

SPOSÓB KONFIGURACJI DWUETAPOWEGO UWIERZYTELNIENIA W POCZCIE

Od dnia 04 kwietnia 2025 r. logowanie do poczty UKS poza siecią Kliniki wymaga dwuskładnikowego uwierzytelnienia.

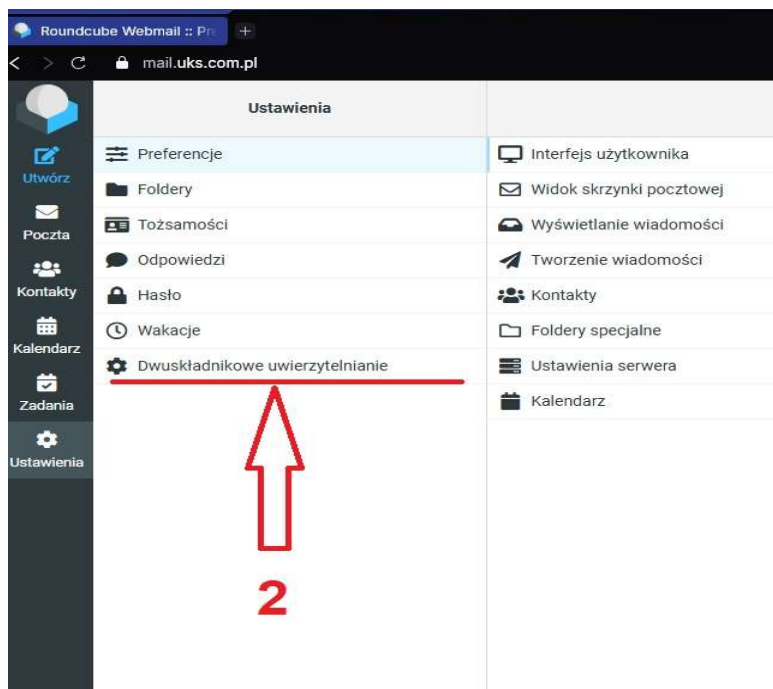
W pierwszym etapie należy zainstalować „*autentykator*” na urządzeniu, które będzie służyć do generowania kodów potrzebnych do zalogowania. Na telefonie mogą to być na przykład „*Microsoft authenticator*” lub „*Google authenticator*”, na komputerze można użyć dodatków do przeglądarek internetowych (*firefox authenticator, chrome authenticator itp.*). Należy zdecydować się na jedno rozwiązanie.

W drugim etapie należy zalogować się do poczty przez przeglądarkę internetową podając login i hasło.

Po zalogowaniu do poczty przez stronę internetową wyświetli się komunikat (1).



Następnie należy przejść do sekcji „dwuskładnikowego uwierzytelniania” (2).



Na stronie ustawień dwuetapowego uwierzytelnienia należy zaznaczyć pole „aktywuj” (3) a następnie kliknąć przycisk „generuj wszystkie pola” (4).

