	IMIĘ PSA/ KOTA ~
	Odpowiedź	TAKUŚ
	Usługa uwierzytelnia Dokończ konfigura wygenerowany Ko Kod QR	inia dwuskładnikowego icję instalując aplikacje Google Authenticator lub Microsoft Authenticator i zeskanuj d QR, a następnie wciśnij Zapisz
	Potwierdź poprawną Nazwa urządzenia	konfigurację poprzez wprowadzenie kodu z aplikacji
		Zapisz Rezygnuj

Należy zaznaczyć checkbox w polu 'Włącz usługę uwierzytelniania dwuskładnikowego'.

Po zaznaczeniu odblokuje się przycisk 'Kod QR'.

Włącz usługę uwierzytelniania dwuskładnikowego	
Dokończ konfigurację instalując aplikacje Google Authenticator wyg enerowany K od QR, a następnie wciśnij Zapisz Kod QR	lub Microsoft Authenticator i zeskanuj

Przycisk pozwala wygenerować kod QR konieczny do powiązania urządzenia mobilnego z kontem w systemie (należy zeskanować swój kod QR).



Klucz: TEUDXKCJHIKLVXJKSHMKLXVJKJFS

Zamknij

Przykładowy kod QR

W zainstalowanej aplikacji należy skorzystać z wygenerowanego kodu QR i zeskanować go urządzeniem mobilnym z ekranu komputera, tzn. wybrać w aplikacji opcję 'Dodaj' (+), a potem 'Zeskanuj kod QR', np. na takim ekranie (ekran może się różnic w zależności od systemu i wybranej aplikacji):



System CSM (SIMP/SMPT/RLC/ADMIN) będzie oczekiwał potwierdzenia rejestracji urządzenia:

Moje dane - edycja		M
		O 27 min. do zakończenia sesji
	E-mail	moje@mail.pl
	Pytanie kontrolne	IMIĘ PSA/ KOTA v
	Odpowiedź	TAKUŚ
	Usługa uwierzytelnia Dokończ konfigur wygenerowany Ko Kod QR	ania dwuskładnikowego ację instalując aplikacje Google Authenticator lub Microsoft Authenticator i zeskanuj d QR, a następnie wciśnij Zapisz
	Potwierdź poprawną Nazwa urządzenia	konfigurację poprzez wprowadzenie kodu z aplikacji 278115 samsung
		Zapisz Rezygnuj

Po poprawnym zapisaniu system wygeneruje 10 listę jednorazowych kodów awaryjnych na wypadek, gdyby dostęp do urządzenia mobilnego nie był w danym momencie możliwy.

Moje dane - edycja

🕒 29 min. do zakończenia sesji
DANE ZOSTAŁY ZAPISANE POPRAWNIE
Poniżej znajduje się 10 jednorazowych kodów zapasowych, które możesz wykorzystać w przypadku braku dostępu do urządzenia uwierzytelniającego.
WAZNE INFORMACJE: - Zapisz wszystkie 10 kodów w bezpiecznym miejscu i nie udostępniaj nikomu. - Nie przechowuj kodów na tym samym urządzeniu co aplikacja 2FA. - Każdy kod może być użyty tylko raz. - Sprawdź poprawność zapisanych kodów przed zamknięciem tego okna.
 001X-nfhG-eXfm-A8eV U3V2-AHYj-b3lr-iDR6 19nP-tJrF-kTcm-nE6i WsY7-Zljo-qwmV-NIBg vjuI-MhYI-GHuP-kMKI 8QzE-Lmsi-xUCm-69dd GMwI-Jx2l-30P9-C6yk 3iF1-ugIZ-5xvL-7MUj pDwT-yJLP-ovDa-MW51 CR3n-0kHp-2asC-wOKD
ОК

Należy przeczytać i stosować zasady opisane w sekcji WAŻNE INFORMACJE.

Po wyczerpaniu kodów jednorazowych lub ich zagubieniu można uzyskać listę kolejnych 10 na ekranie 'Moje dane' poprzez przycisk 'Generuj listę kodów'.

Moje dane - edycja						M
		(9 28 min. do za	kończenia sesj	i	
	E-mail	moje@mail.pl				
	Pytanie kontrolne	IMIĘ PSA/ KOTA		~		
	Odpowiedź	TAKUŚ]
	Usługa uwierzytelnia	ania dwuskładnikowego	0			
	Nazwa urządzenia				urządzenie domyślne	
	Generuj listę kodó	w				
			Zapisz	Rezygnuj		

Wygenerowanie nowych kodów skutkuje anulacją wcześniej wygenerowanych kodów jednorazowych.

Po włączeniu usługi i konfiguracji zainstalowanej aplikacji, przy każdym następnym logowaniu system będzie wymagał wprowadzenia:

• Użytkownika i hasła (jak dotychczas)



• Po prawidłowym wpisaniu prawidłowych wartości następuje zalogowanie do systemu i uruchomienie drugiego etapu autoryzacji. Pojawi się dodatkowy ekran autoryzującym kodem z aplikacji AUTHENTICATOR:

WPROWADŹ KOD Z APLIKACJI AUTHENTICATOR
Wprowadzenie błędnego kodu spowoduje wylogowanie. Kod
Użyj kodu jednorazowego

• Należy na urządzeniu mobilnym uruchomić aplikację AUTHENTICATOR



• przepisać kod wygenerowany przez tę aplikacje do okienka w systemie



Uwaga: operator ma 30 sekund na wprowadzenie kodu. Po upływie tego czasu aplikacja generuje automatycznie nowy kod, który będzie obowiązywał przez kolejne 30 sekund..

WPROWADŹ KOD Z APLIKACJI AUTHENTICATOR
Trzykrotne wprowadzenie błędnego kodu spowoduje wylogowanie. Kod 000000
Użyj kodu jednorazowego
OK Bernari

• Po prawidłowym wpisaniu kodu oraz przyciśnięciu OK logowanie zostanie zakończone i system udostępni przydzielone funkcje.

W przypadku braku dostępu do urządzenia mobilnego można skorzystać kodu jednorazowego. W tym przypadku należy zaznaczyć pole 'Użyj kodu jednorazowego'. Ekran zmienia wygląd – pole 'Kod' zwiększa swoją długość do 16 znaków w 4 grupach.

	WPROWADŹ KOD KOD JEDNORAZOWY
Trzykrotne	wprowadzenie błędnego kodu spowoduje wylogowanie.
Kod	2000(-)000(-)000()
2 1	Jżyj kodu jednorazowego
	OK Rezygnuj

Po prawidłowym wprowadzeniu dowolnego kodu z 10 możliwości i przyciśnięciu OK, nastąpi zalogowanie do systemu.

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 <u>https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-</u> <u>client/ocglkepbibnalbgmbachknglpdipeoio</u>
- 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 <u>https://apps.microsoft.com/detail/xp9m33rjsvd6jr?hl=pl-pl&gl=PL</u>
- OTPKEY Authenticator https://apps.microsoft.com/detail/xp9mcl9t4jfz0b?hl=en-us&gl=US
- Oracle Mobile Authenticator
 <u>https://apps.microsoft.com/detail/9nblggh4nsh8?hl=en-us&gl=US</u>

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.