

Procedura postępowania w przypadku wymuszenia podwójnego uwierzytelniania przez administratora - iOS

Uniwersytet Jagielloński

Centrum Informatyki

Dział Infrastruktury Systemów Informatycznych

Data dokumentu: lipiec 2024, Wersja:1.0

Autorzy:

Estera Ambroż (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

Procedura postępowania w przypadku wymuszenia podwójnego uwierzytelniania przez administratora - iOS	1
Etap 1 – Pierwsze logowanie po wymuszeniu podwójnego uwierzytelniania	3
Etap 2 - Pobieranie aplikacji na urządzenie mobilne	4
Etap 3 - Włączanie zabezpieczenia na koncie UJ	6
Etap 4 - logowanie z wykorzystaniem podwójnego uwierzytelniania	16
Dodatkowe czynności wymagane dla niektórych urządzeń oraz aplikacji	17
Klient synchronizacji OneDrive	17

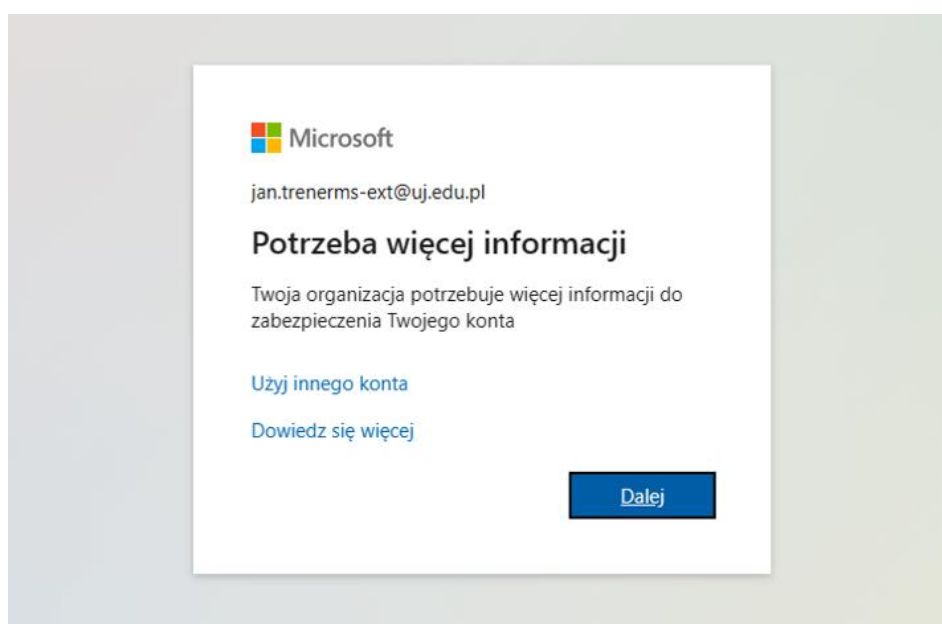
ETAP 1 - PIERWSZE LOGOWANIE PO WYMUSZENIU PODWÓJNEGO UWIERZYTELNIANIA

W dniu wskazanym jako dzień włączenia logowania dwuskładnikowego pierwsze zalogowanie wymagać będzie wykonania dodatkowych czynności przez użytkownika.

Podczas pierwszego logowania kontem w domenę @uj.edu.pl (np. do aplikacji MS Teams, Outlook, czy na stronie <https://portal.office.com>) zostanie wyświetlony komunikat *Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta*. Następnie użytkownik zostanie przekierowany do strony, na której rozpocznie się proces dodawania drugiego składnika uwierzytelniania.



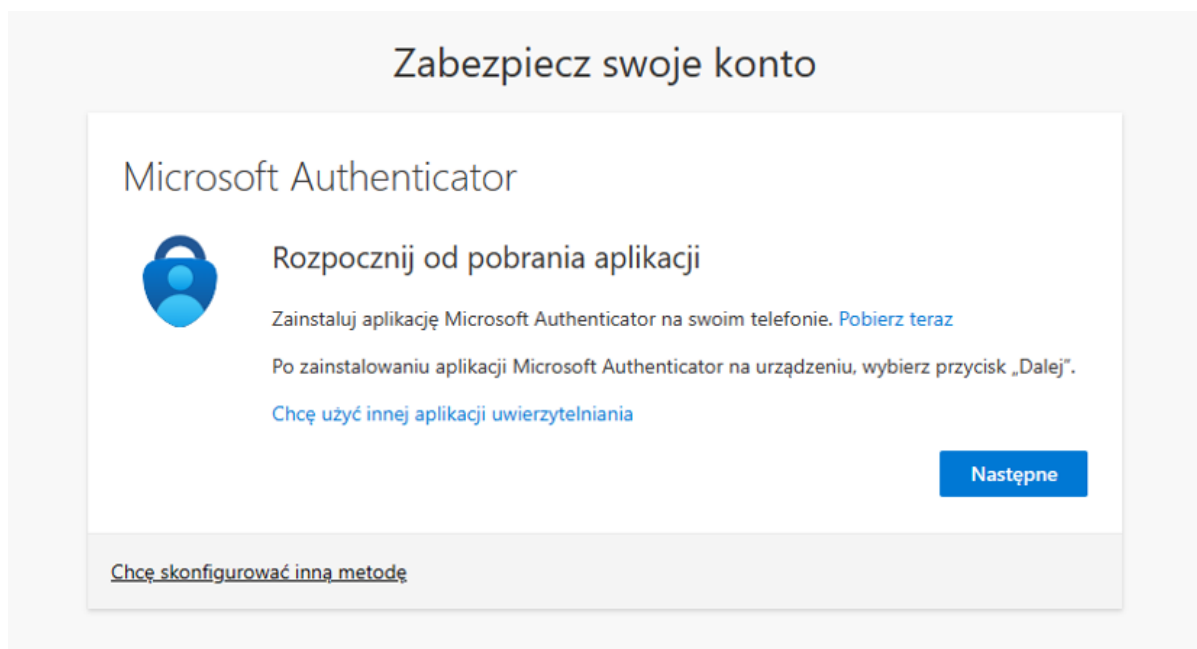
Po wyświetleniu strony z komunikatem *Potrzeba więcej informacji* należy kliknąć przycisk *Dalej*.