Dwuskładnikowe uwierzytelnianie

Aktywuj  3

Tajny klucz

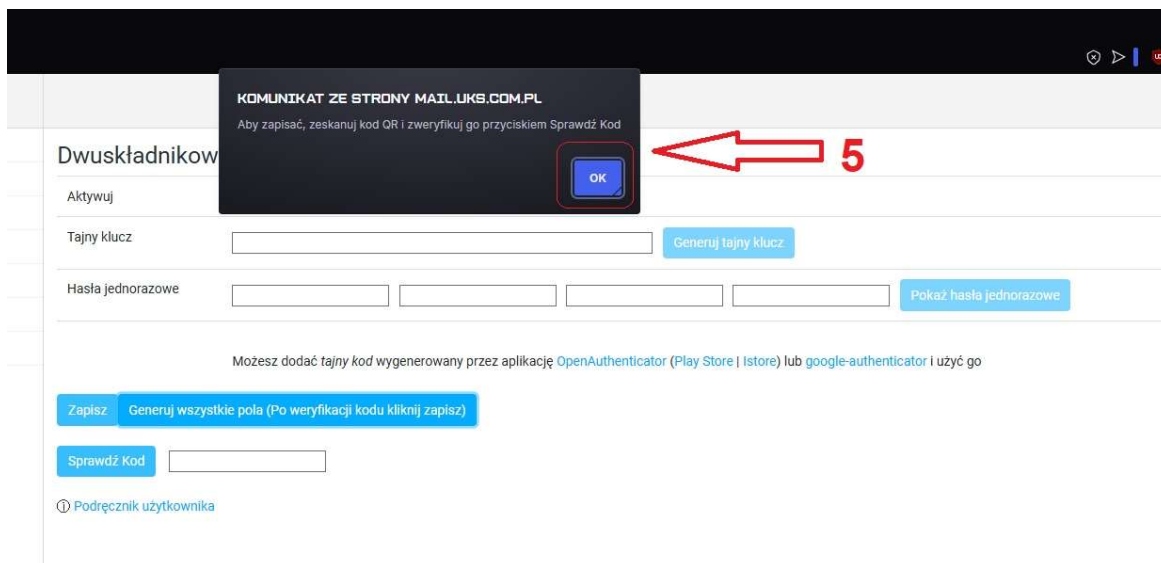
Hasła jednorazowe

Możesz dodać *tajny kod* wygenerowany przez aplikację [OpenAuthenticator](#) ([Play Store](#) | [Istore](#)) lub [google-authenticator](#) i użyć go

 4

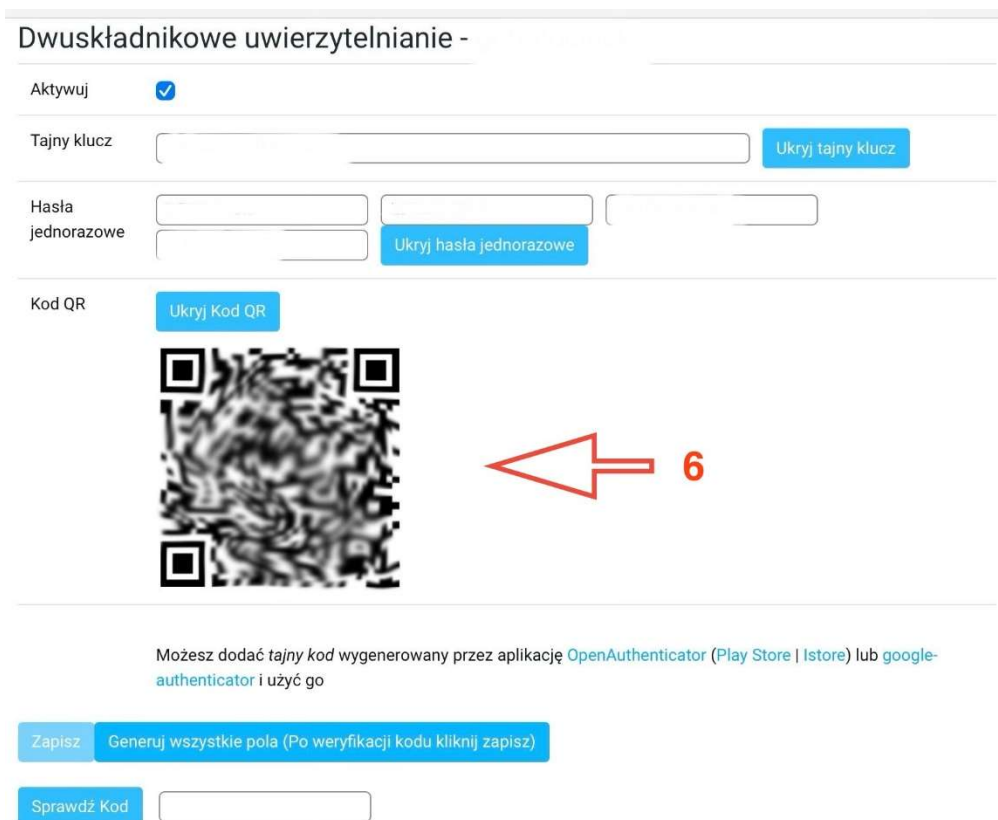
[Podręcznik użytkownika](#)

Pojawi się stosowny komunikat (5), który należy potwierdzić naciskając „ok”.



