

Instrukcja aktywacji aplikacji Microsoft Authenticator v3

Celem aktywacji Microsoft Authenticator na urządzeniu mobilnym jest umożliwienie logowania się do poczty UM, Office 365, Wirtualnej Uczelni, Intranetu oraz Process Portalu z publicznych sieci internetowych (poza siecią UM). W celu aktywacji aplikacji należy wykonać niżej opisane kroki.

Uwaga: opisane poniżej kroki muszą być wykonane na urządzeniu włączonym do sieci internetowej UM, w jednej z poniższych lokalizacji:

- Kampus Hallera – pl. Hallera 1 (z wyłączeniem budynku Dermatologii)
- ul. Żeligowskiego 7/9
- al. Kościuszki 4
- ul. Żeromskiego 113 – USK im. WAM (wszystkie budynki)
- Kampus CKD – Pomorska 251 (wszystkie budynki)
- ul. Kniaziewiczza 1/5 – Szpital im. Biegańskiego (wyłącznie w oddziałach Kardiologii i Dermatologii)
- ul. Urzędnicza 44
- ul. Lindleya 6
- ul. Jaracza 63
- ul. Narutowicza 60
- ul. Muszyńskiego 1 i 2
- osiedle Lumumby - 1 i 2 DS.
- ul. Mazowiecka 6/8
- ul. Sporna 22 – USK im. Marii Konopnickiej (wyłącznie Klinika Pediatrii Onkologii i Hematologii)

Krok 1 Instalacja aplikacji

W celu instalacji aplikacji należy wejść (w zależności od posiadanego urządzenia mobilnego) do Sklepu Play (Android) lub AppStore (iOS) a następnie odnaleźć, pobrać i zainstalować aplikację Microsoft Authenticator.

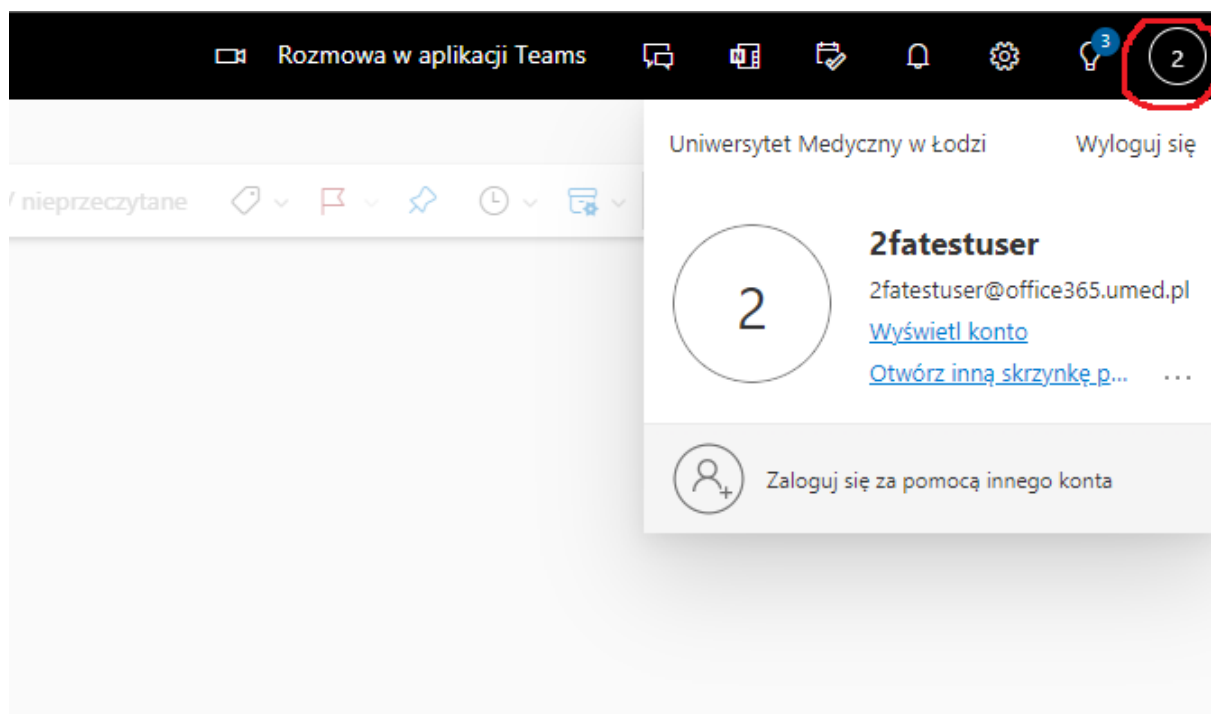


Można również skorzystać z poniższych kodów QR:



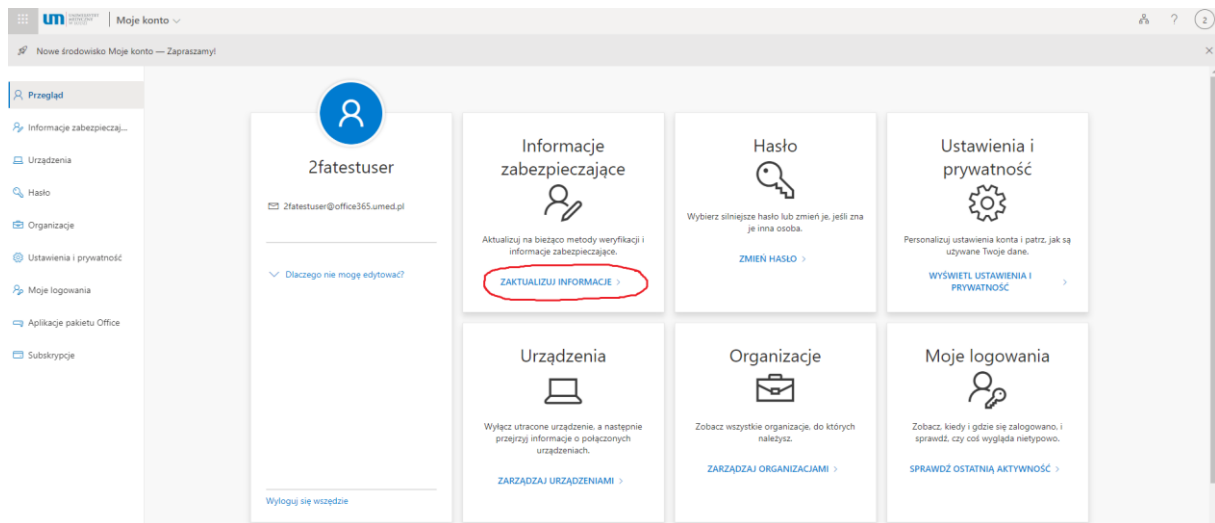
Krok 2a Aktywacja konta UM w aplikacji Microsoft Authenticator – działania na koncie Office365

W celu rozpoczęcia procesu aktywacji konta UM w aplikacji Microsoft Authenticator należy zalogować się do swojej pracowniczej poczty e-mail pod adresem: <https://poczta.umed.lodz.pl>, a następnie kliknąć ikonę konta użytkownika widoczną w prawym, górnym rogu okna przeglądarki:

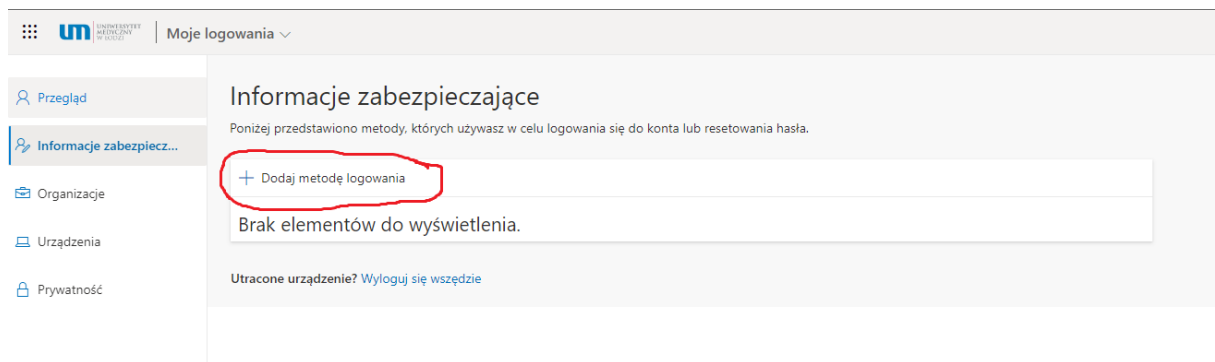


Następnie należy kliknąć „Wyświetl konto” i z poniższego menu kafelkowego wybrać opcję „Zaktualizuj informacje” dostępną na kafelku „Informacje zabezpieczające”