Pojawi się okno *Zabezpiecz swoje konto*. Aplikacja Microsoft Authenticator jest podpowiadana jako domyślny drugi składnik uwierzytelniania.

W tym miejscu można zmienić aplikację uwierzytelniania na inną *Chcę użyć innej aplikacji uwierzytelniania* lub dodać metodę uwierzytelniania poprzez numer telefonu *Chcę skonfigurować inną metodę*.

W przypadku wybrania aplikacji należy rozpocząć od jej pobrania ze Sklepu Google Play.



ETAP 2 - POBIERANIE APLIKACJI NA URZĄDZENIE MOBILNE

Pierwszym krokiem, aby poprawnie rozpocząć konfigurację dwuskładnikowego 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 *Zgadzam się*.



Twoja prywatność jest ważna

Zbieramy wymagane dane diagnostyczne, aby aplikacja była bezpieczna i aktualna. Nie obejmuje to Twojego nazwiska ani danych poufnych.

Gromadzimy też opcjonalne dane dotyczące użycia, aby poprawić środowisko aplikacji. W dowolnej chwili możesz zrezygnować z udostępniania opcjonalnych danych użycia, przechodząc do ustawień aplikacji.

Zgadzam się

[Zasady zachowania poufności informacji](#)

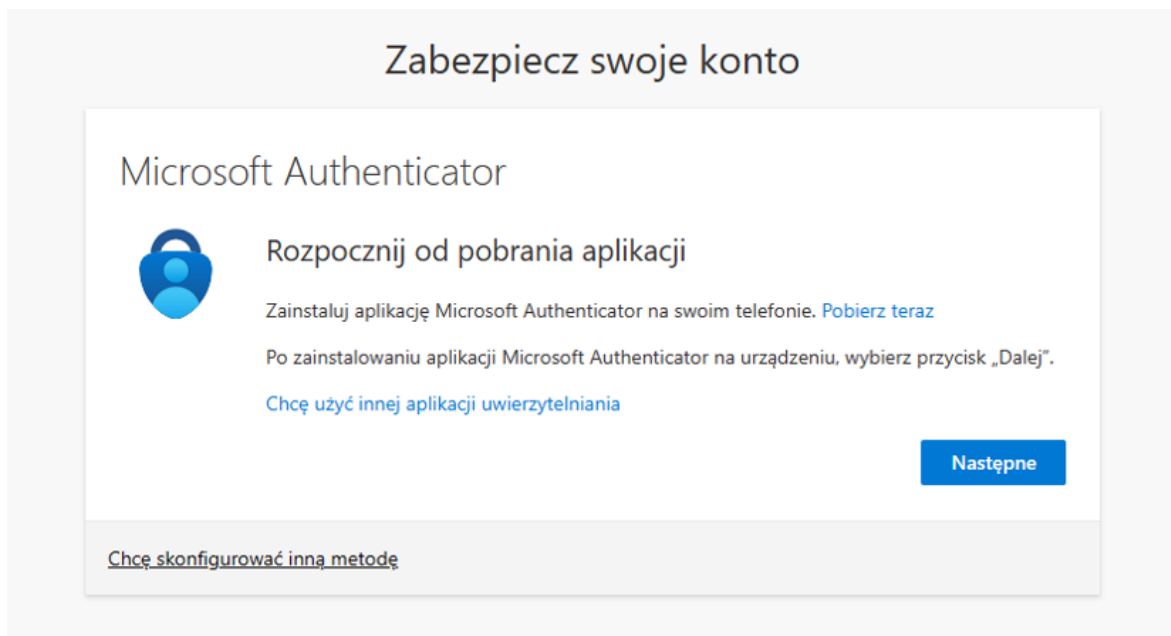
Następnie wyświetli się kolejny ekran, w którym możliwy jest wybór sposobu połączenia aplikacji z kontem uniwersyteckim.

Na ten moment należy zamknąć aplikację Microsoft Authenticator na urządzeniu mobilnym i przejść do okna przeglądarki internetowej na komputerze (z etapu 1)

