

Konfiguracja uwierzytelniania dwuskładnikowego (2FA) w serwisie pocztowym

Aby zwiększyć bezpieczeństwo swojego konta pocztowego, możesz włączyć uwierzytelnianie dwuskładnikowe (2FA). Poniżej znajdziesz instrukcję krok po kroku jak włączyć dodatkowe zabezpieczenie konta.

Spis treści

1.	Instalacja aplikacji do uwierzytelniania dwuskładnikowego.....	2
1.1.	Instalacja oprogramowania do uwierzytelniania dwuskładnikowego (2FA).....	2
1.2.	Instalacja aplikacji na smartfonie	2
2.	Włączenie uwierzytelniania dwuskładnikowego w serwisie pocztowym.....	3
2.1.	Przejdź do ustawień.....	3
2.2.	Pierwsze uruchomienie oraz konfiguracja ogólna na przykładzie popularnych aplikacji 5	
2.3.	Codzienne korzystanie z 2FA (podstawowy scenariusz).....	13
2.4.	Sytuacje awaryjne	13

1. Instalacja aplikacji do uwierzytelniania dwuskładnikowego

1.1. Instalacja oprogramowania do uwierzytelniania dwuskładnikowego (2FA)

Aby móc korzystać z 2FA, niezbędna jest instalacja aplikacji typu „authenticator”, która będzie generować jednorazowe kody uwierzytelniające. Najczęściej używane aplikacje to:

- Microsoft Authenticator
- Google Authenticator

1.2. Instalacja aplikacji na smartfonie

Otwórz sklep z aplikacjami na swoim smartfonie (w zależności od używanego systemu):

- ✓ Google Play (dla Androida)
- ✓ App Store (dla iPhone)

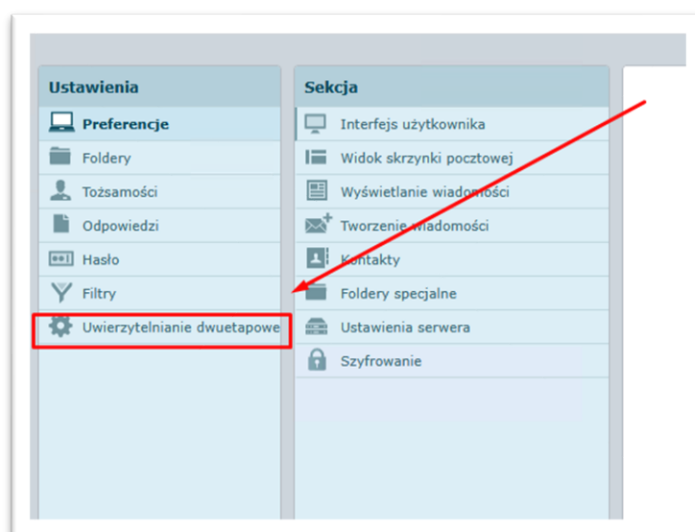
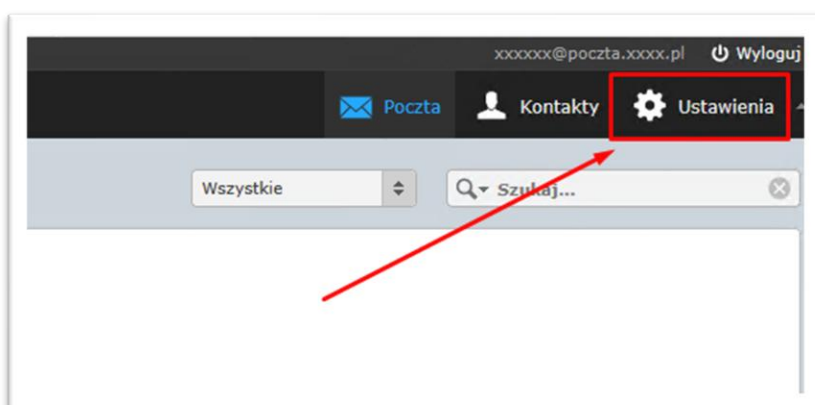
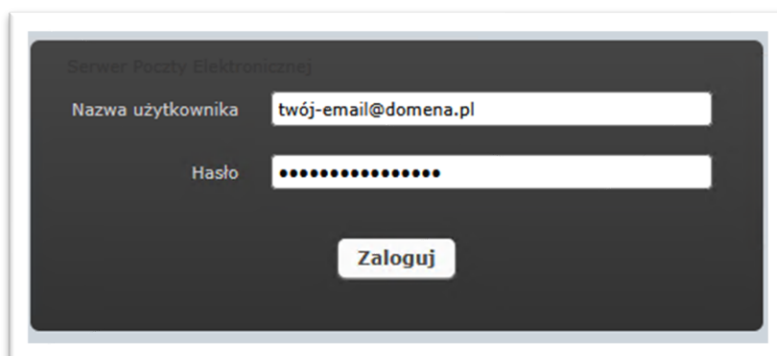
Następnie:

