

Konfiguracja podwójnego uwierzytelniania (MFA) dla urządzeń mobilnych z systemem iOS

Uniwersytet Jagielloński

Centrum Informatyki

Dział Infrastruktury Systemów Informatycznych

Data dokumentu: październik 2024, Wersja:1.2

Autorzy:

Estera Ambroź (estera.ambroz@uj.edu.pl)

INFORMACJA TELEADRESOWA

Centrum Informatyki, Dział Infrastruktury Systemów Informatycznych, ul. Reymonta 4, Kraków

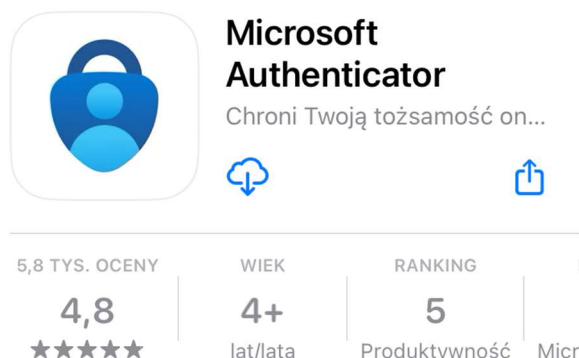
E-mail: ci@uj.edu.pl | **Web:** <https://it.uj.edu.pl>

Spis treści

Konfiguracja podwójnego uwierzytelniania (MFA) dla urządzeń mobilnych z systemem iOS	1
Etap 1 - Pobieranie aplikacji na urządzenie mobilne	3
Etap 2 - Włączanie zabezpieczenia na koncie UJ	5
Etap 3 - Zgłoszenie gotowości do włączenia podwójnego uwierzytelnienia	14
Etap 4 - logowanie po włączeniu podwójnego uwierzytelniania	15
Dodatkowe czynności wymagane dla niektórych urządzeń oraz aplikacji	18
Urządzenia z systemem iOS, na których konto UJ było uprzednio skonfigurowane	18
Klient synchronizacji OneDrive	23

ETAP 1 - POBIERANIE APLIKACJI NA URZĄDZENIE MOBILNE

Pierwszym krokiem, aby poprawnie rozpocząć konfigurację dwufaktorowego logowania (podwójnego uwierzytelniania), jest pobranie na swoje urządzenie mobilne (smartfon lub tablet) aplikacji **Microsoft Authenticator** z App Store.



Po pobraniu aplikacji i jej uruchomieniu wyświetli się informacja o prywatności danych, którą należy zatwierdzić wybierając opcję *Akceptuj*. Na kolejnym ekranie należy wybrać opcję *Kontynuuj*. Nie ma konieczności wyrażania zgody na zbieranie przez aplikację dodatkowych danych.



Firma Microsoft szanuje Twoją prywatność

Zbieramy wymagane dane diagnostyczne, aby zapewnić bezpieczeństwo i aktualizację aplikacji. Nie obejmuje to żadnych danych osobowych.

Akceptuj

Oświadczenie o ochronie prywatności
firmy Microsoft



Pomóż nam ulepszyć aplikację Microsoft Authenticator

Zezwalając nam na zbieranie dodatkowych danych innych niż osobiste, możesz pomóc nam ulepszyć aplikację. Możesz włączyć lub wyłączyć tę funkcję w dowolnym momencie na stronie Ustawienia



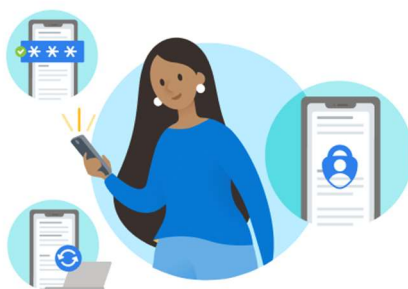
Ulepsz aplikację,
udostępniając dane użycia
aplikacji

Kontynuuj

Oświadczenie o ochronie prywatności
firmy Microsoft

Następnie wyświetli się kolejny ekran, w którym możliwy jest wybór sposobu połączenia aplikacji z kontem uniwersyteckim.

Na tym chwilowo kończymy używanie naszej aplikacji, aż do momentu włączenia zabezpieczenia na swoim koncie na komputerze. Oznacza to, że chwilowo nie wybieramy żadnej z poniższych opcji.



Zabezpiecz swoje życie cyfrowe



Zaloguj się przy użyciu
konta Microsoft

W przypadku zalogowania się przy użyciu konta Microsoft, wszystkie zapisane hasła, adresy i inne informacje wypełniane automatycznie będą dostępne na tym urządzeniu.



Dodaj konto służbowe

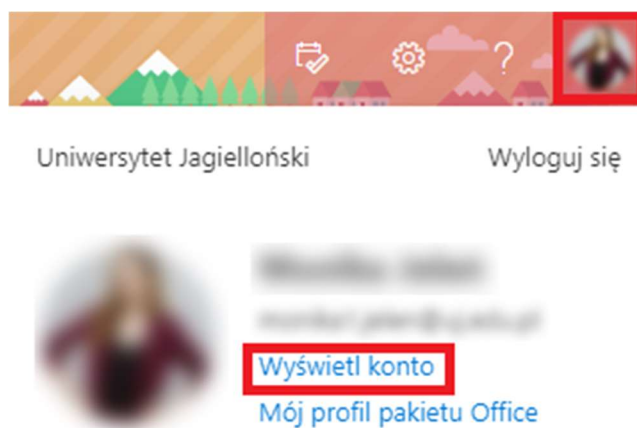


Zeskanuj kod QR

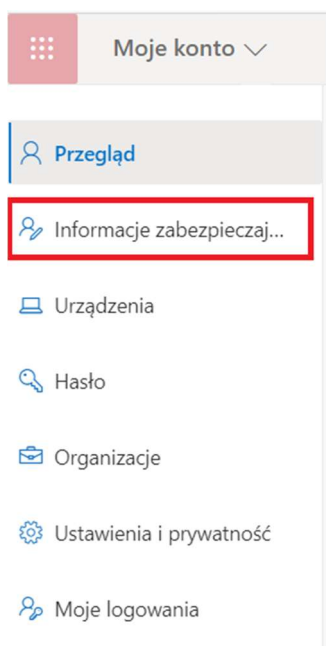
Przywróć z kopii zapasowej

ETAP 2 - WŁĄCZANIE ZABEZPIECZENIA NA KONCIE UJ

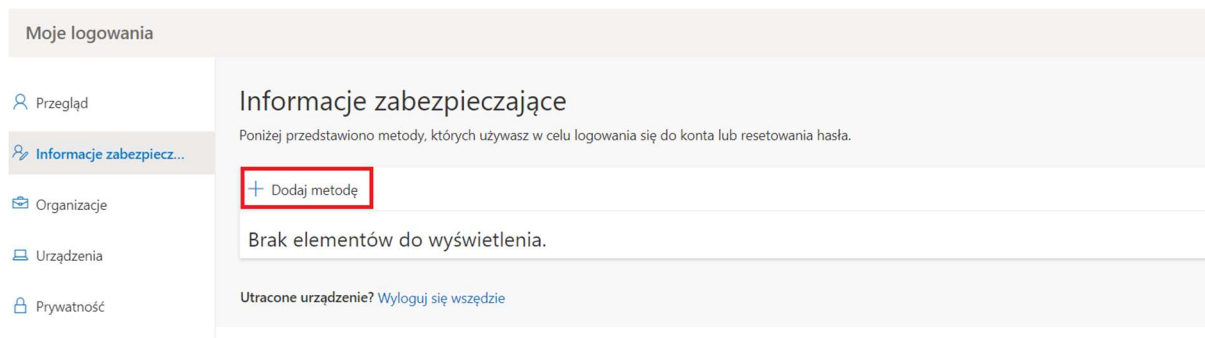
Korzystając z komputera należy otworzyć przeglądarkę internetową i zalogować się na stronie *office.com* używając uniwersyteckiego identyfikatora logowania. Następnie należy kliknąć w ikonę profilu (ze swoimi inicjałami, bądź zdjęciem), która znajduje się w prawym górnym rogu i wybrać *Wyświetl konto*.