ETAP 3 - WŁĄCZANIE ZABEZPIECZENIA NA KONCIE UJ

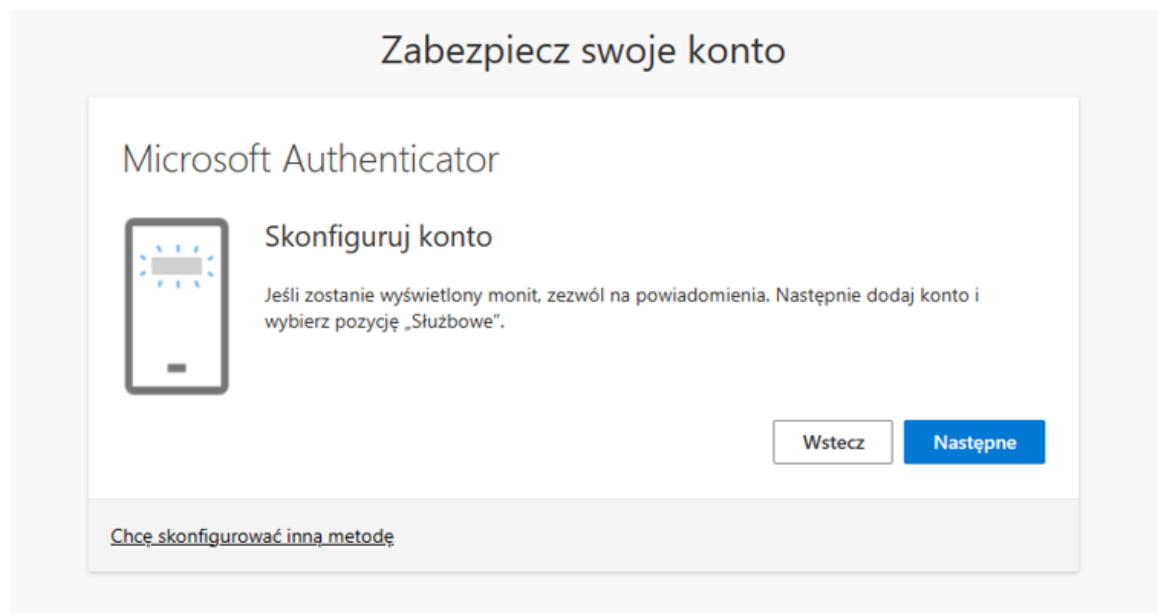
Jeśli pobieranie aplikacji uległo wydłużeniu i okno w przeglądarce pozostawało otwarte przez dłuższy czas zaleca się odświeżenie go lub zamknięcie i ponowną próbę zalogowania na stronie <https://www.office.com/>.

Po pobraniu aplikacji wybieramy w oknie „Zabezpiecz swoje konto” przycisk „Następne”.

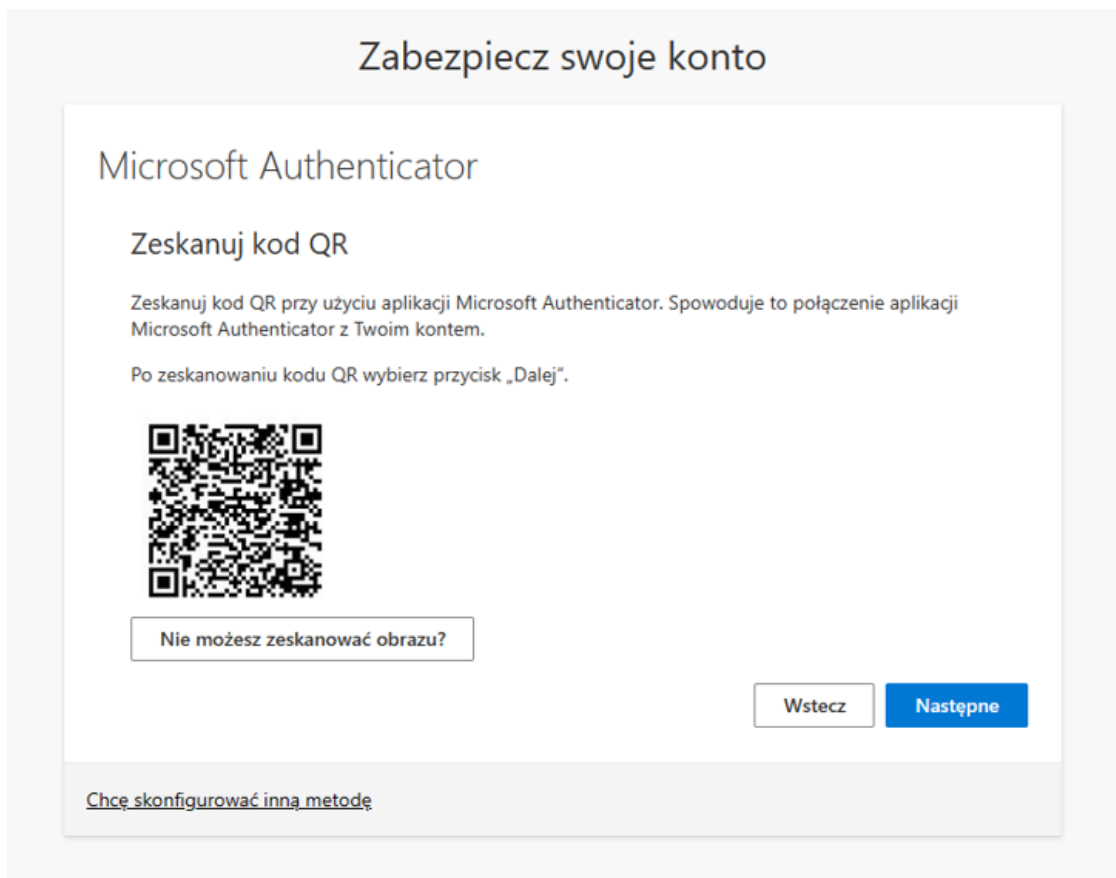


W kolejnym kroku również należy wybrać opcję *Następne*.

Warto również zwrócić uwagę na informację zawartą w komunikacie dotyczącym konfiguracji konta. W przypadku, jeśli w aplikacji na telefonie zostanie wyświetlony monit należy zezwolić na powiadomienia.



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.