The screenshot shows a web interface for two-factor authentication. A dark grey dialog box is overlaid on top, titled "KOMUNIKAT ZE STRONY MAIL.UKS.COM.PL" with the subtitle "Aby zapisać, zeskanuj kod QR i zweryfikuj go przyciskiem Sprawdź Kod". Inside the dialog is a blue "OK" button. A red arrow labeled "5" points to this button. Below the dialog, the form includes fields for "Tajny klucz" (Secret key) and "Hasła jednorazowe" (One-time passwords), along with buttons for "Generuj tajny klucz" and "Pokaż hasła jednorazowe". At the bottom, there are buttons for "Zapisz" (Save) and "Sprawdź Kod" (Verify Code), and a link for "Podręcznik użytkownika" (User manual).

Na kolejnym ekranie pojawi się kod QR (6).



The screenshot shows the next step in the two-factor authentication process. The title is "Dwuskładnikowe uwierzytelnianie -". The "Aktywuj" (Activate) checkbox is checked. There are input fields for "Tajny klucz" (Secret key) and "Hasła jednorazowe" (One-time passwords), with buttons for "Ukryj tajny klucz" (Hide secret key) and "Ukryj hasła jednorazowe" (Hide one-time passwords). A "Kod QR" (QR code) section features a QR code and a button "Ukryj Kod QR" (Hide QR code). A red arrow labeled "6" points to the QR code. At the bottom, there are buttons for "Zapisz" (Save) and "Sprawdź Kod" (Verify Code), and a link for "Podręcznik użytkownika" (User manual).

Postępowanie przy wybraniu opcji wykorzystania aplikacji „autentykator” do generowania kodów na urządzeniu mobilnym (telefonie):

Należy otworzyć wybrany przez siebie autentykator (na urządzeniu mobilnym, telefonie), dodać nowe konto i po wybraniu rodzaju konta pojawi się możliwość zeskanowania kodu QR. Na telefonie należy zeskanować kod QR (6) za pomocą wbudowanego aparatu.


Dwuskładnikowe uwierzytelnianie -

Aktywuj

Tajny klucz [Ukryj tajny klucz](#)

Hasła jednorazowe [Ukryj hasła jednorazowe](#)

Kod QR [Ukryj Kod QR](#)



Możesz dodać tajny kod wygenerowany przez aplikację [OpenAuthenticator \(Play Store | Istore\)](#) lub [google-authenticator](#) i użyć go

[Zapisz](#) Generuj wszystkie pola (Po weryfikacji kodu kliknij zapisz)

[Sprawdź kod](#)

Po prawidłowym zeskanowaniu kodu QR w aplikacji „autentykator” pojawi się sześciocyfrowy kod, który należy przepisać w polu (7) i potwierdzić poprzez kliknięcie pola „sprawdź kod” (8). Pojawi się komunikat potwierdzający poprawność kodu, który należy zatwierdzić, a następnie należy zakończyć konfigurację klikając przycisk „zapisz” (10).