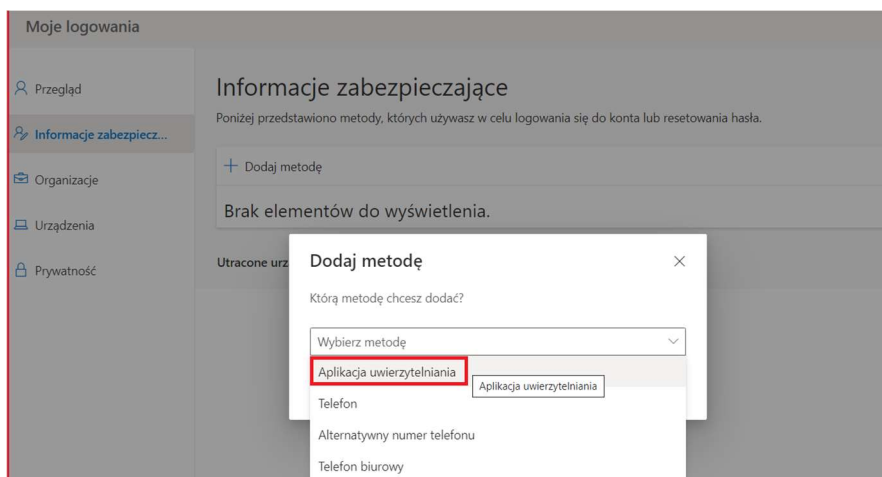
Następnie w menu po lewej stronie wybieramy *Informacje zabezpieczające*.



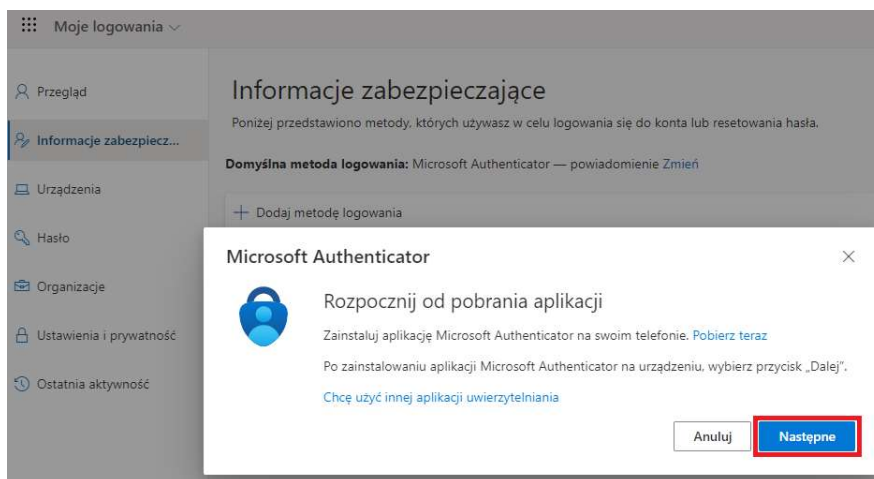
Na stronie *Informacji zabezpieczających* należy wybrać opcję *Dodaj metodę*.



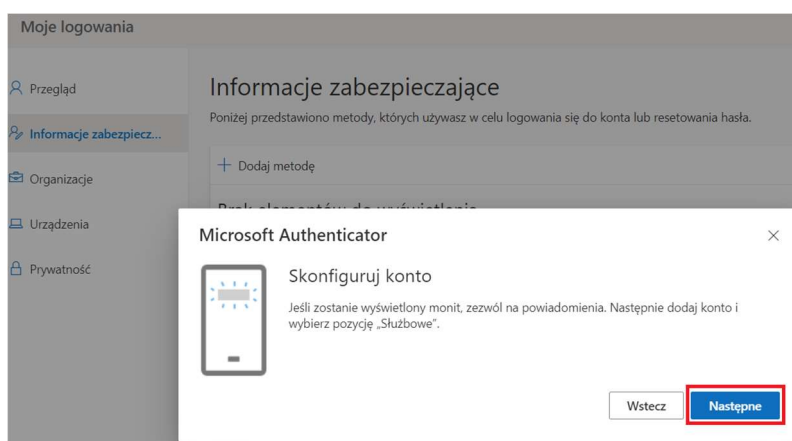
Następnie otworzy się okno, w którym wybieramy metodę drugiego uwierzytelniania. Należy wybrać pozycję *Aplikacja uwierzytelniania*, a następnie kliknąć przycisk *Dodaj*.



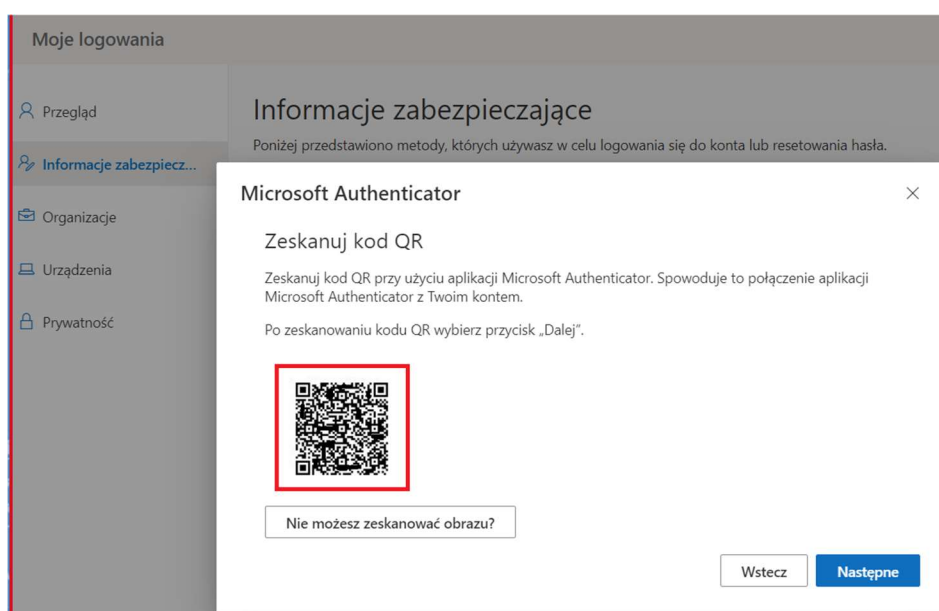
Następnie system poprosi o pobranie aplikacji. Postępując zgodnie z tą instrukcją aplikację na telefonie mamy już zainstalowaną, dlatego wybieramy opcję *Następne*.