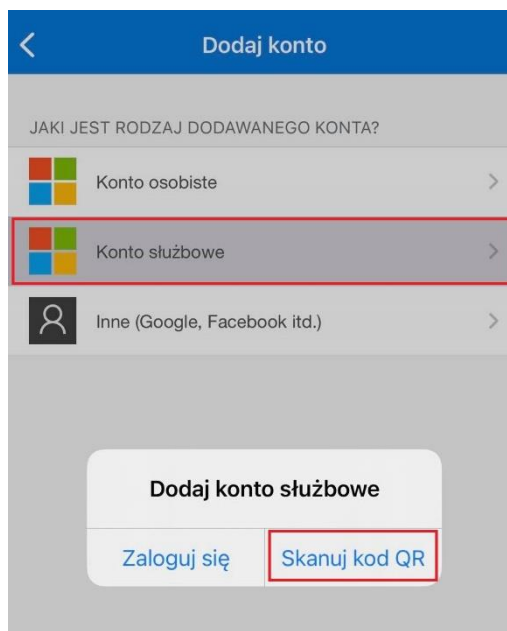
Istnieją dwa możliwe scenariusze wyświetlenia informacji na urządzeniu mobilnym użytkownika.

Wariant 1. Widok dodawania nowego konta

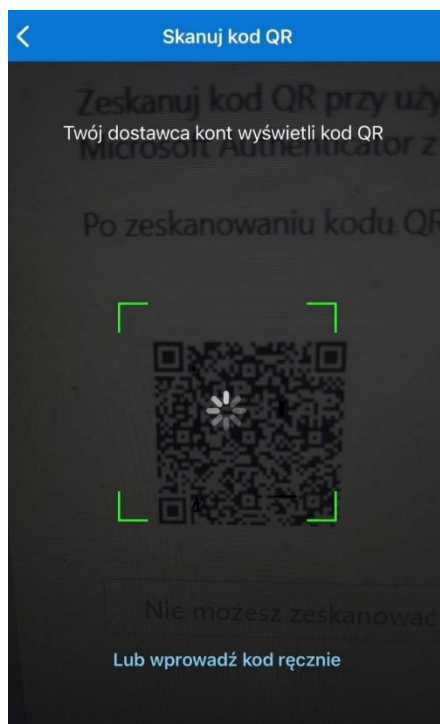
Jeśli wyświetli się poniższy widok należy wybrać *Dodaj konto* lub wybrać ikonę „+”. Jeśli widok ekranu jest inny należy przejść do Wariantu 2 opisanego dalej.



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

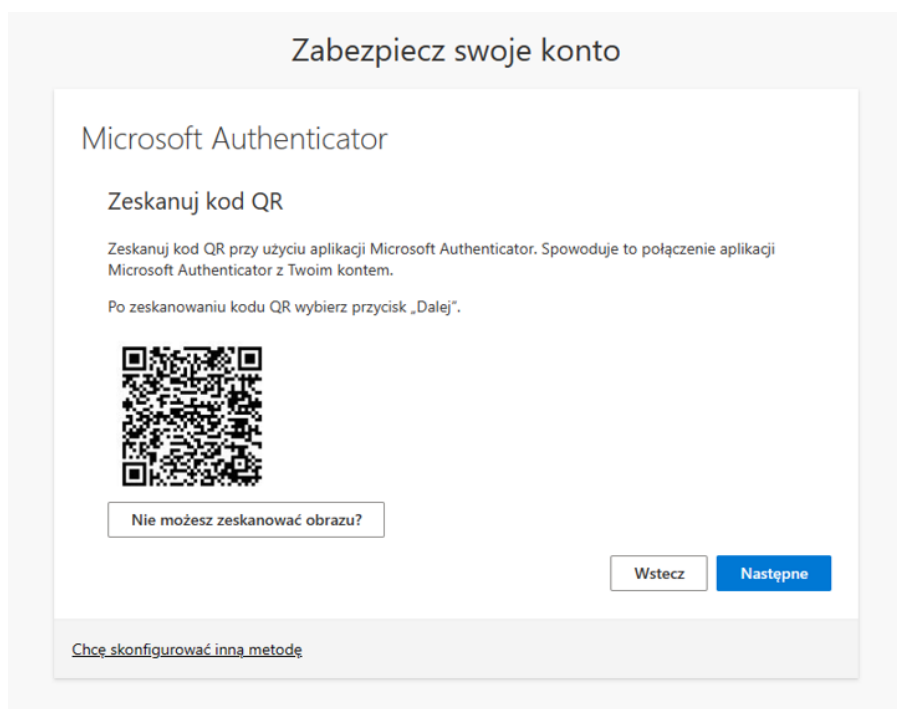


Kod QR należy zeskanować telefonem przy użyciu aplikacji Microsoft Authenticator.



Na urządzeniu pojawić się może 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 okna *Zabezpiecz swoje konto* otwartego uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.



Wyświetlony zostanie dwucyfrowy kod, który należy wprowadzić w aplikacji na telefonie. Po wprowadzeniu kodu w aplikacji należy wybrać opcję Tak, a następnie zatwierdzić w ten sam sposób w jaki odblokowujemy telefon.