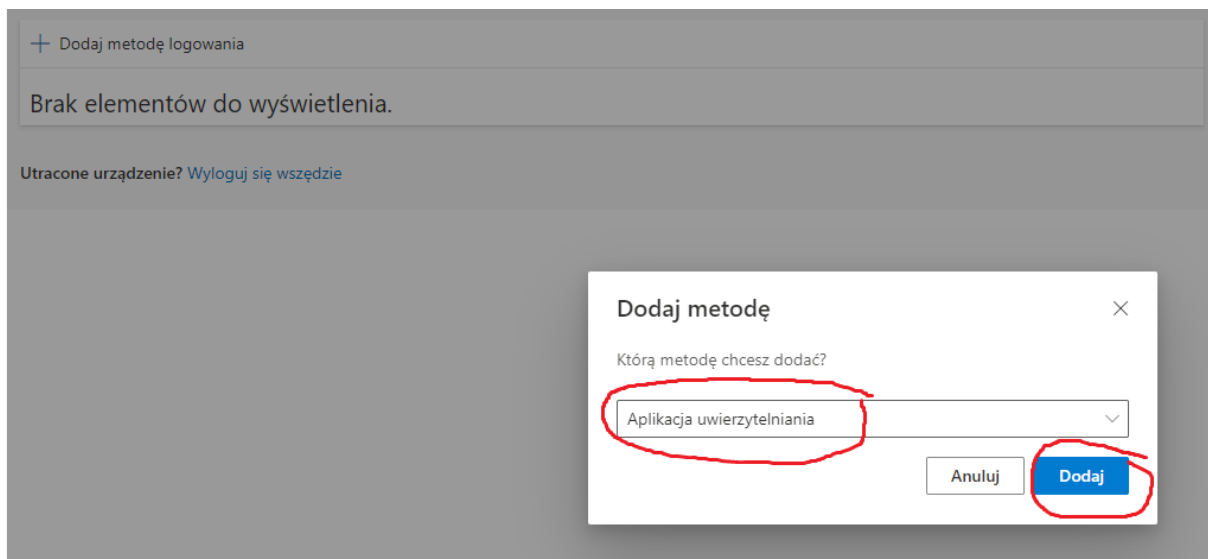
Uwaga: dostęp do wskazanych powyżej ustawień możliwe jest wyłącznie z sieci uczelnianej.