W kolejnym kroku również należy wybrać opcję *Następne*.



Wyświetlony zostanie kod QR, który należy zeskanować za pomocą zainstalowanej wcześniej aplikacji Microsoft Authenticator.

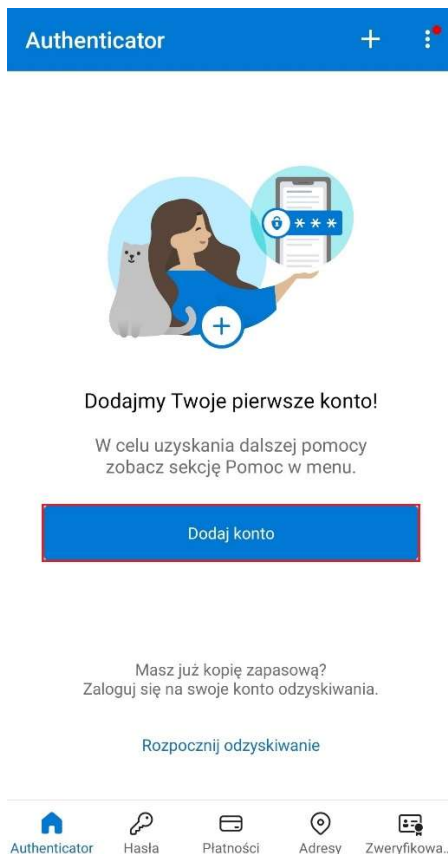


W tym celu należy ponownie uruchomić aplikację Microsoft Authenticator na urządzeniu mobilnym.

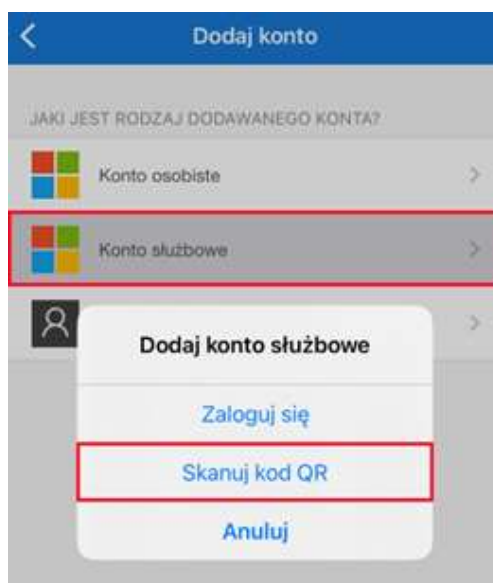
Istnieją dwa możliwe scenariusze wyświetlenia informacji na urządzeniu mobilnym użytkownika.

1. Widok dodawania nowego konta

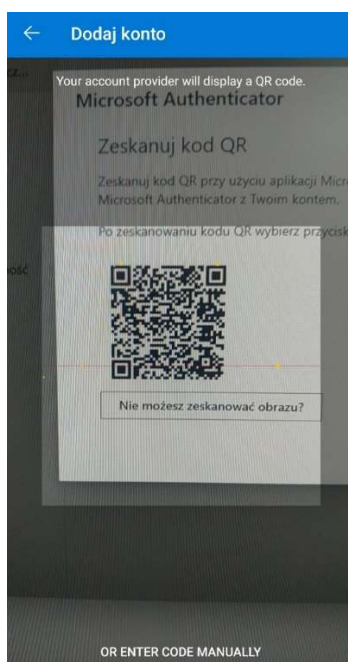
Jeśli wyświetli się poniższy widok należy wybrać *Dodaj konto*.



Następnie należy wybrać z listy *Konto służbowe*, co spowoduje pojawienie się okna. W oknie należy wybrać opcję *Skanuj kod QR*.

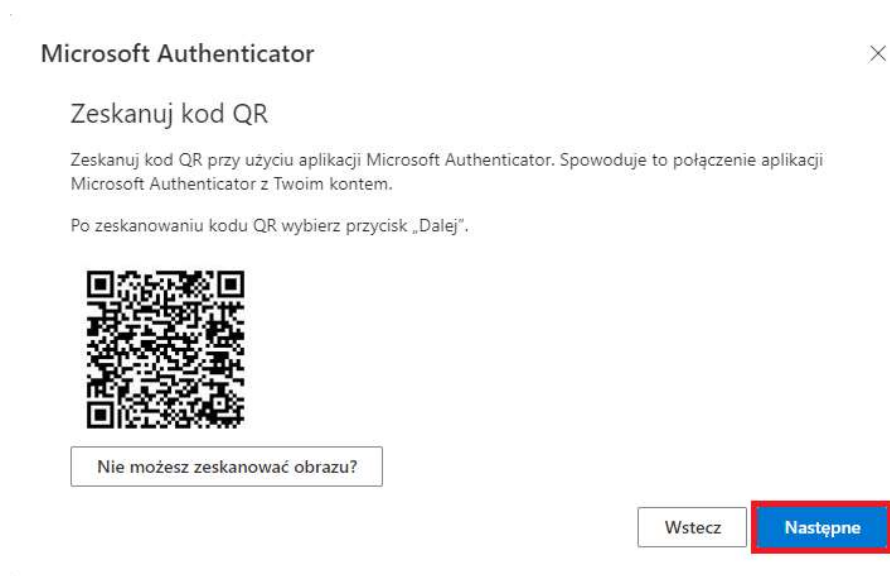


Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.

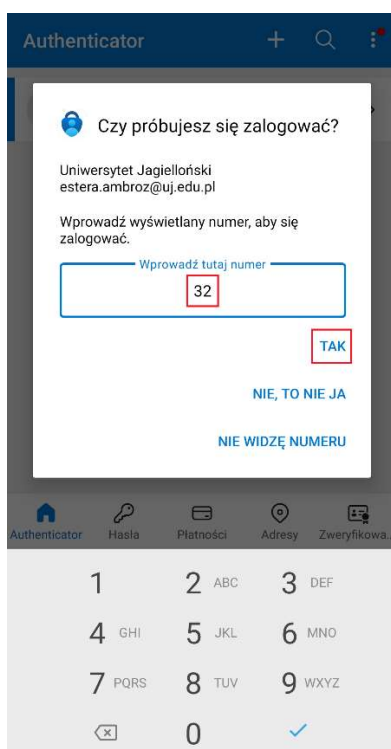


Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień aplikacji.* Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.



W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

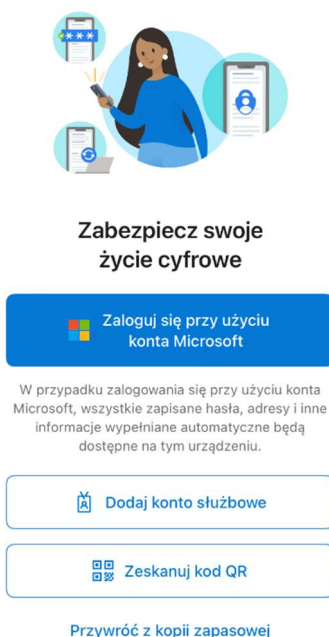


Ostatnim krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce. Po wykonaniu powyższych czynności metoda powinna zostać poprawnie skonfigurowana.