- Wyszukaj aplikację w sklepie z aplikacjami, wpisując np. Microsoft Authenticator.
- Kliknij „Zainstaluj” i poczekaj na zakończenie instalacji.
- Po zakończeniu instalacji uruchom aplikację – możesz zostać poproszony o skonfigurowanie zabezpieczeń (np. kod PIN lub biometryka) przy pierwszym uruchomieniu.

2. Włączenie uwierzytelniania dwuskładnikowego w serwisie pocztowym

2.1. Przejdź do ustawień

Po zalogowaniu się do serwisu pocztowego przez przeglądarkę, kliknij „Ustawienia”, a następnie wybierz zakładkę „Uwierzytelnianie dwuetapowe”.



Następnie na ekranie urządzenia powinien pojawić się następujący wybór:

Włącz uwierzytelnianie dwuetapowe

Uwierzytelnianie dwuetapowe chroni Twoje konto przed nieautoryzowanym dostępem. Wybierz metodę weryfikacji, której chcesz używać i kliknij Włącz aby rozpocząć proces konfiguracji.



Aplikacja mobilna

Używaj aplikacji mobilnej, żeby generować kody weryfikacyjne.

Włącz



Email

Używaj wiadomości e-mail w celu uzyskania kodów weryfikacyjnych.

Włącz

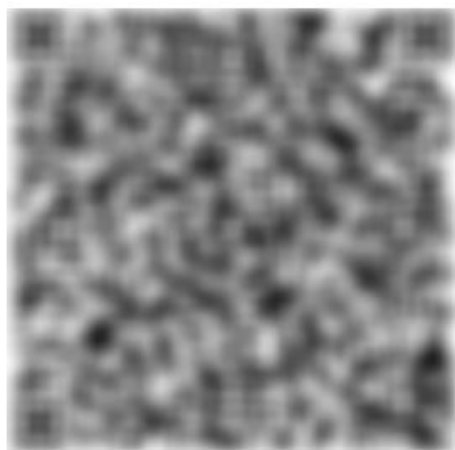
Wybieramy opcję Aplikacja mobilna, klikamy „Włącz”. Następnie przechodzimy do konfiguracji uwierzytelniania poprzez aplikację mobilną. Na naszym ekranie pojawi się krótka instrukcja oraz kod QR, który będziemy skanować przez aplikację 2FA, którą już pobraliśmy.



Konfiguracja uwierzytelniania poprzez aplikację mobilną

W [App Store](#) lub [Google Play](#) poszukaj "TOTP authenticator" i zainstaluj jedną z powyżej wyświetlonych darmowych aplikacji, takich jak: 2FA Authenticator, Microsoft Authenticator, Google Authenticator.

Skonfiguruj aplikację skanując kod QR lub wprowadzając ręcznie kod konfiguracji.



