Urząd Miasta Stołecznego Warszawy
Biuro Informatyki
pl. Bankowy 2, 00-095 Warszawa, tel. 22 325 90 00
adres do korespondencji: Aleje Jerozolimskie 44, 00-024 Warszawa
Sekretariat.it@um.warszawa.pl, um.warszawa.pl

INSTRUKCJA KONFIGURACJI UWIERZYTELNIENIA WIELOSKŁADNIKOWEGO (MFA)

Warszawa, 2023

Metryka dokumentu

Cel dokumentu

Instrukcja przedstawia sposób ustawienia potwierdzenia logowania, tzw. uwierzytelniania wieloskładnikowego (MFA – MultiFactor Authentication).
Logowanie do usług Microsoft 365 wymaga obecnie uwierzytelnienia wieloskładnikowego. Polega ono na tym, że oprócz podania hasła do konta wymagane jest dodatkowe potwierdzenie logowania. Możesz je wykonać odbierając połączenie telefoniczne lub zatwierdzając w aplikacji mobilnej. W instrukcji znajdziesz metodę konfiguracji obu metod.

Adresaci dokumentu

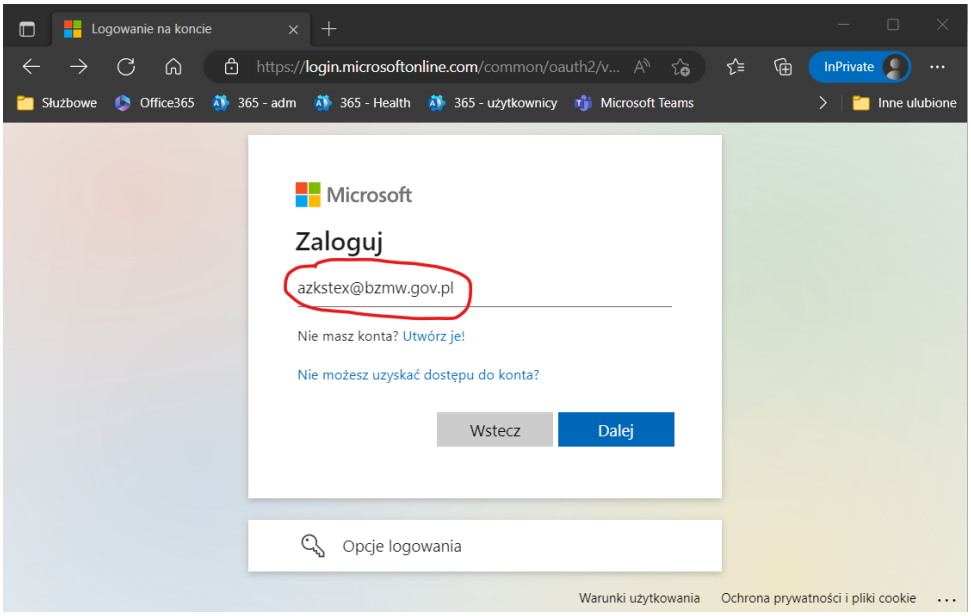
Dokument został przygotowany dla pracowników Urzędu m.st. Warszawy, pracowników Urzędów Dzielnic, pracowników zintegrowanych jednostek organizacyjnych m.st. Warszawy, w dalszej części instrukcji określanych jako pracownicy.

Potwierdzanie logowania

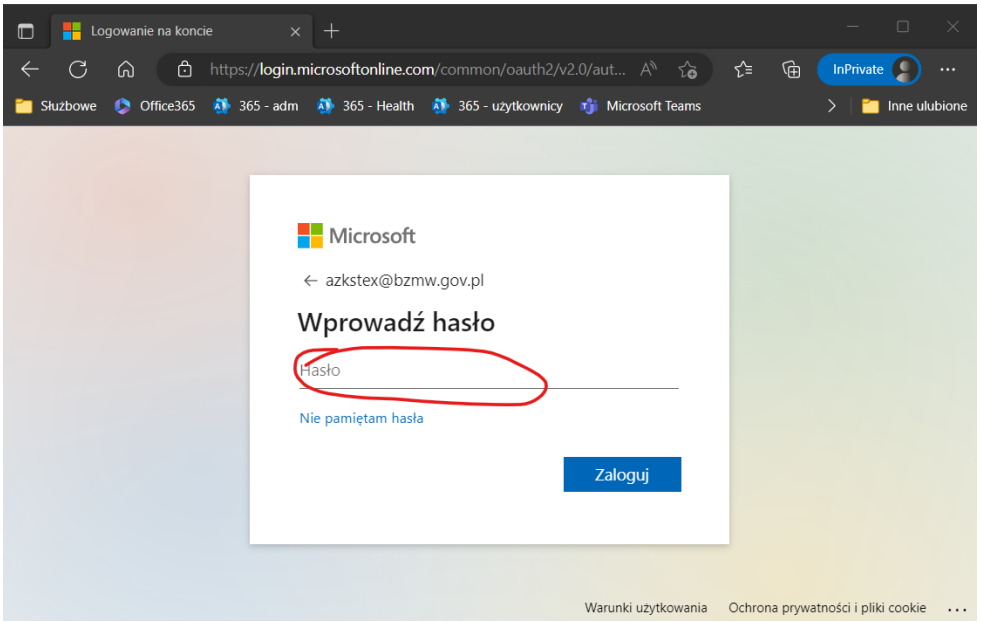
Potwierdzanie przez połączenie telefoniczne