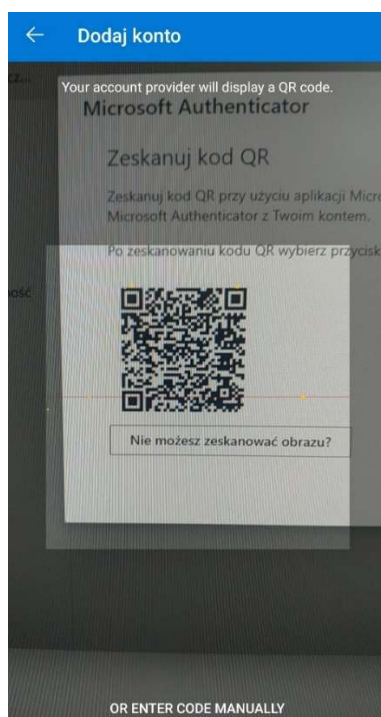


2. Widok wyboru akcji

Jeśli wyświetli się poniższy widok należy wybrać *Zeskanuj kod QR*.



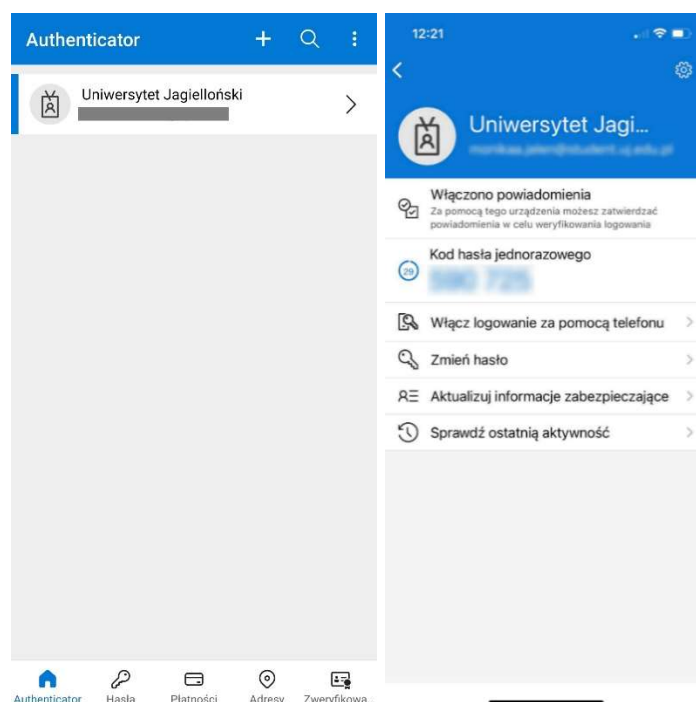
Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.



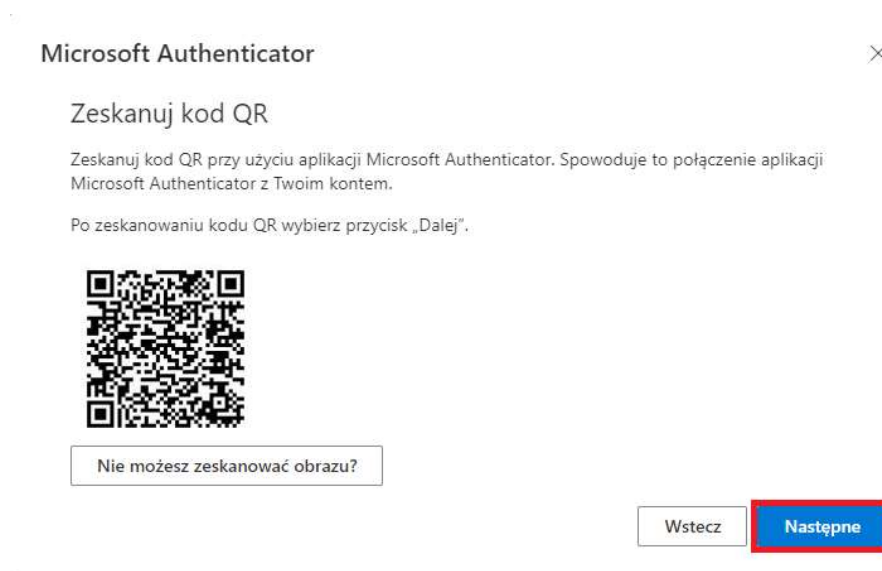
Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień*

aplikacji. Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

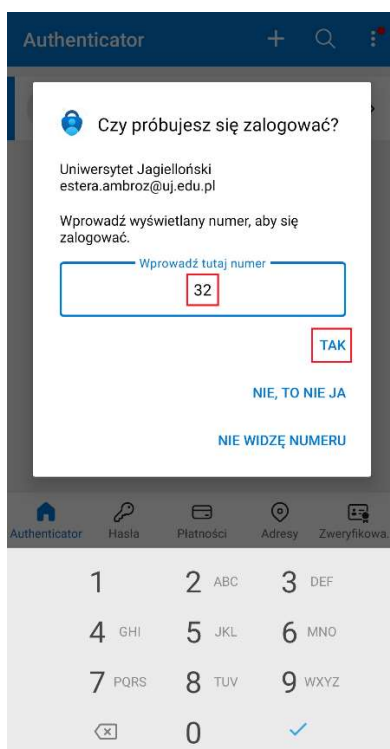
Po zeskanowaniu kodu QR w aplikacji mobilnej pojawi się konto uniwersyteckie.



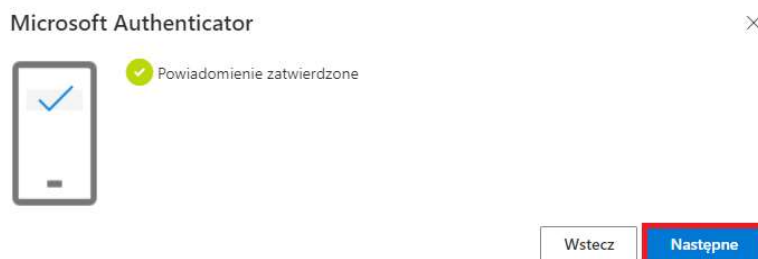
Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.



W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.



Kolejnym krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce.



Ostatnim krokiem jest wybranie domyślnej metody logowania w zakładce *Informacje zabezpieczające*. Należy wybrać *Uwierzytelnianie oparte na aplikacji – powiadomienie*.

The screenshot shows the 'Informacje zabezpieczające' (Security Information) screen in the Microsoft Authenticator app. At the top, it says 'Poniżej przedstawiono metody, których używasz w celu logowania się do konta lub resetowania hasła.' Below this, a red box highlights the text 'Domyślna metoda logowania: Microsoft Authenticator — powiadomienie Zmień'. Below this is a modal window titled 'Zmień domyślną metodę' (Change default method) with a close button (X). Inside the modal, it asks 'Której metody chcesz użyć do zalogowania się?' (Which method do you want to use to log in?). A red box highlights the selected option 'Uwierzytelnianie oparte na aplikacji — powiadomienie' (App-based authentication — notification) with a dropdown arrow. At the bottom of the modal are two buttons: 'Wstecz' (Back) and 'Potwierdź' (Confirm).