REFKEASROXUI37IR5M375VUW

Następna

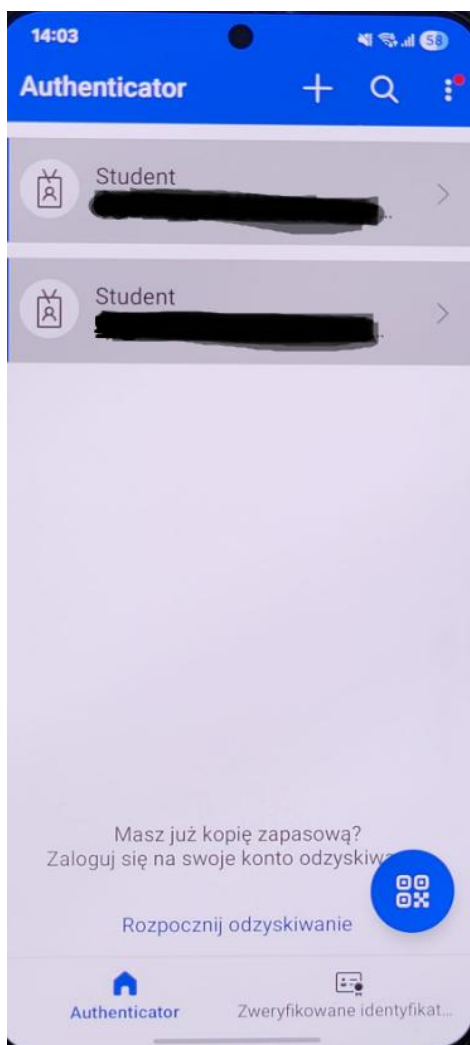
Anuluj

Przejdźmy więc do aplikacji. Omówimy konfigurację zarówno dla aplikacji Microsoft Authenticator jak i Google Authenticator.

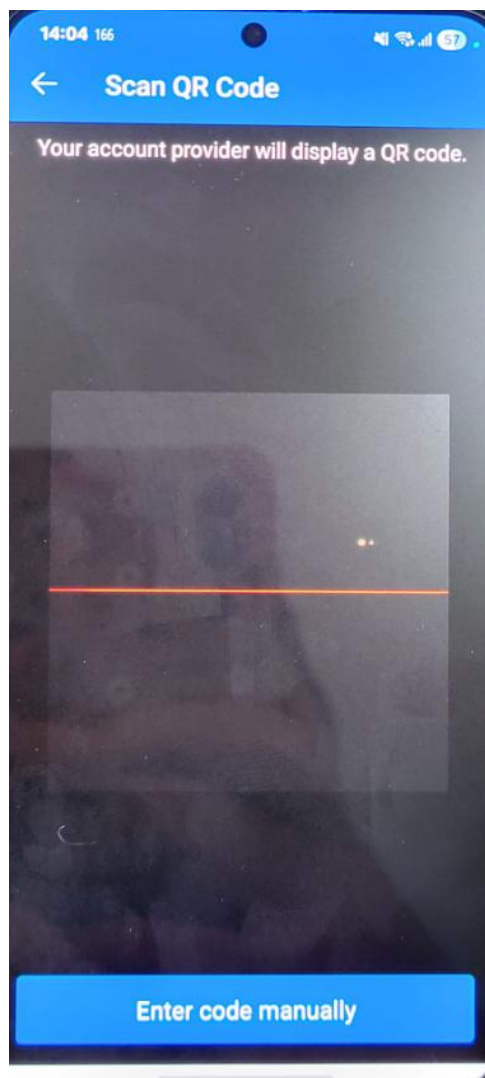
2.2. Pierwsze uruchomienie oraz konfiguracja ogólna na przykładzie popularnych aplikacji