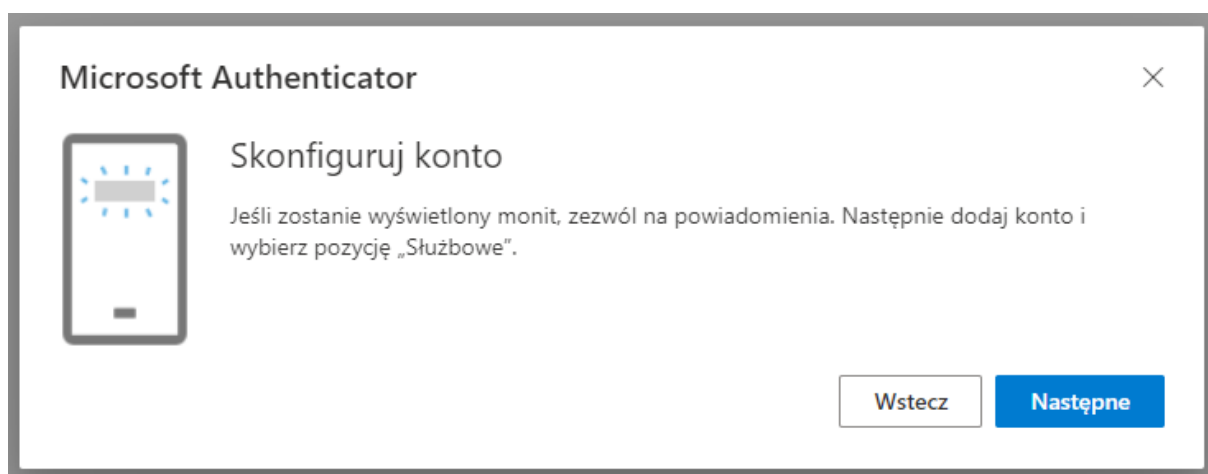
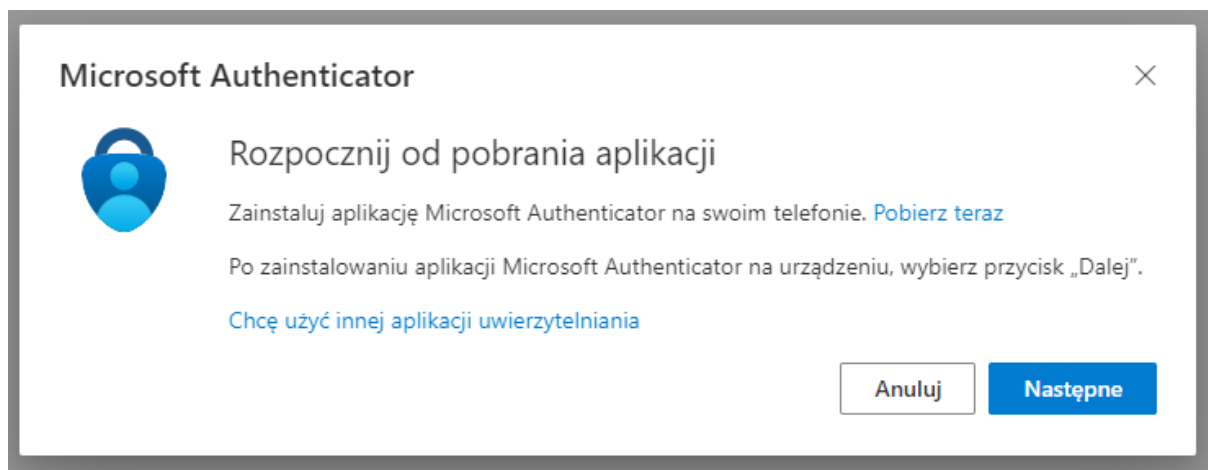
Następnie należy wybrać opcję „dodaj metodę logowania”



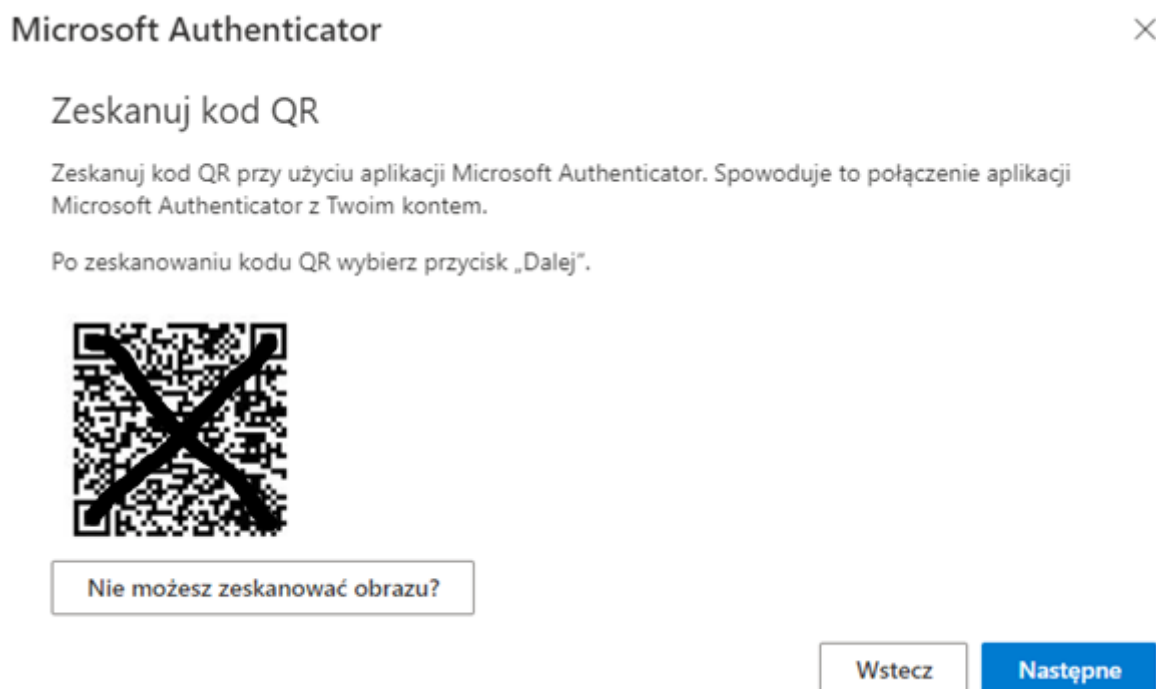
Z dostępnej listy rozwijanej należy wybrać opcję „Aplikacja Uwierzytelniania” i kliknąć „Dodaj”:



W kolejnych krokach pojawią się poniższe okna, na których należy kliknąć przycisk „Następne”:



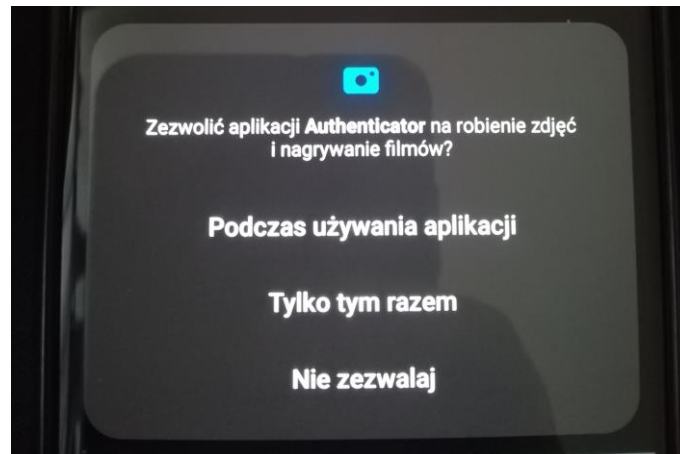
W kolejnym oknie pojawi się kod QR, który należy zeskanować w aplikacji Microsoft Authenticator:



Krok 2b Aktywacja konta UM w aplikacji Microsoft Authenticator – działania w aplikacji

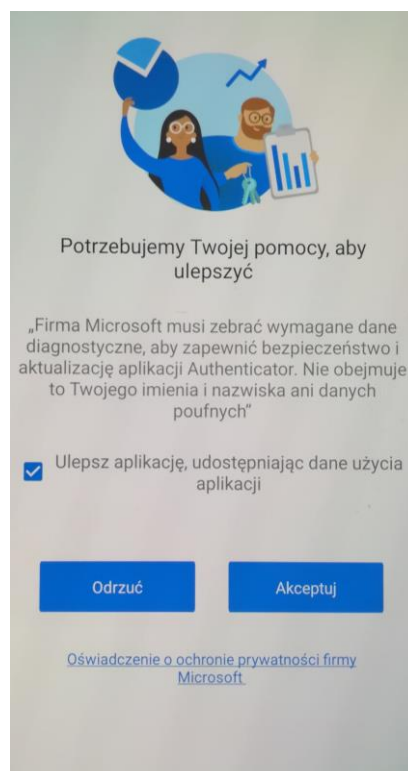
Aby dokończyć proces aktywacji konta UM w aplikacji Microsoft Authenticator należy uruchomić na urządzeniu mobilnym zainstalowaną w kroku 1 aplikację i postępować zgodnie z poniższymi wytycznymi:

Po uruchomieniu aplikacja pojawi się monit o udzielenie zezwolenia aplikacji na robienie zdjęć i nagrywanie filmów. Udzielenie tych uprawnień jest konieczne do zakończenia procesu aktywacji konta UM. Należy wybrać opcję „Podczas używania aplikacji” lub „Tylko tym razem” (uprawnienie ma zostać udzielone jednorazowo):

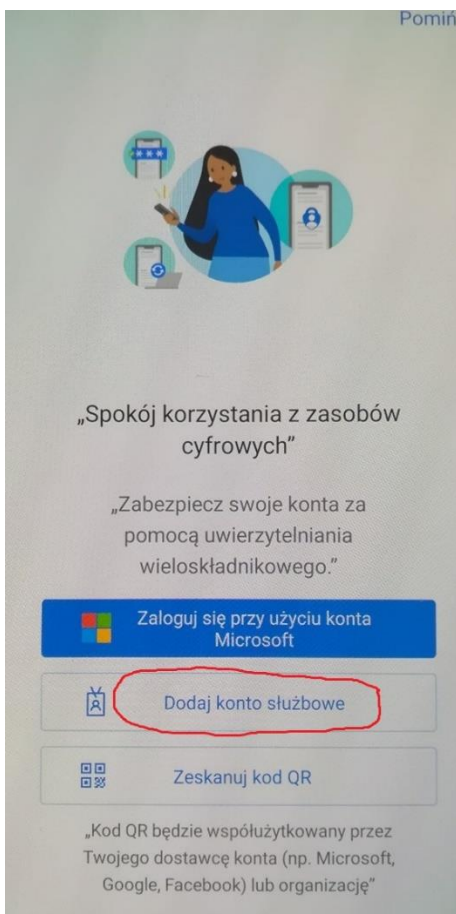


Następnie pojawi się ekran powitalny na którym należy zaakceptować gromadzenie wymaganych danych, poprzez kliknięcie przycisku „Akceptuj”. Opcjonalnie można zaznaczyć checkbox przy polu „Ulepsz aplikację, udostępniając dane użycia aplikacji” (nie jest to konieczne do poprawnego działania aplikacji).

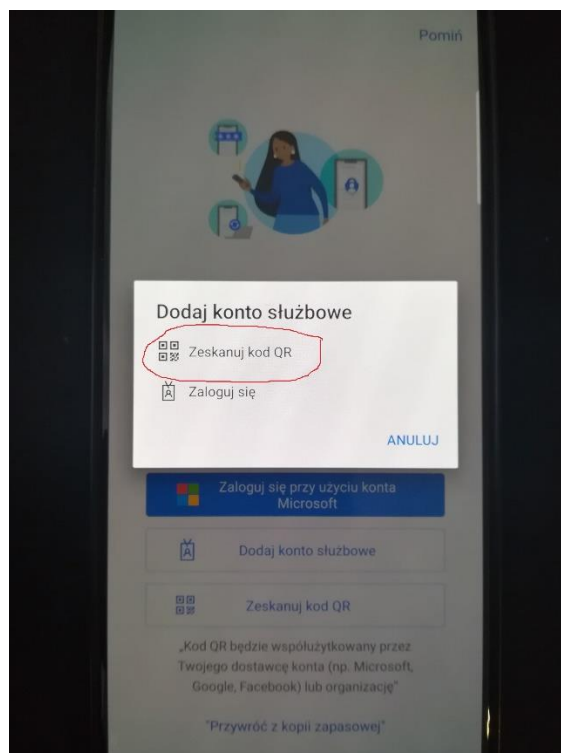
Uwaga: w przypadku kliknięcia opcji „Odrzuć” nie będzie możliwa dalsza konfiguracja aplikacji.