ETAP 3 - ZGŁOSZENIE GOTOWOŚCI DO WŁĄCZENIA PODWÓJNEGO UWIERZYTELNIENIA

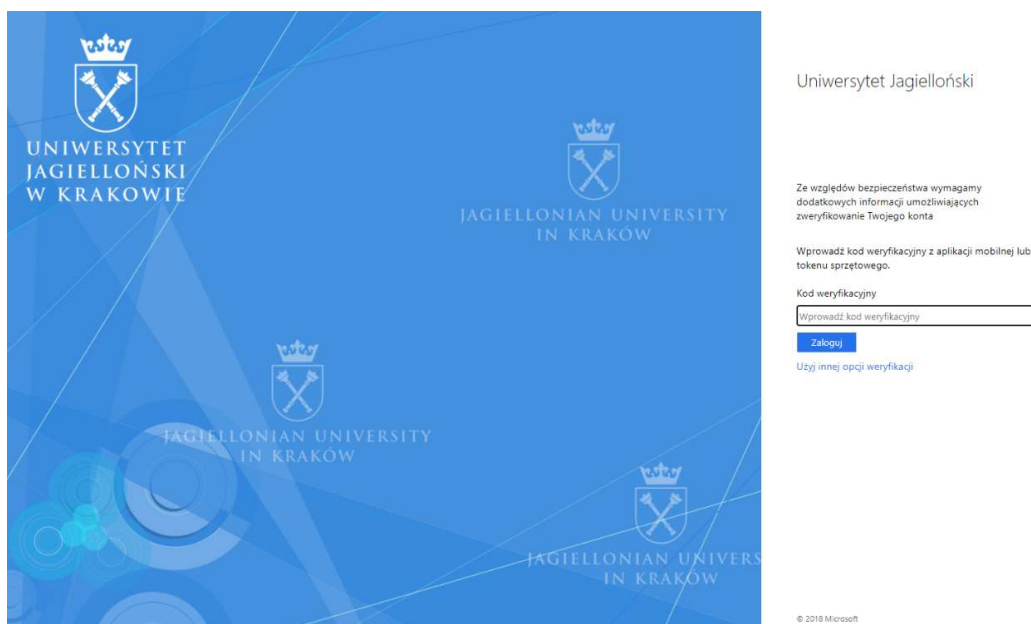
Po wykonaniu powyższych czynności można zgłosić gotowość do wcześniejszego uruchomienia podwójnego uwierzytelniania na koncie użytkownika lub poczekać do wyznaczonego terminu, który został podany w otrzymanym powiadomieniu.

Aby zgłosić chęć wcześniejszego uruchomienia metody należy skontaktować się z Działem Pomocy IT pod adresem pomocit@uj.edu.pl.

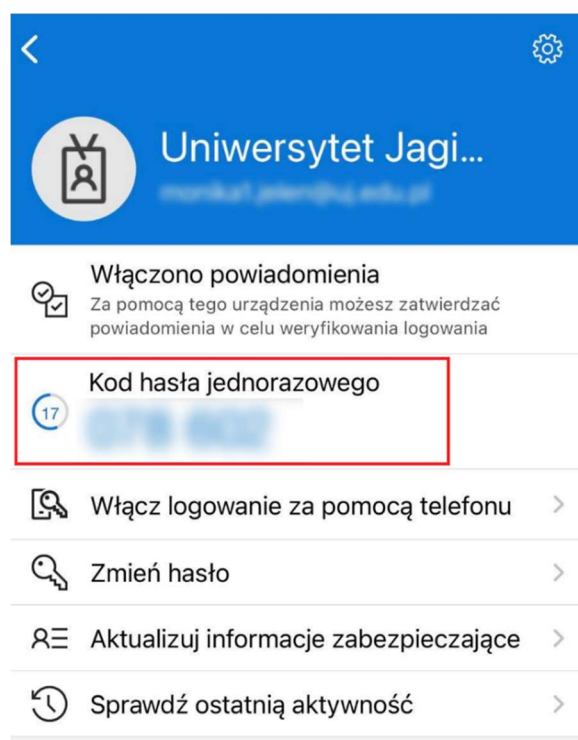
ETAP 4 - LOGOWANIE PO WŁĄCZENIU PODWÓJNEGO UWIERZYTELNIANIA

W ciągu kilku kolejnych godzin aplikacje na komputerze bądź na innych urządzeniach będą zgłaszały prośbę o potwierdzenie logowania drugim faktorem.

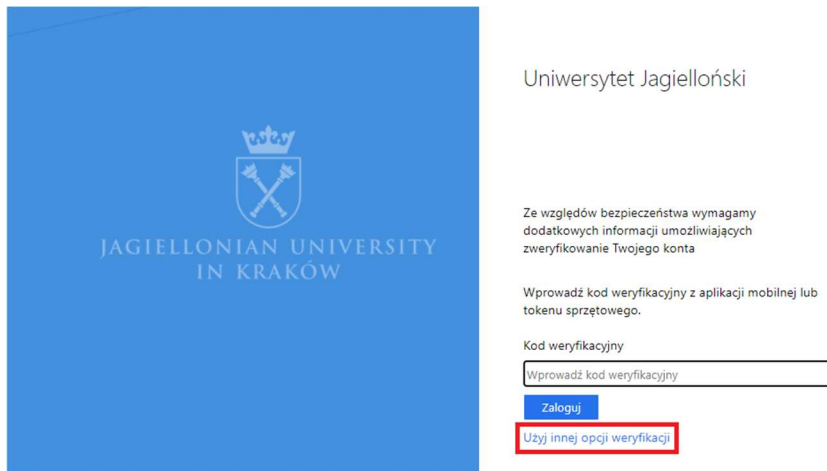
Gdy jesteśmy zalogowani na urządzeniach to zostaniemy wylogowani i poproszeni o ponowne zalogowanie, a kolejno o potwierdzenie logowania w aplikacji Microsoft Authenticator na urządzeniu mobilnym.



Gdy użytkownik zostanie poproszony o wpisanie kodu weryfikacyjnego powinien uruchomić aplikację na swoim telefonie (urządzeniu mobilnym) i wprowadzić wyświetlany kod.



Możliwa jest również zmiana opcji weryfikacji poprzez wybranie *Użyj innej opcji weryfikacji*.



Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Wprowadź kod weryfikacyjny z aplikacji mobilnej lub tokenu sprzętowego.

Kod weryfikacyjny

Zaloguj

Użyj innej opcji weryfikacji

Kolejno należy wybrać *Wyślij powiadomieni do mojej aplikacji mobilnej*.