Microsoft Authenticator



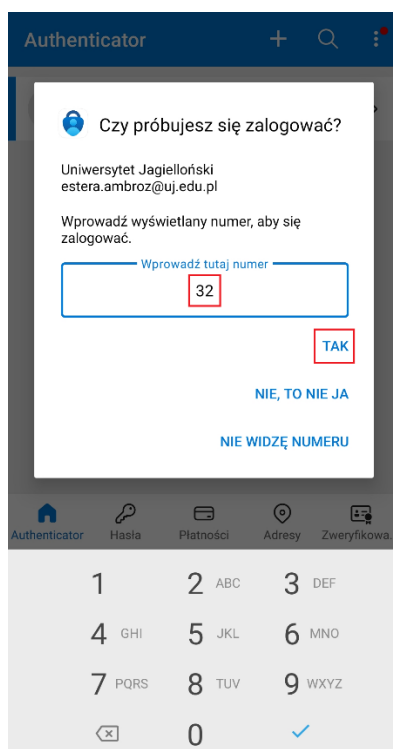
Spróbujmy

Zatwierdź powiadomienie, które wysyłamy do Twojej aplikacji, wprowadzając numer pokazany poniżej.

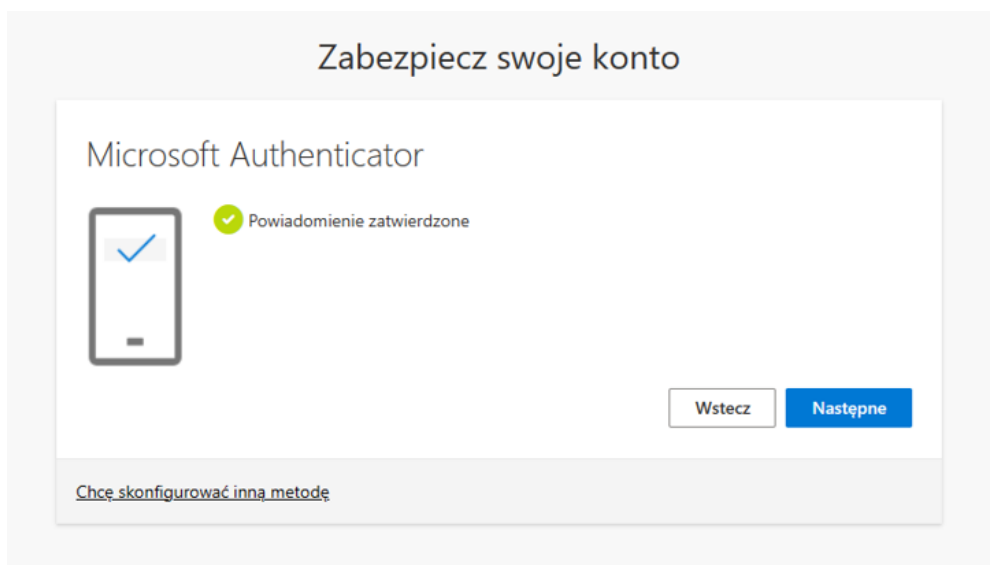
32

Wstecz

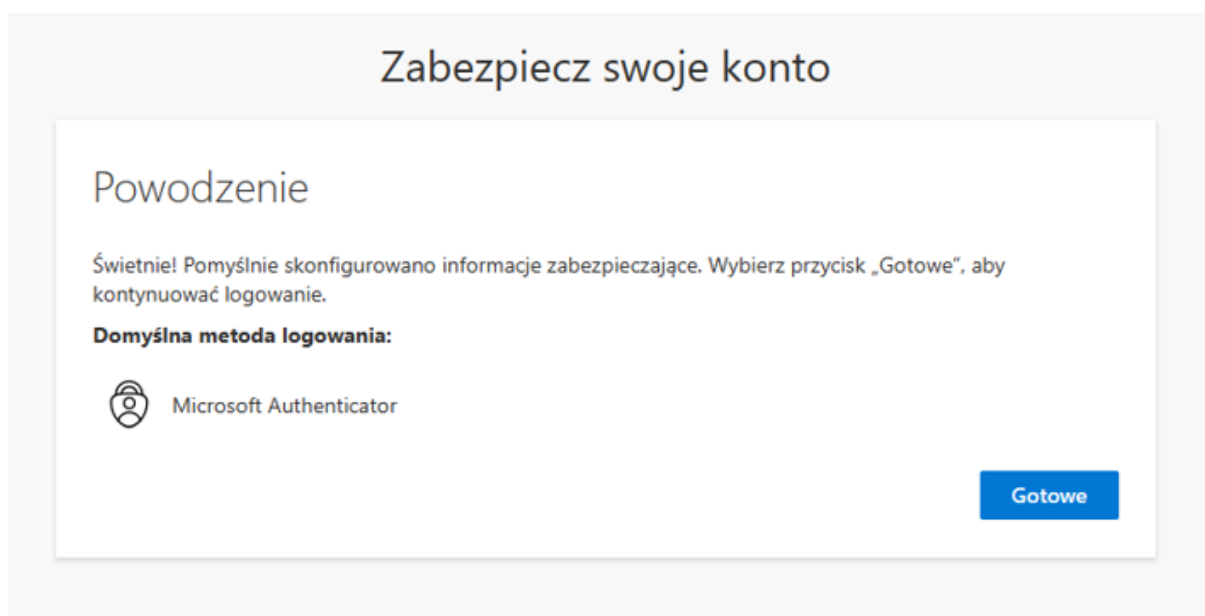
Następne



Jeśli wszystko przebiegnie poprawnie powinniśmy otrzymać komunikat, że powiadomienia zostały zatwierdzone. W tym oknie należy kliknąć przycisk „Następne”.