 **10** [Zapisz](#) Generuj wszystkie pola (Po weryfikacji kodu kliknij zapisz)

[Sprawdź kod](#)

[Podręcznik użytkownika](#)

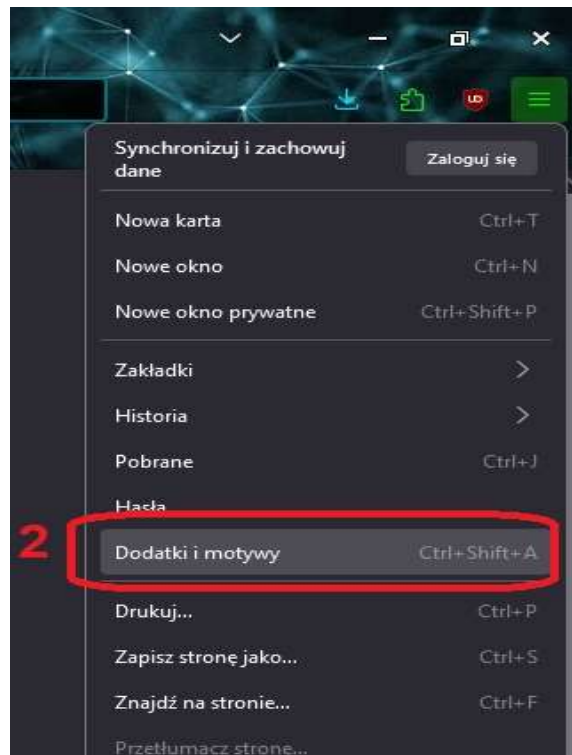
Postępowanie przy wybraniu opcji wykorzystania dodatków do przeglądarek internetowych (*firefox authenticator, chrome authenticator itp.*):

Uruchomienie „*authenticator*” w przeglądarce Firefox na terminalu lub komputerze:

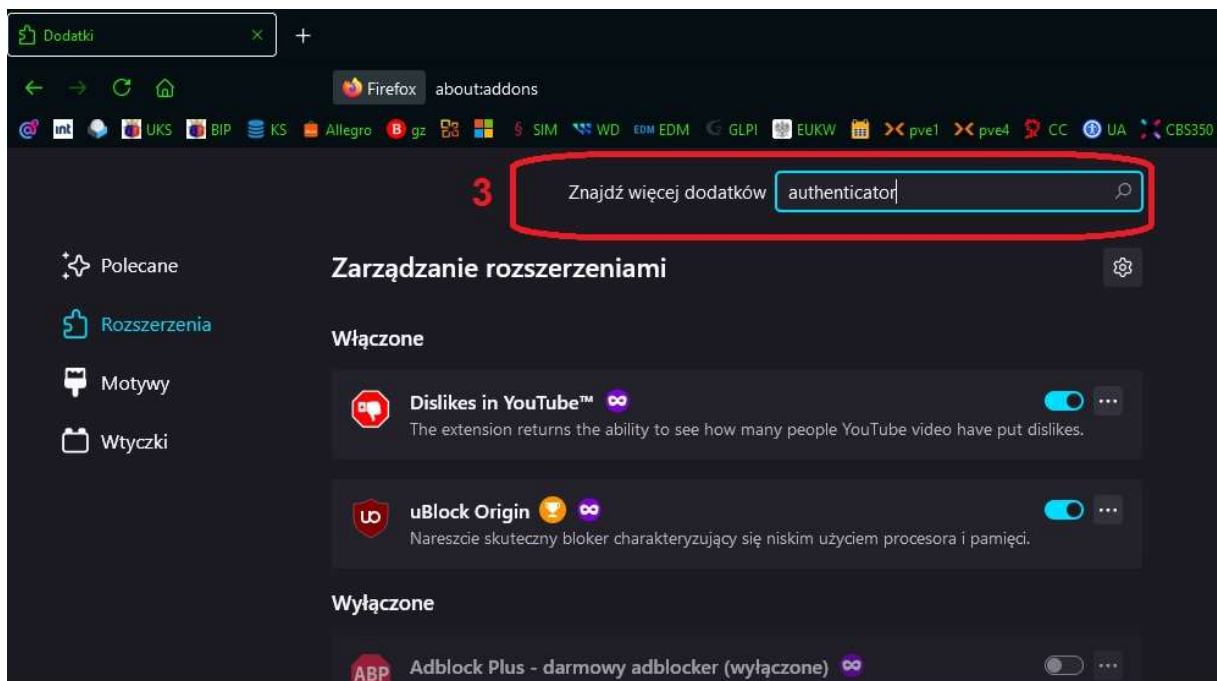
W celu instalacji „*authenticator*” należy otworzyć okno przeglądarki Mozilla Firefox. W prawym górnym rogu należy nacisnąć ikonę ustawień **(1)**.