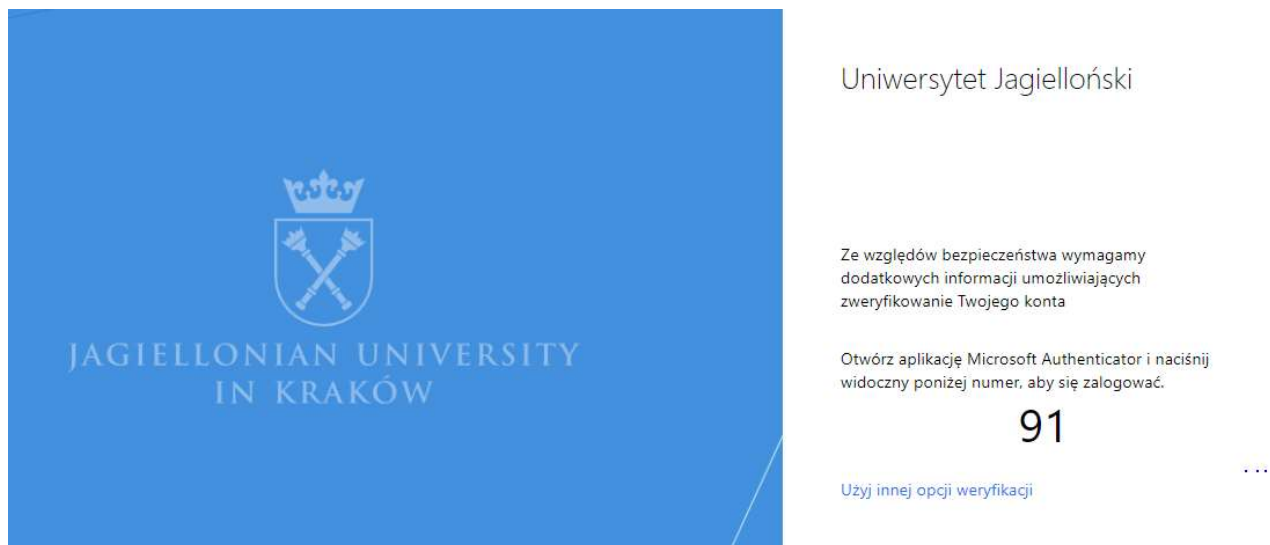
Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Jak mamy zweryfikować Twoje konto?
Użyj kodu weryfikacyjnego z aplikacji mobilnej lub tokenu sprzętowego

Wyślij powiadomienie do mojej aplikacji mobilnej

Wtedy na ekranie komputera wyświetli się liczba:



Uniwersytet Jagielloński

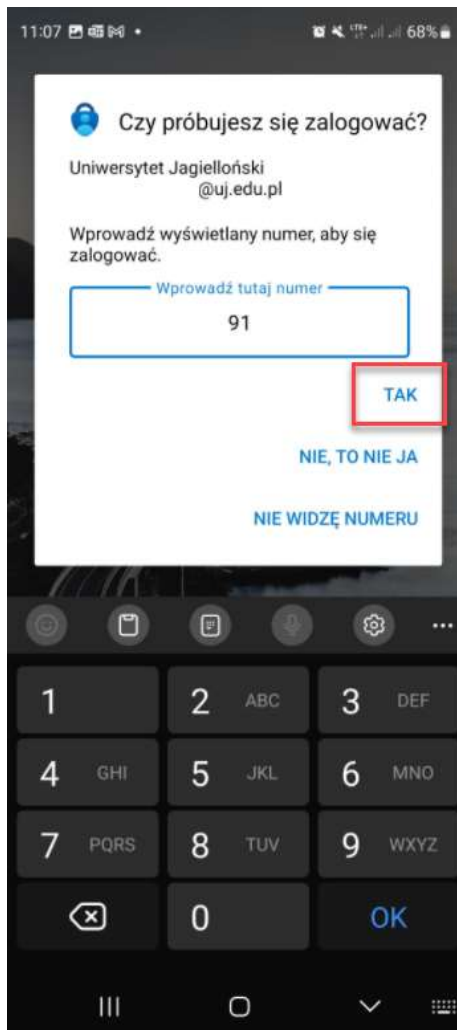
Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Otwórz aplikację Microsoft Authenticator i naciśnij widoczny poniżej numer, aby się zalogować.

91

Użyj innej opcji weryfikacji

Na naszym urządzeniu mobilnym wyświetli się komunikat, który poprosi o zatwierdzenie logowania poprzez podanie liczby wyświetlonej na ekranie komputera i kliknięcie opcji TAK.



Po wpisaniu liczby należy potwierdzić logowanie wzorem lub kodem blokady ekranu urządzenia mobilnego.

DODATKOWE CZYNNOŚCI WYMAGANE DLA NIEKTÓRYCH URZĄDZEŃ ORAZ APLIKACJI

Dla niektórych urządzeń oraz aplikacji będzie wymagane dodatkowe działanie, aby podwójne uwierzytelnianie zostało w pełni skonfigurowane oraz synchronizacja danych na urządzeniu nie została wstrzymana.

Urządzenia z systemem iOS, na których konto UJ było uprzednio skonfigurowane

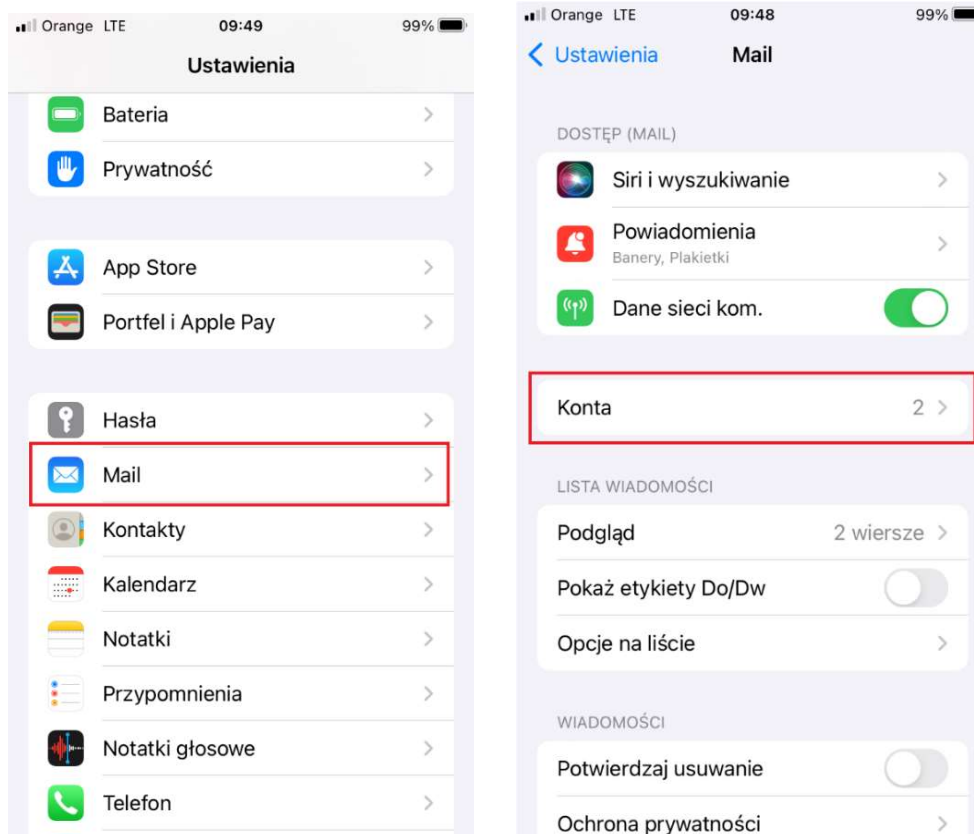
Urządzenia z systemem operacyjnym iOS (iPhone lub iPad) nie wyświetlają informacji o konieczności ponownego zalogowania się do konta po skonfigurowaniu podwójnego uwierzytelniania. Niezbędne jest w takim wypadku usunięcie konta UJ z urządzenia i ponowne dodanie.