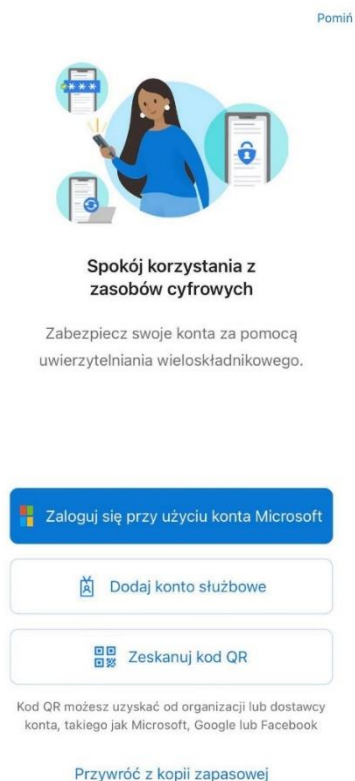


W tym miejscu powinien pojawić się komunikat informację o tym, że udało się pomyślnie dodać metodę logowania do konta. Po wybraniu opcji „Gotowe” procedura dodawania drugiego składnika uwierzytelniania zostanie zakończona.

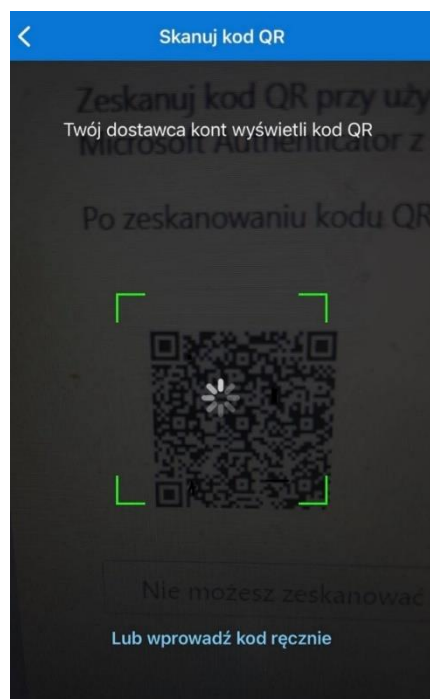


Wariant 2. Widok wyboru akcji

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

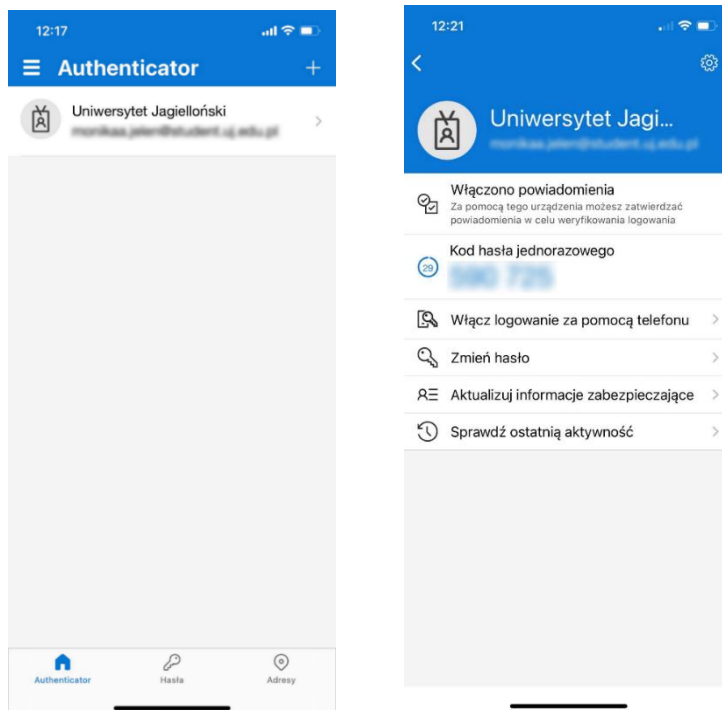


Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.

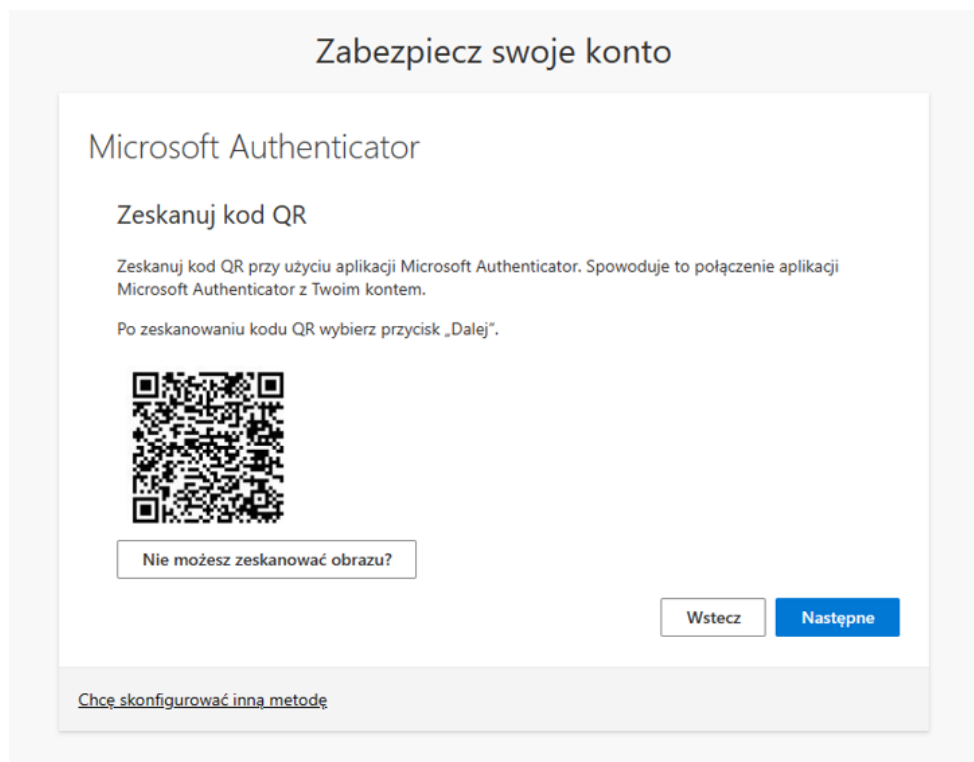


Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień aplikacji.* Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie 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 okna *Zabezpiecz swoje konto* otwartego uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.