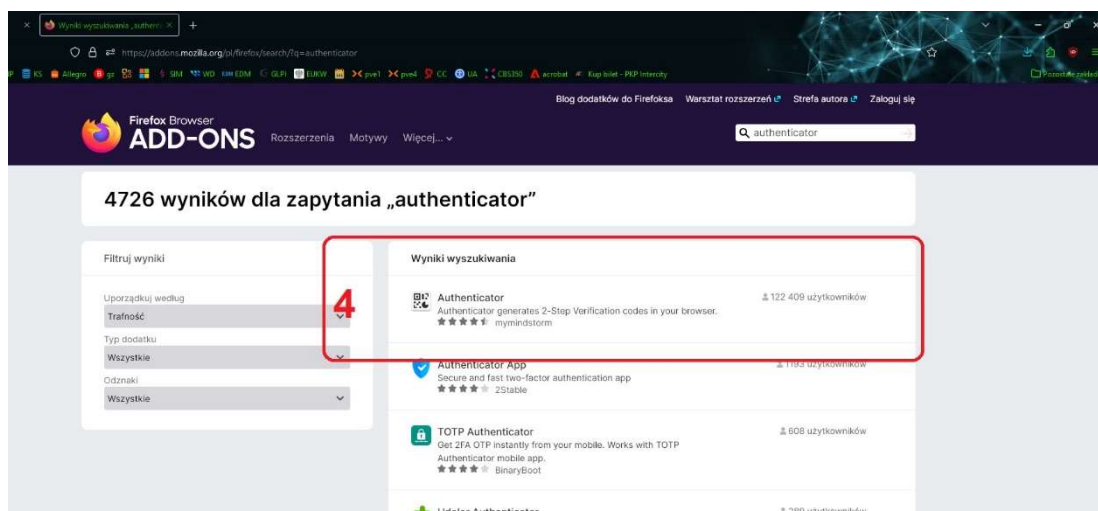
Następnie wybrać pozycję „dodatki i motywy”**(2)**



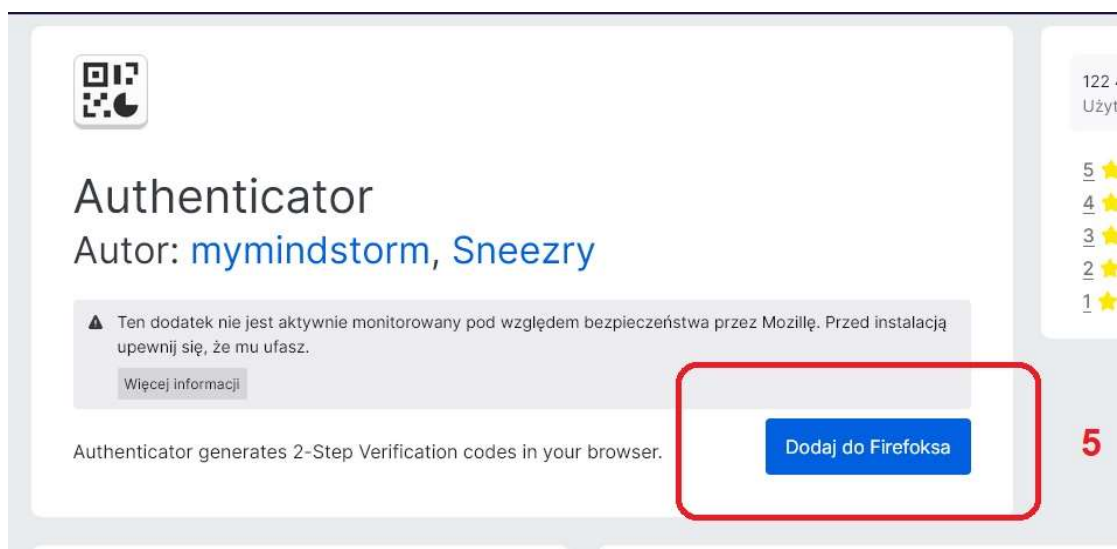
Na stronie dodatków należy w wyszukiwarce wpisać słowo „*authenticator*” (3) i nacisnąć „enter” na klawiaturze.