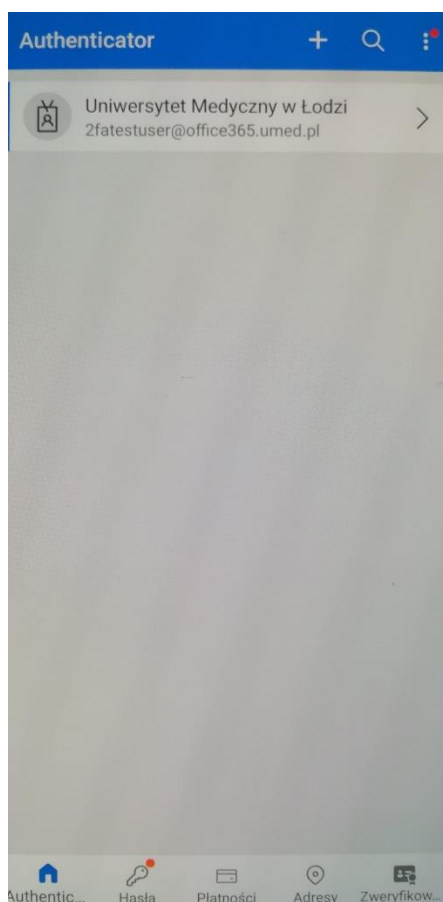
Kolejną czynnością jest wybór rodzaju konta, które ma zostać aktywowane (w tym przypadku należy wybrać opcję „Dodaj konto służbowe”):



Następnie należy wskazać sposób, w jaki będzie aktywowane konto (w tym przypadku, należy wybrać opcję „Zeskanuj kod QR”):



Po poprawnym zeskanowaniu kodu QR i aktywacji aplikacji pojawi się w niej skonfigurowane konto UM:



Następnie należy wrócić do okna przeglądarki w którym wyświetlony był kod QR umożliwiający aktywację konta w aplikacji i kliknąć przycisk „Następne”:

Microsoft Authenticator



Zeskanuj kod QR

Zeskanuj kod QR przy użyciu aplikacji Microsoft Authenticator. Spowoduje to połączenie aplikacji Microsoft Authenticator z Twoim kontem.

Po zeskanowaniu kodu QR wybierz przycisk „Dalej”.



Nie możesz zeskanować obrazu?

Wstecz

Następne

W oknie przeglądarki pojawi się poniższy komunikat zawierający dwucyfrową liczbę, którą należy wprowadzić w oknie aplikacji Microsoft Authenticator w celu potwierdzenia rejestracji aplikacji:

Microsoft Authenticator



Spróbujmy

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

43

Wstecz

Następne

Po zatwierdzeniu dostępu w aplikacji Microsoft Authenticator, w oknie przeglądarki pojawi się poniższy komunikat, w którym należy wybrać opcję „Następne”:

Microsoft Authenticator

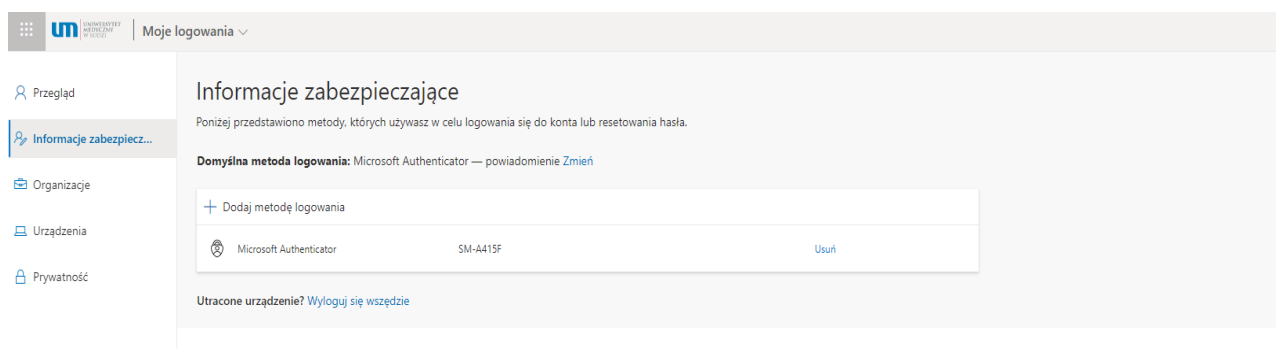


✓ Powiadomienie zatwierdzone

Wstecz

Następne

Po poprawnej konfiguracji konta UM w aplikacji Microsoft Authenticator pojawi się ostatnie okno informujące o poprawnej konfiguracji domyślnej metody logowania:




Po włączeniu przez zespół IT UM mechanizmu podwójnego uwierzytelnienia (zgodnie z datą podaną w komunikacie informującym o terminie jego włączenia), każdorazowe logowanie się do usług publicznych UM takich jak poczta UM, Office 365, Wirtualna Uczelnia, Intranet oraz Process Portal z publicznych sieci internetowych (poza siecią UM), będzie wymagało zatwierdzenia logowania w aplikacji Microsoft Authenticator (komunikat PUSH w aplikacji).