Aby usunąć konto UJ z urządzenia iOS, należy:

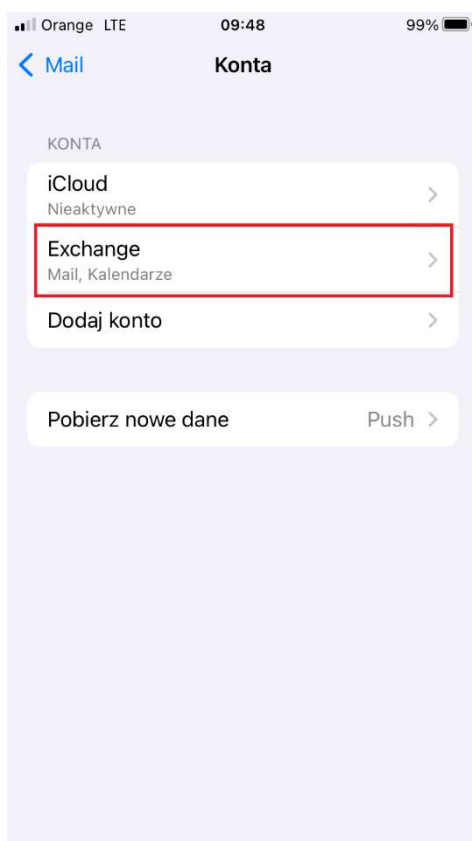
1. Otworzyć *Ustawienia* urządzenia ikoną:



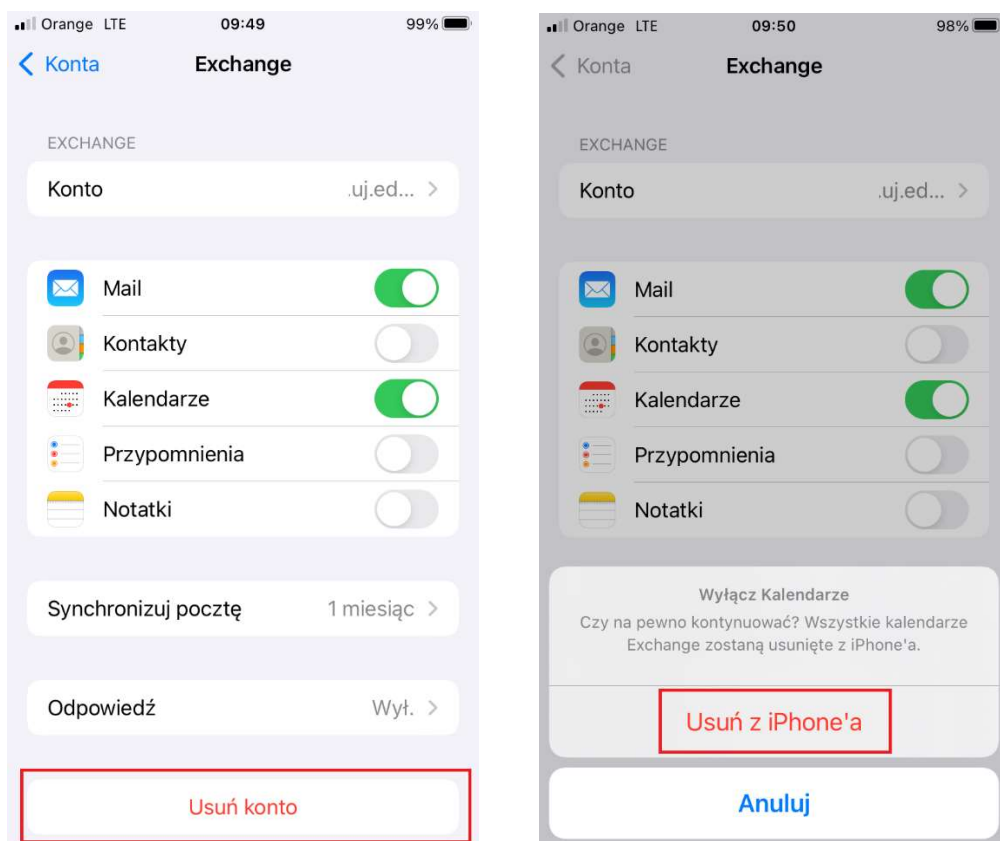
2. W ustawieniach należy przejść do opcji *Hasła i konta* (dla wersji iOS 13.x lub starszej) lub do opcji *Mail*, a następnie *Konta* (dla wersji iOS 14.x lub nowszej)