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

Microsoft Authenticator



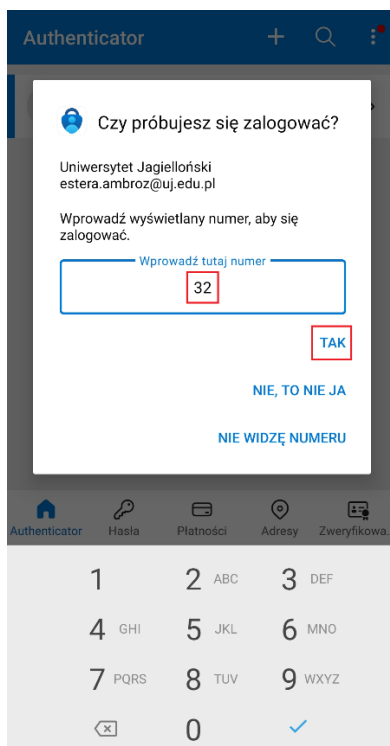
Spróbujmy

Zatwierdź powiadomienie, które wysyłamy do Twojej aplikacji, wprowadzając numer pokazany poniżej.

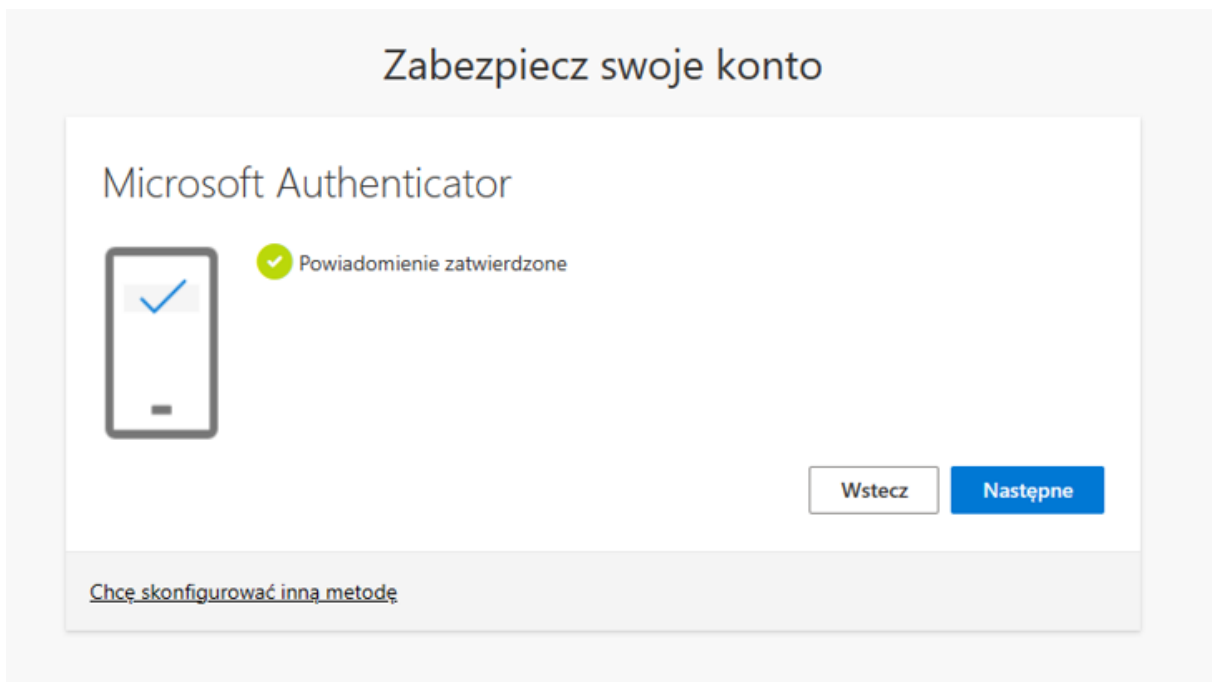
32

Wstecz

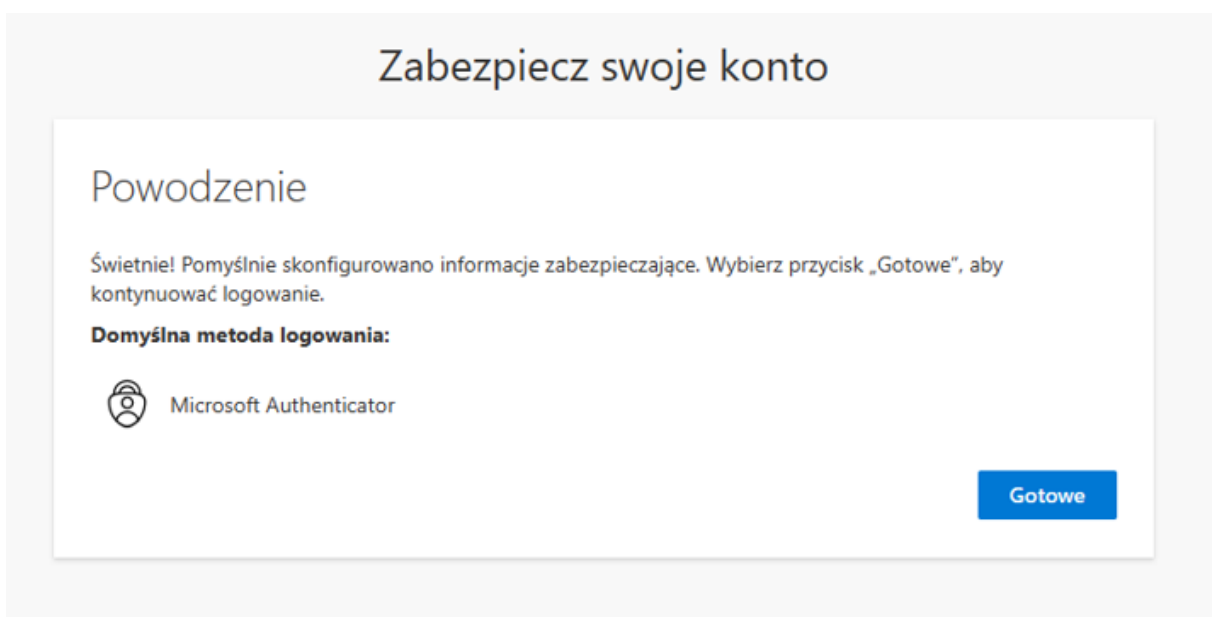
Następne



Jeśli wszystko przebiegnie poprawnie powinniśmy otrzymać komunikat, że powiadomienia zostały zatwierdzone. W tym oknie należy kliknąć przycisk „Następne”.

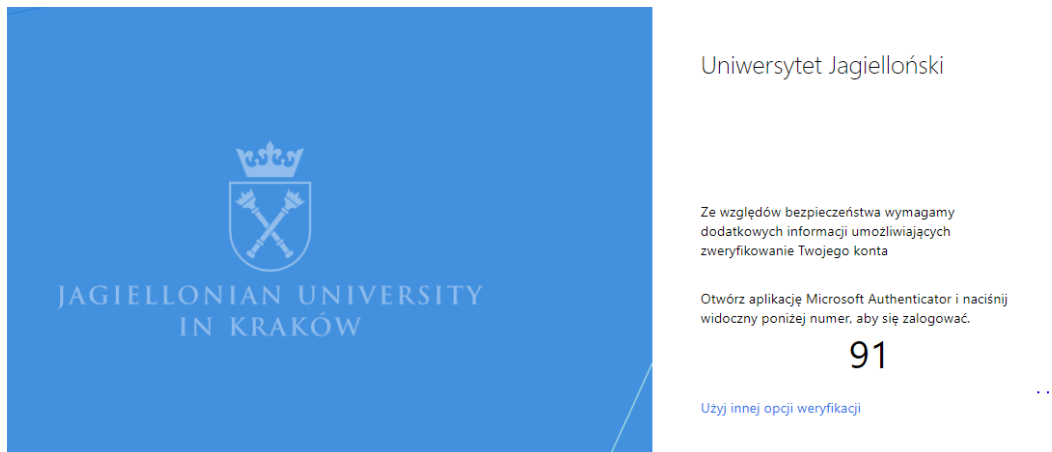


W tym miejscu powinien pojawić się komunikat informację o tym, że udało się pomyślnie dodać metodę logowania do konta. Po wybraniu opcji „Gotowe” procedura dodawania drugiego składnika uwierzytelniania zostanie zakończona.