Logowanie się do systemu informatycznego z wykorzystaniem aplikacji Microsoft Authenticator:

Po poprawnym dodaniu metody dwuskładnikowego uwierzytelnienia w oparciu o aplikację Microsoft Authenticator, w celu zalogowania się do systemu IT spoza sieci uczelnianej konieczne będzie zatwierdzenie logowania w aplikacji Microsoft Authenticator. Proces zatwierdzenia jest dwukrokowy, w pierwszym kroku po podaniu loginu i hasła w przeglądarce pojawi się poniższy komunikat, zawierający liczbę dwucyfrową:

Zatwierdzenie żądania logowania

-  Otwórz aplikację Authenticator i wprowadź wyświetlany numer, aby się zalogować.

11

Brak numerów w Twojej aplikacji? Uaktualnij ją do najnowszej wersji.

[Nie mogę użyć teraz aplikacji Microsoft Authenticator](#)

[Więcej informacji](#)

W drugim kroku, należy zatwierdzić komunikat PUSH w aplikacji Microsoft Authenticator podając dwucyfrowa liczbę, która wyświetla się na ekranie przeglądarki:

 Czy próbujesz się zalogować?

Uniwersytet Medyczny w Łodzi
@office365.umed.pl

Aplikacja
Office 365 Exchange Online

Lokalizacja
Wielkopolskie, Polska



Wprowadź wyświetlany numer, aby się zalogować.

Wprowadź tutaj numer

TAK

NIE, TO NIE JA

NIE WIDZĘ NUMERU

Wskazana w aplikacji lokalizacja jest pobierana na podstawie łącza internetowego z którego aktualnie korzysta użytkownik i ma charakter orientacyjny. Może się zdarzyć, że będąc np. w Łodzi wyświetli się lokalizacja np. Warszawa. Wynika to najczęściej z tego, gdzie zarejestrowaną ma siedzibę operator Państwa usługi internetowej. Ważne jest aby zwrócić uwagę, czy wyświetlana lokalizacja nie pochodzi spoza granic kraju w którym aktualnie przebywa użytkownik np. z Chin, Rosji itp. W takim przypadku należy bezwzględnie anulować taką prośbę o autoryzację.

Uwaga: jeśli pojawi się w Państwa aplikacji Microsoft Authenticator komunikat PUSH informujący o konieczności zatwierdzenia logowania, ale to nie Państwo zainicjowali proces logowania lub prośba o autoryzację pochodzi z innego kraju niż aktualnie Państwo przebywacie, należy odrzucić taką prośbę i niezwłocznie poinformować Centrum Informatyczno – Telekomunikacyjne o takim zdarzeniu podając jego datę i godzinę oraz nazwę konta, którego sytuacja ta dotyczy. W żadnym wypadku nie należy zatwierdzać takiej prośby, ponieważ może to być próba przejęcia Państwa konta.

Uwaga: Aby ponownie aktywować aplikację Microsoft Authenticator (np. w przypadku zagubienia, wymiany lub przywrócenia ustawień fabrycznych telefonu) należy skontaktować się z operatorem CIT pod numerem telefonu.: 42 272 5003 lub mailowo na adres cit@umed.lodz.pl w celu umożliwienia ponownej aktywacji aplikacji (konieczne jest usunięcie dotychczasowego urządzenia z listy urządzeń służących do autoryzacji). Po wykonaniu tej operacji, należy przystąpić do ponownej aktywacji aplikacji zgodnie z niniejszą instrukcją.

W przypadku problemów z konfiguracją aplikacji, prosimy o kontakt z zespołem IT pod adresem: cit@umed.lodz.pl lub telefonicznie pod numerami: 042 272 5369 lub 5012 lub 5013.