a) Microsoft Authenticator

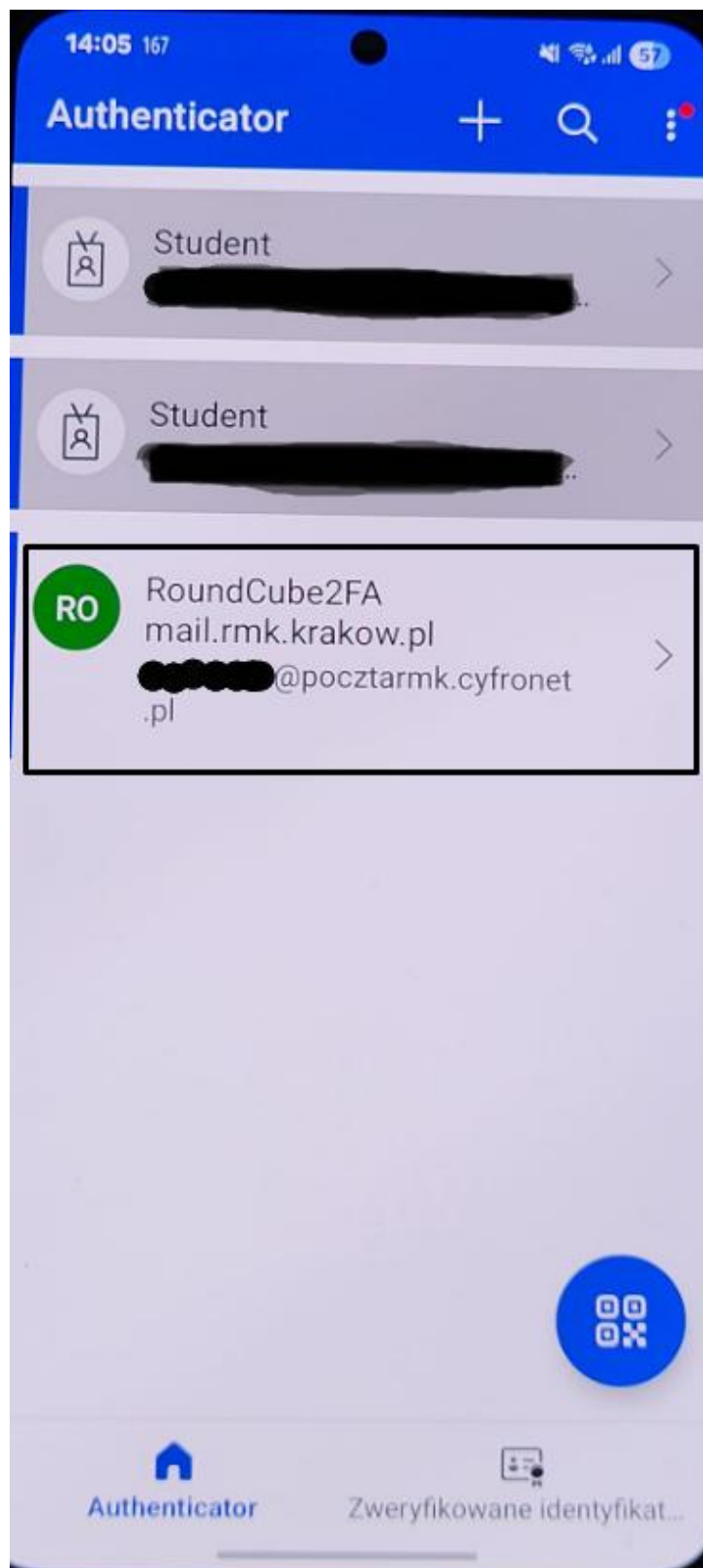
- Otwórz aplikację Microsoft Authenticator na swoim smartfonie.
- Jeśli uruchamiasz ją po raz pierwszy, przejdź przez wstępną konfigurację – ustaw zabezpieczenia dostępu do aplikacji (np. PIN, odcisk palca, rozpoznawanie twarzy).
- Gdy znajdziesz się w głównym widoku aplikacji, kliknij ikonę „+” (zwykle w górnej części ekranu), aby dodać nowe konto. Może być to również ikona kodu QR, najczęściej występująca w prawym dolnym rogu aplikacji.