Otworzy się okno z listą dodatków gdzie na pierwszym miejscu powinien być potrzebny „authenticator” (4).



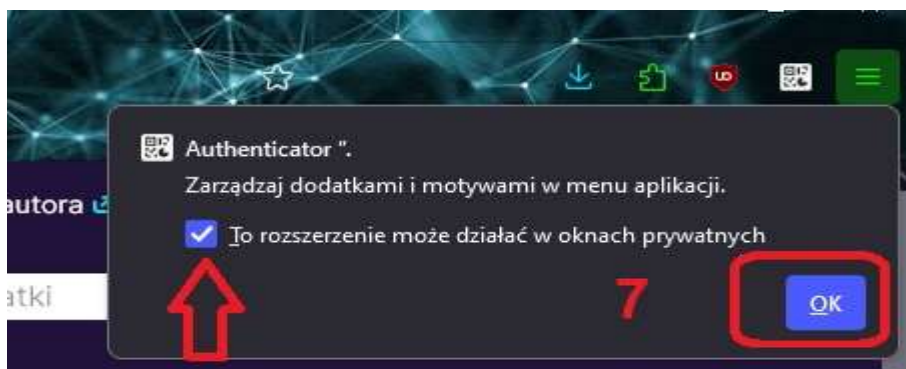
Kliknięcie na nim myszą wywoła kolejny ekran na którym należy kliknąć przycisk „dodaj do Firefoksa”(5)



W prawym górnym rogu wyświetli się potwierdzenie instalacji dodatku na którym należy kliknąć „dodaj” (6).



A następnie w kolejnym oknie „ok” (7). W tym momencie można też opcjonalnie zaznaczyć pole „to rozszerzenie może działać w oknach prywatnych” ale nie jest to konieczne.