Uwaga! Podczas logowania do przesłanego przez nas loginu dopisz **@bzmw.gov.pl**

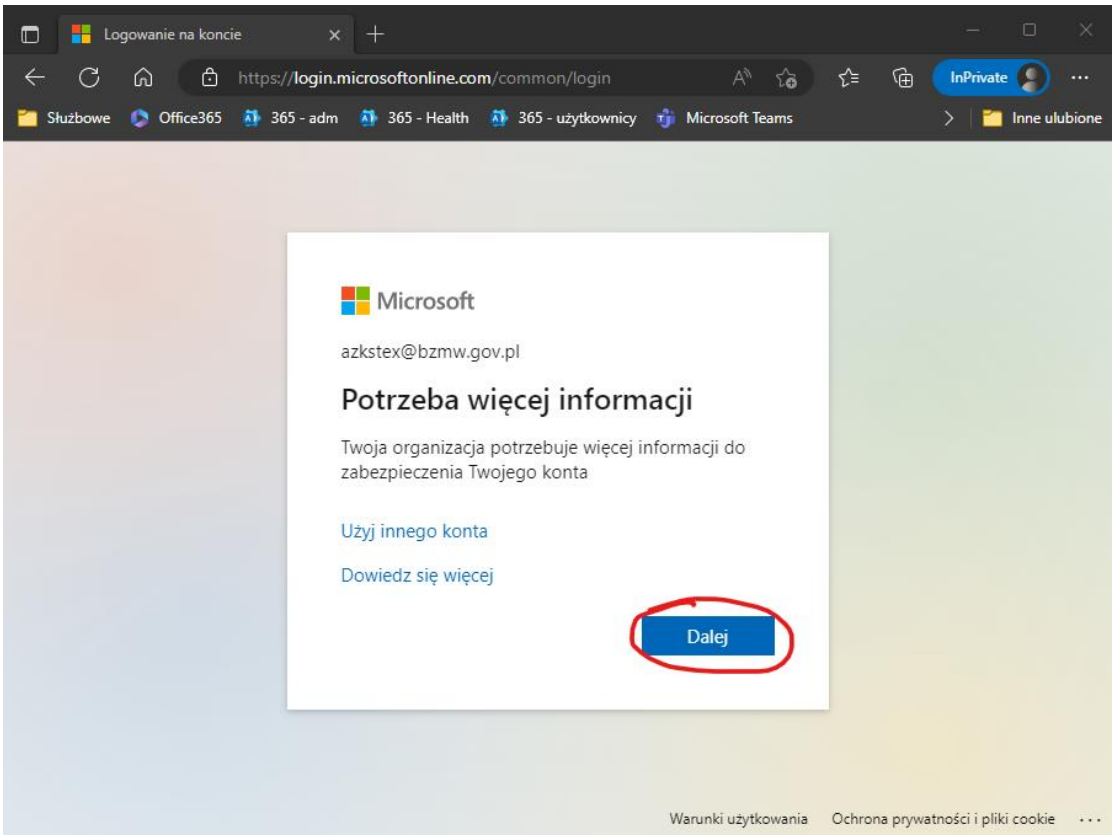
login@bzmw.gov.pl



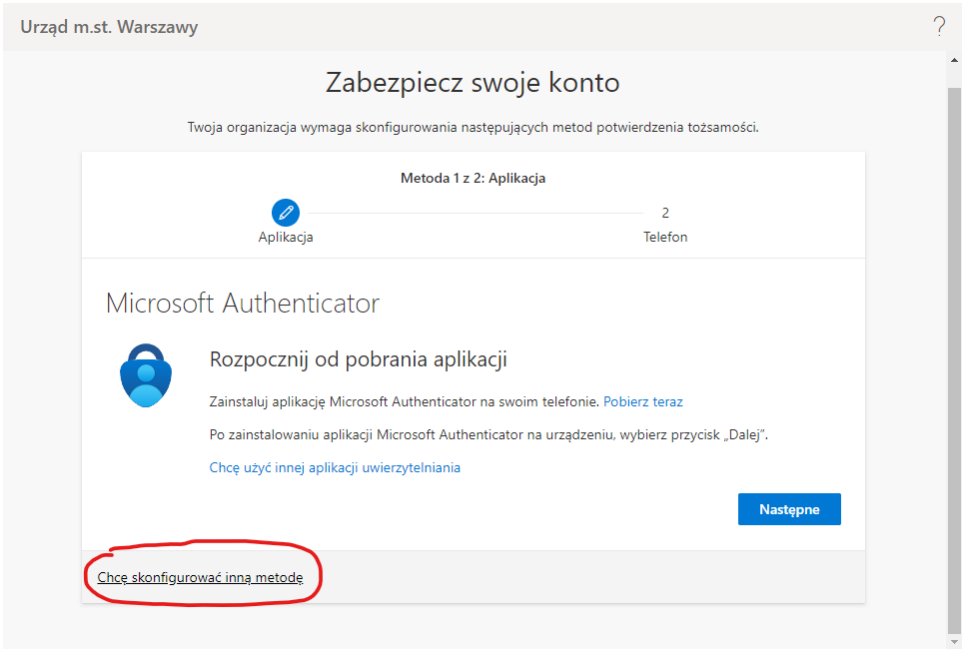
W kolejnym oknie podaj hasło:



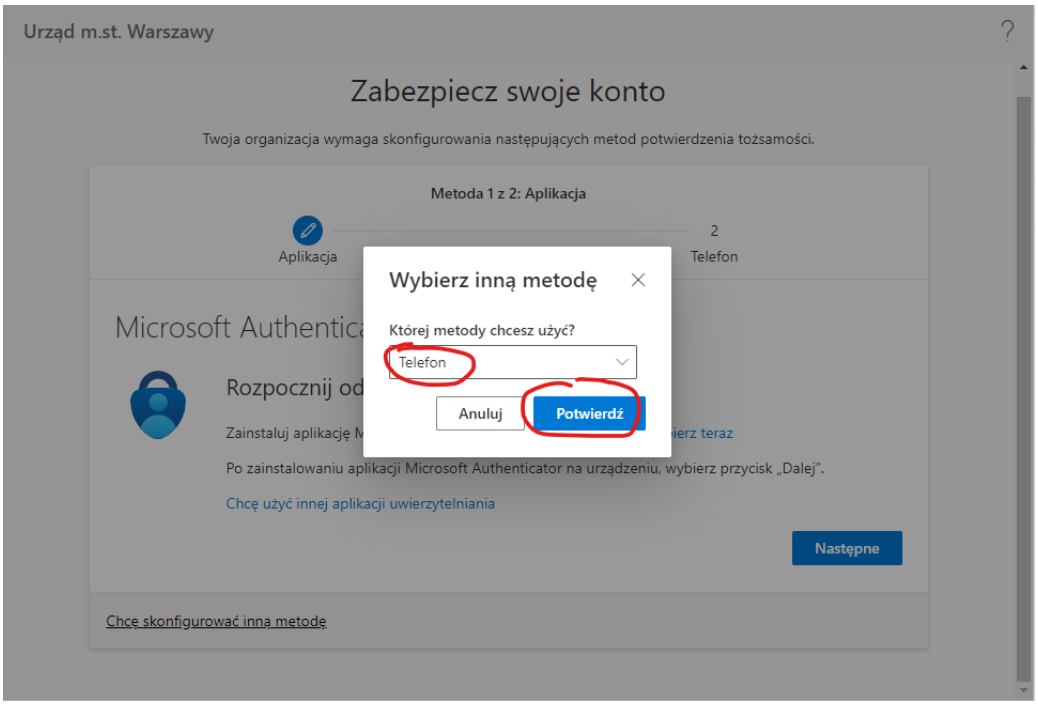
Jeśli pierwszy raz ustawiasz numer telefonu do potwierdzenia logowania, po podaniu hasła pojawi się ekran Potrzeba więcej informacji. Kliknij klawisz Dalej:



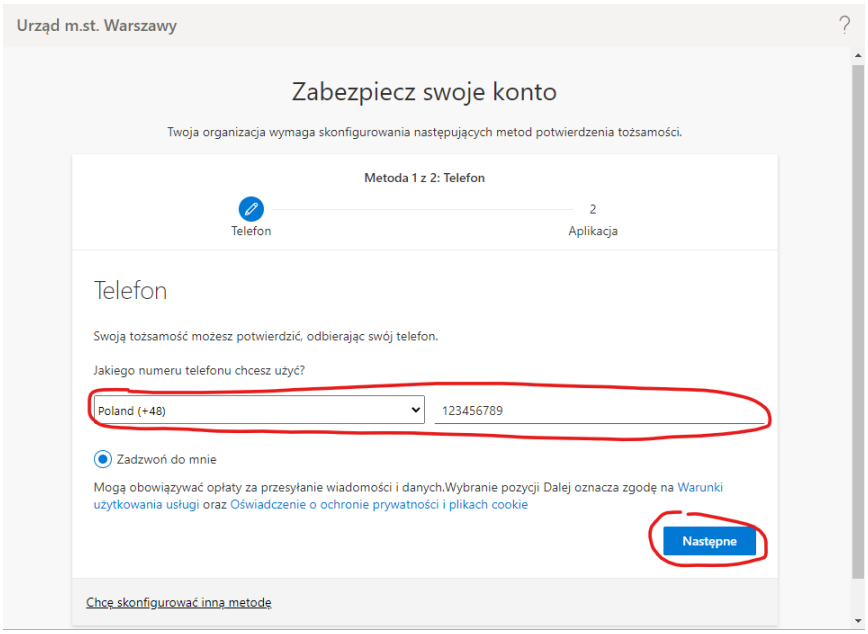
W kolejnym kroku pojawi się okno do konfiguracji dodatkowego zabezpieczenia. Domyślnie program zasugeruje skorzystanie z aplikacji Microsoft Authenticator. Aby ustawić telefoniczne potwierdzanie logowania wybierz polecenie: Chcę skonfigurować inną metodę:



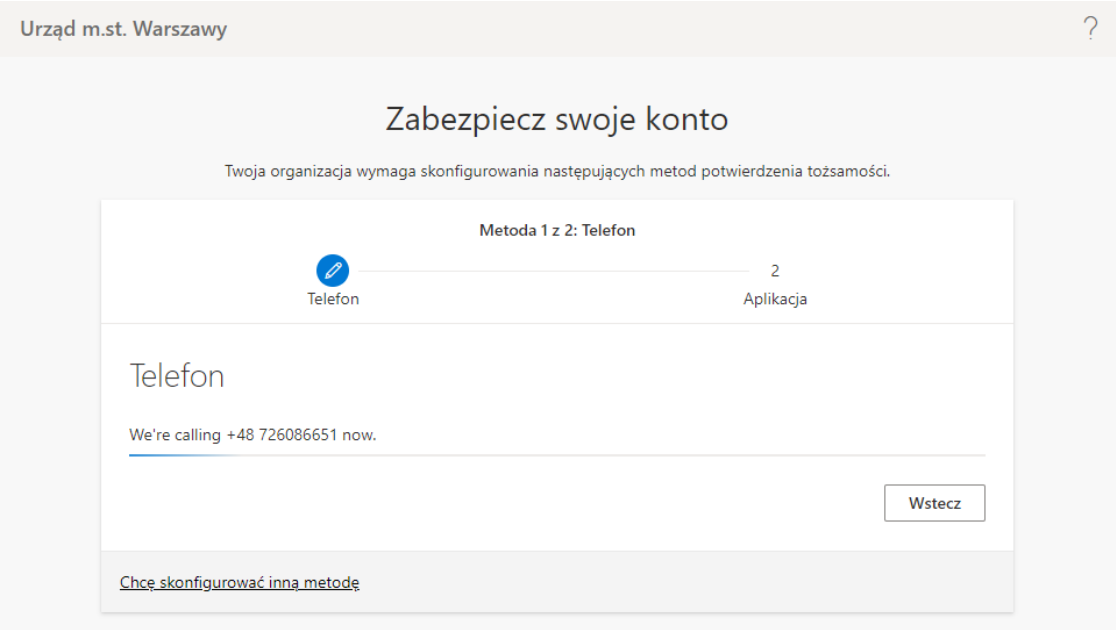
W okienku Wybierz inną metodę rozwiń listę i wybierz pozycję Telefon. Następnie zatwierdź przyciskiem Potwierdź:



Następnie wybierz kraj, w którym się logujesz: Poland (+48) i podaj numer swojego telefonu np. komórkowego. Wprowadź tylko cyfry, bez znaku „+". Jeśli podajesz numer komórki wprowadź 9 cyfr. Jeśli korzystasz z numeru stacjonarnego (nie zalecamy) podaj numer telefonu wraz z numerem kierunkowym do Warszawy (np. 22 1234567). Na ten numer będzie dzwonił automat potwierdzający logowanie. Zatwierdź wprowadzone dane klawiszem Następne:

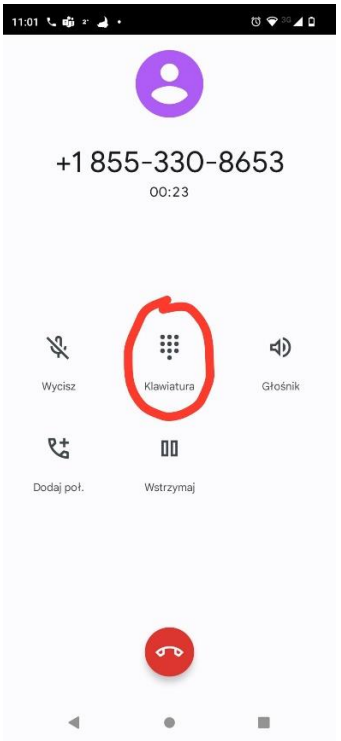


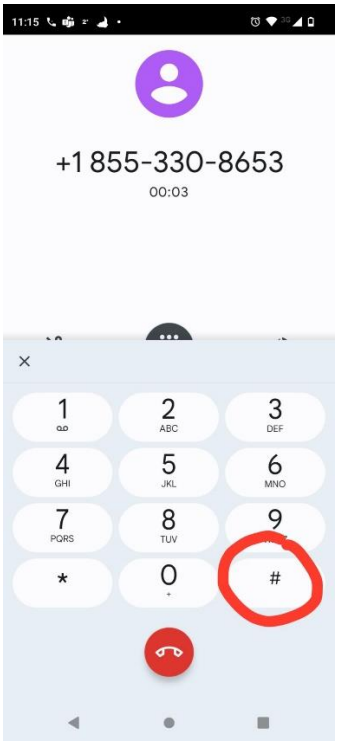
Teraz automat z Microsoft zadzwoni do Ciebie z numeru rozpoczynającego się od +1855… Na komputerze pojawi się informacja o tym, że połączenie jest właśnie wykonywane.



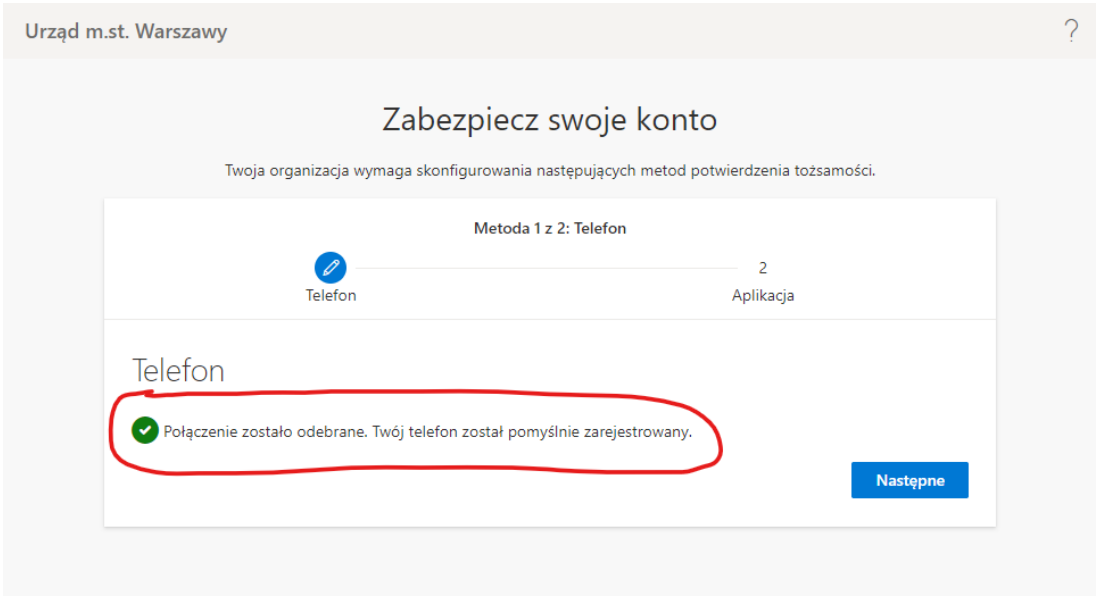
!Pamiętaj! Żeby potwierdzenie logowania się powiodło, **linia telefoniczna musi być wolna**. Jeśli telefon będzie zajęty Microsoft podejmie jeszcze dwie próby zadzwonienia. Jeśli się to nie uda, proces logowania będzie trzeba zacząć od początku!