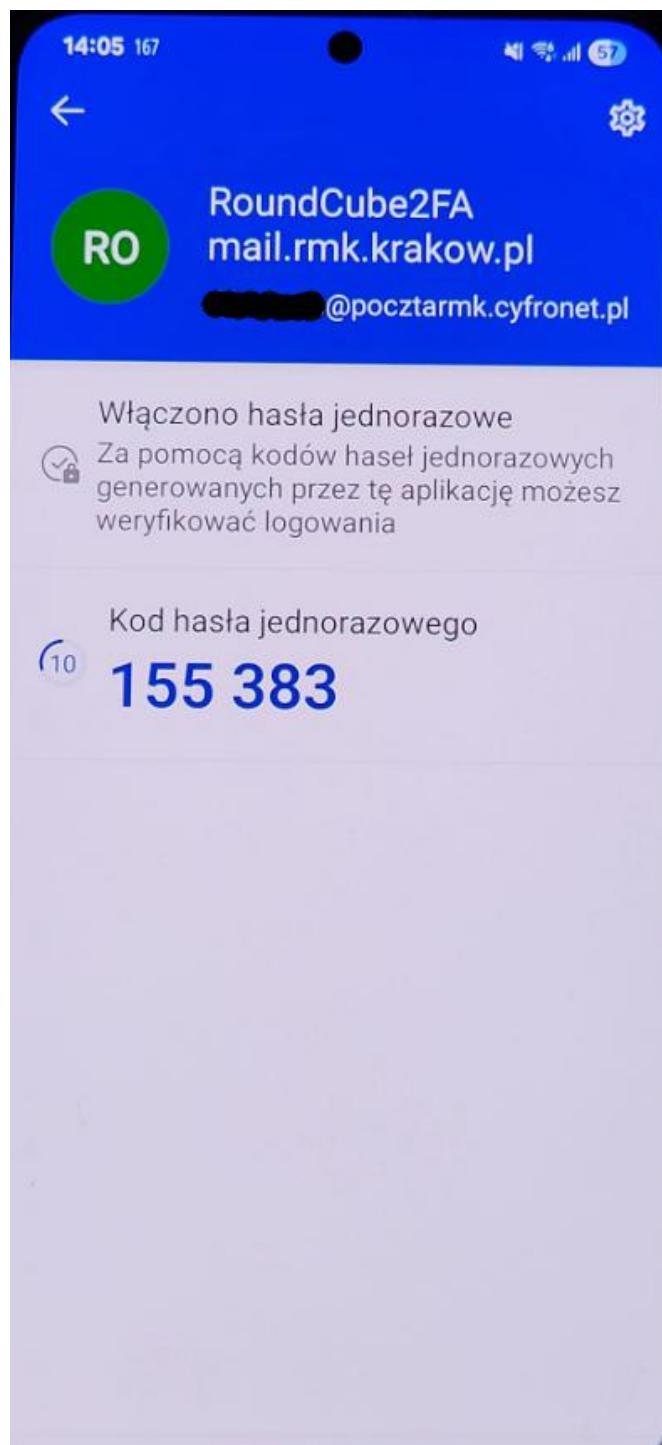
- Jeśli aplikacja poprosi o dostęp do aparatu – zezwól na to, aby możliwe było zeskanowanie kodu.
- Skieruj aparat telefonu na kod QR wyświetlony na ekranie komputera – aplikacja automatycznie doda konfigurację.



- Sprawdź nazwę dodawanego konta oraz dane

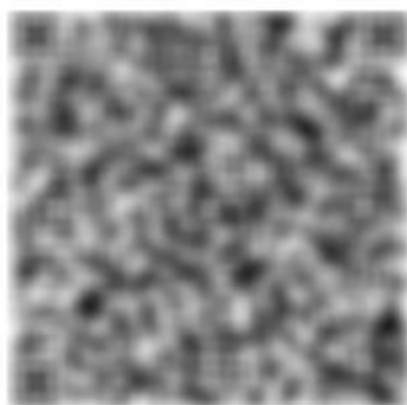


- Po wejściu w dodany serwis/usługę na ekranie smartfona pojawi się sześciocyfrowy kod – jest to Twój kod jednorazowy.



- Wróćmy teraz do naszego serwisu pocztowego. Kliknijmy w przycisk „Następna”:

ację skanując kod QR lub wprowadzając ręcznie kod konfiguracji.



REFKEASROXUI37IR5M375VUW

Następna

Anuluj

- W tym miejscu zostaniemy poproszeni o przepisanie kodu z aplikacji celem weryfikacji oraz sfinalizowania procesu dodawania dwuskładnikowego uwierzytelniania.



Konfiguracja uwierzytelniania poprzez aplikację mobilną

Podaj kod weryfikacyjny wygenerowany przez Twoją aplikację.

Zakończ

Anuluj

- Wpisujemy kod oraz klikamy „Zakończ”.
- Od teraz nasze konto posiada już aktywne uwierzytelnianie dwuskładnikowe.
- Poniżej możemy zauważyć następującą sekcję:



Kody zapasowe (10)

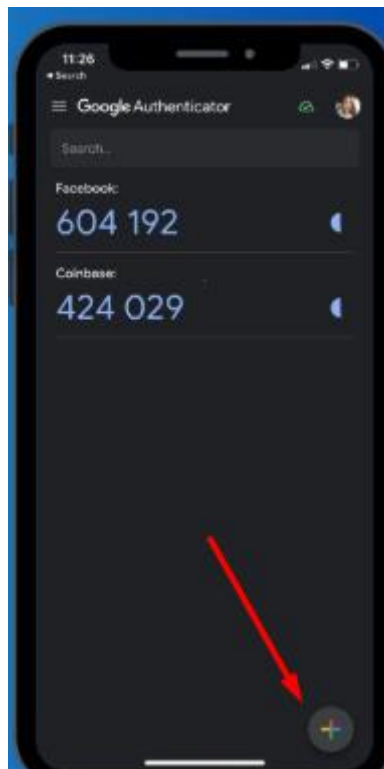
Kody zapasowe mogą być użyte zamiast standardowych kodów weryfikacyjnych w sytuacjach awaryjnych. Skopiuj je i przechowaj w bezpiecznym miejscu. Każdy z kodów zapasowych może być użyty tylko raz.