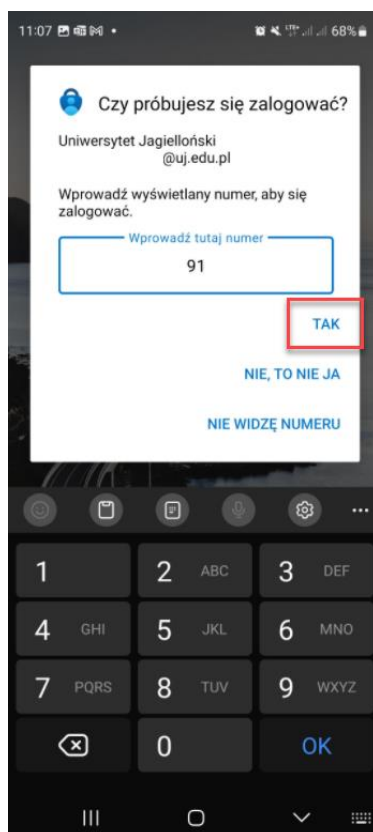


ETAP 4 - LOGOWANIE Z WYKORZYSTANIEM PODWÓJNEGO UWIERZYTELNIANIA

Dla kont objętych logowaniem dwuskładnikowym, poza podaniem identyfikatora logowania i hasła, konieczne jest potwierdzenie logowania w aplikacji MS Authenticator.



Po podaniu prawidłowego loginu i hasła pojawi się ekran prezentujący dwucyfrowy kod numeryczny. Równocześnie na urządzeniu mobilnym z aplikacją MS Authenticator pojawi się powiadomienie z prośbą o zatwierdzenie logowania w aplikacji.



Po wpisaniu kodu identycznego z prezentowanym na ekranie podczas logowania należy kliknąć TAK i potwierdzić logowanie kodem/wzorem ekranu blokady lub odciskiem palca.

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.

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.