3. Należy wybrać konto UJ, nazwane standardowo *Exchange*:

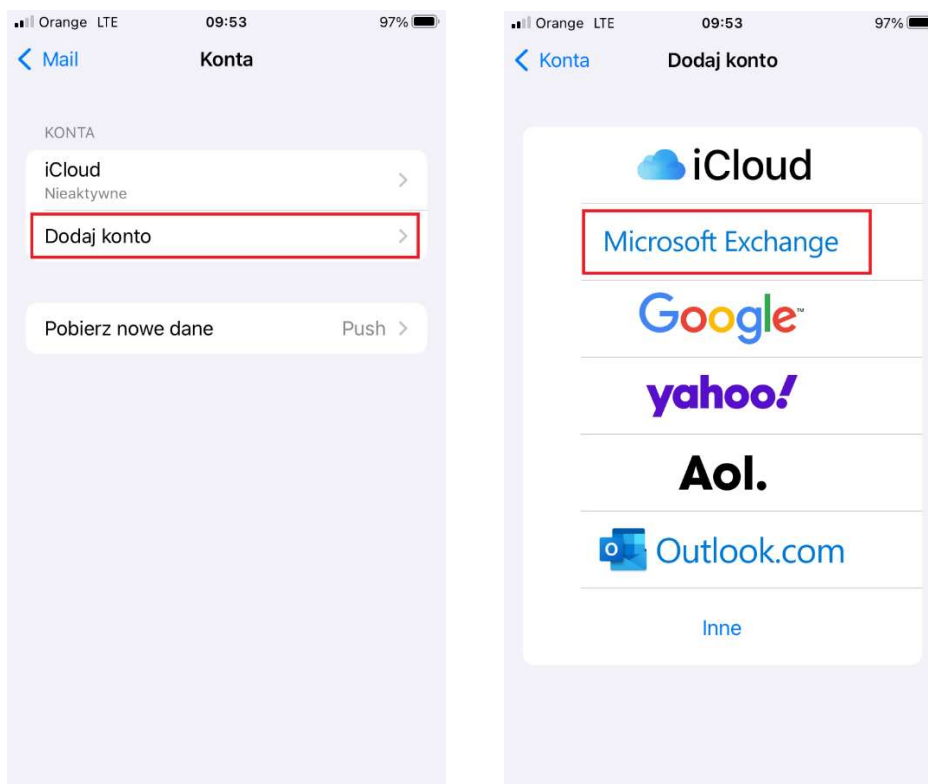


4. W widoku konta u dołu strony należy kliknąć *Usuń konto* oraz potwierdzić operację usuwania:

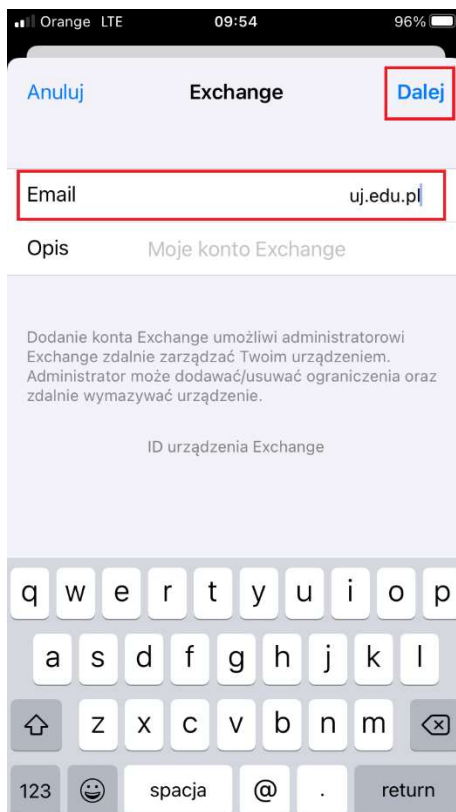


Po usunięciu konta UJ z urządzenia wyświetli się widok *Konta*, na którym nie będzie już widoczne konto UJ. W tym momencie można dodać konto na nowo poprzez następujące kroki:

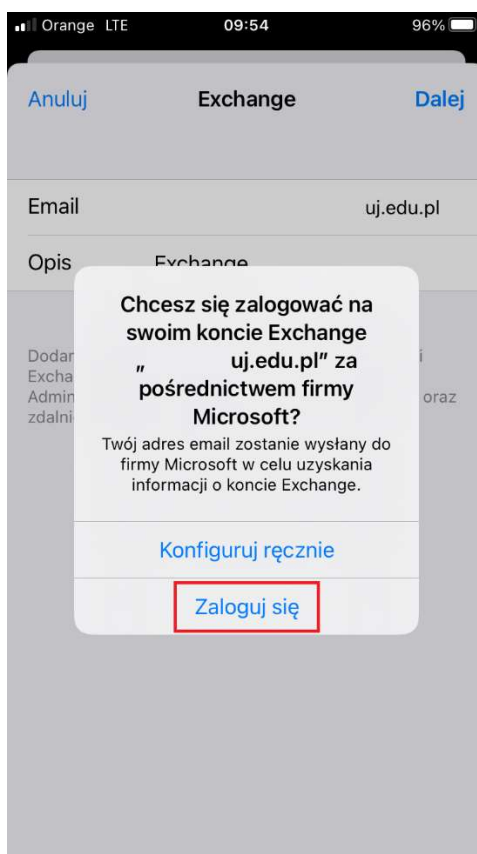
1. W widoku *Konta* wybierz opcję *Dodaj konto*, a następnie *Microsoft Exchange*:



2. W pole *Email* należy wprowadzić adres mailowy z domeny UJ oraz kliknąć *Dalej*:



3. W oknie *Czy chcesz zalogować się na swoim koncie Exchange* należy kliknąć *Zaloguj się*:



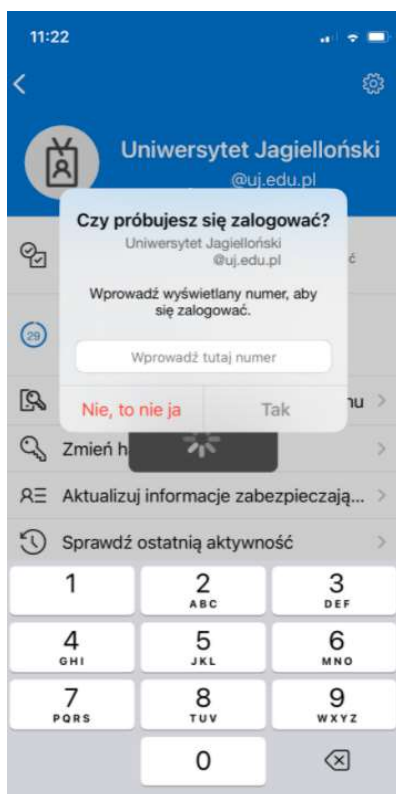
4. Zostanie wyświetlona strona logowania UJ, na której należy podać hasło:



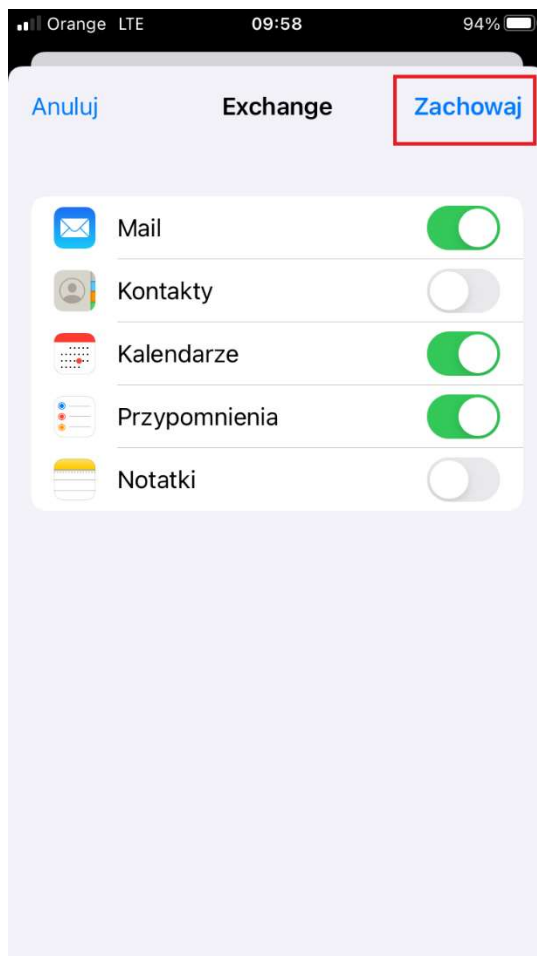
5. Następnie wyświetli się komunikat o konieczności zweryfikowania logowania drugim faktorem z informacją o liczbie, którą należy wpisać:



6. W aplikacji Microsoft Authenticator pojawi się prośba o zatwierdzenie logowania wraz z miejscem na wpisanie liczby:



7. Po zatwierdzeniu logowania należy wybrać aplikacje, które mają synchronizować dane z konta UJ do urządzenia według preferencji oraz kliknąć przycisk *Zachowaj*. Po tej czynności konto UJ jest dodane do urządzenia, a dane są synchronizowane:



Klient synchronizacji OneDrive

Aplikacja OneDrive instalowana na komputerze do synchronizacji plików z dyskiem chmurowym wymaga po skonfigurowaniu podwójnego uwierzytelnienia ponownego zalogowania się do usługi.

W tym celu należy kliknąć ikonę klienta OneDrive na pasku zadań komputera  a następnie klikając w monit z prośbą o ponowne zalogowanie, zalogować się kontem UJ.

W aplikacji Microsoft Authenticator na urządzeniu mobilnym pojawi się prośba o zatwierdzenie logowania. Po tym zatwierdzeniu aplikacja OneDrive ponownie rozpocznie synchronizację plików z komputerem.