[Pokaż kody zapasowe](#) [Wygeneruj nowe kody zapasowe](#)

- Są to tzw. kody zapasowe, czyli jednorazowe hasła/klucze, dzięki którym możemy uzyskać dostęp do konta w sytuacji gdy utracimy urządzenie do dwuskładnikowej weryfikacji (np. telefon). Warto zapisać kilka kodów na przyszłość, by w sytuacji awaryjnej nie utracić dostępu do swojego konta.

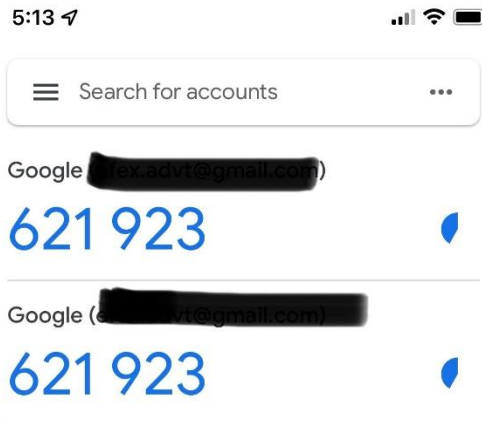
b) Google Authenticator

- Analogicznie jak w przypadku aplikacji Microsoft Authenticator, w prawym dolnym rogu wybieramy opcję dodania nowej usługi:



- Następnie wybieramy „Scan a QR code” lub „Skanuj kod QR” i skanujemy smartfonem kod QR z ekranu komputera





- Po zeskanowaniu kodu, usługa zostanie dodana do listy i możemy korzystać już z generowanych kodów



Konfiguracja uwierzytelniania poprzez aplikację mobilną

Podaj kod weryfikacyjny wygenerowany przez Twoją aplikację.

Zakończ

Anuluj

- Analogicznie jak w przypadku poprzedniej aplikacji - wpisujemy kod oraz klikamy „Zakończ”.

2.3. Codzienne korzystanie z 2FA (podstawowy scenariusz)

Podczas każdej próby logowania do systemu z aktywnym 2FA:

- Odblokuj telefon.
- Uruchom aplikację typu 2FA np. Authenticator.
- Odszukaj odpowiednią konfigurację (nazwa systemu/konta/serwisu).
- Przepisz aktualny 6-cyfrowy kod z aplikacji do formularza logowania w przeglądarce.

UWAGA: Kod jest ważny tylko przez krótki czas, dlatego wpisz go jak najszybciej po jego wygenerowaniu. Nigdy nie udostępniaj kodu osobom trzecim!

2.4. Sytuacje awaryjne

W razie utraty dostępu do aplikacji uwierzytelniającej (np. zgubiony lub zresetowany telefon), możliwe są różne scenariusze awaryjne:

Wskazówki bezpieczeństwa:

- Zapisz kody awaryjne w bezpiecznym miejscu (np. zaszyfrowanym pliku) i zawsze pamiętaj gdzie możesz je odnaleźć.
- Nie udostępniaj ich innym osobom.
- Nie instaluj aplikacji typu „authenticator” na współdzielonych urządzeniach.
- Jeśli zmienisz telefon – pamiętaj, by przenieść konfigurację aplikacji uwierzytelniającej przed zresetowaniem starego urządzenia.

UWAGA: Kody generują się automatycznie po wejściu w aplikację. Częstym i obserwowanym zjawiskiem jest również sytuacja, w której użytkownik wpisuje kod z aplikacji, który wygaśnie za kilka sekund. Może to prowadzić do komunikatów typu „Nieprawidłowy kod uwierzytelniający”. Proszę zwrócić uwagę, że nie liczy się czas w którym przepisujemy kod z urządzenia uwierzytelniającego, lecz faktycznie kiedy go wyślemy np. poprzez formularz logowania.

PORADA: Aby uniknąć potencjalnego wysłania wygaśniętego już kodu z aplikacji, zaleca się aby wpisywać wyłącznie kody o dłuższym czasie ważności np. od 20 sekund i więcej. Pozwoli to uniknąć tego typu sytuacji.