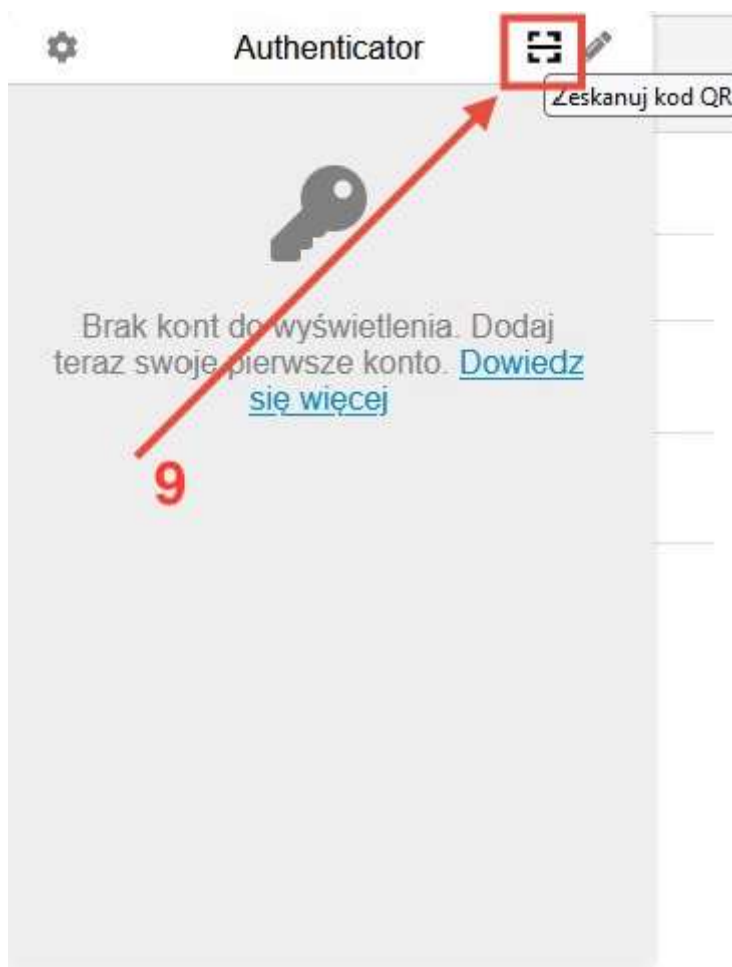


Zainstalowany dodatek będzie dostępny po naciśnięciu ikony (8).



Dla wygody można przypiąć go do paska narzędzi. Po rozwinięciu listy po prawej stronie znajduje się ikona „zębatki” po naciśnięciu której rozwinię się lista dostępnych akcji. Należy wybrać „przypnij do paska narzędzi”. Ikona „*authenticator*” (wskazana strzałką) będzie wówczas wyświetlana na prawo od ikony oznaczonej na powyższym obrazku numerem (8).

W dalszej kolejności należy uruchomić „*authenticator*” przez kliknięcie na jego ikonę. Kolejno należy kliknąć na ikonę wskazaną na rycinie (9).



Kursor myszy zmieni się na „+”. Należy obrysować kursorem wyświetlony kod QR (10).

Dwuskładnikowe uwierzytelnianie -

Aktywuj



Tajny klucz

Ukryj tajny klucz

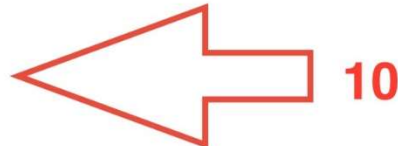
Hasła

jednorazowe

Ukryj hasła jednorazowe

Kod QR

Ukryj Kod QR



Możesz dodać *tajny kod* wygenerowany przez aplikację [OpenAuthenticator](#) ([Play Store](#) | [Istore](#)) lub [google-authenticator](#) i użyć go

Zapisz

Generuj wszystkie pola (Po weryfikacji kodu kliknij zapisz)

Sprawdź Kod

W następnej kolejności wyświetlony zostanie komunikat o dodaniu konta. Komunikat należy zatwierdzić. Ponownie należy uruchomić „*authenticator*” przez kliknięcie na jego ikonę. Wyświetlony 6-cyfrowy kod (11) należy wprowadzić w pole (12).



Wprowadzony kod należy potwierdzić poprzez kliknięcie pola „sprawdź kod” (13). Pojawi się komunikat potwierdzający poprawność kodu, który należy zatwierdzić, a następnie należy zakończyć konfigurację klikając przycisk „zapisz” (14).

Dwuskładnikowe uwierzytelnianie -

Aktywuj

Tajny klucz

Ukryj tajny klucz

Hasła
jednorazowe

Ukryj hasła jednorazowe

Kod QR

Ukryj Kod QR



14



13

Możesz dodać *tajny kod* wygenerowany przez aplikację [OpenAuthenticator](#) ([Play Store](#) | [Istore](#)) lub [google-authenticator](#) i użyć go

Zapisz

Generuj wszystkie pola (Po weryfikacji kodu kliknij zapisz)

Sprawdź Kod

12



Uwaga – pominięcie któregokolwiek kroku spowoduje nieukończenie konfiguracji.

Po wykonaniu powyższych czynności logowanie do poczty poza siecią Kliniki wymagać będzie wprowadzenia loginu i hasła, a po kliknięciu „zaloguj” pojawi się pole w którym należy przepisać kod z autentykatora.