Odbierz telefon. Automat poinformuje Cię (po polsku) o tym, że próbujesz się zalogować. Aby zatwierdzić logowanie **naciśnij przycisk # na klawiaturze telefonu**. Jeśli korzystasz z telefonu komórkowego, aby to zrobić, kliknij w czasie rozmowy na klawisz oznaczający klawiaturę na ekranie telefonu. Następnie kliknij na klawisz #:

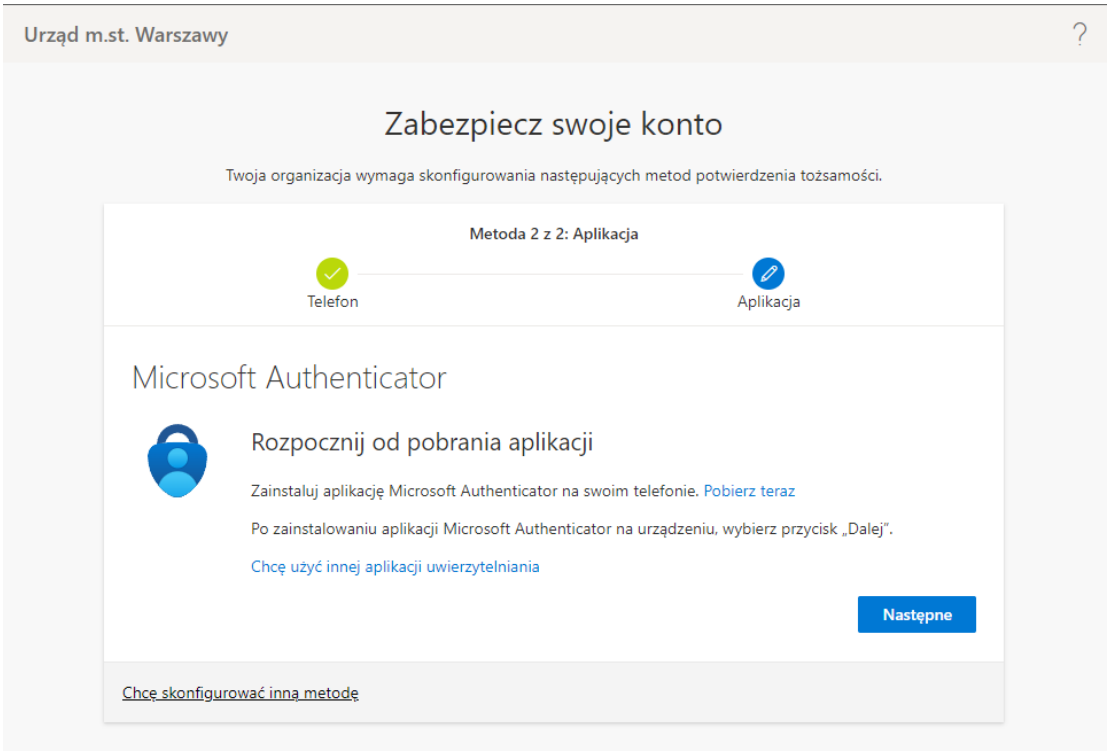




Twoje logowanie zostało potwierdzone a twój numer telefonu został właśnie dodany do uwierzytelnienia wieloskładnikowego. Aby zakończyć proces ustawienia uwierzytelniania kliknij przycisk Następne:



W kolejnym oknie pojawi się sugestia aby ustawić również potwierdzanie logowania przez aplikację mobilną. Zalecamy aby to zrobić. Jeśli chcesz to zrobić, kliknij przycisk Następne:



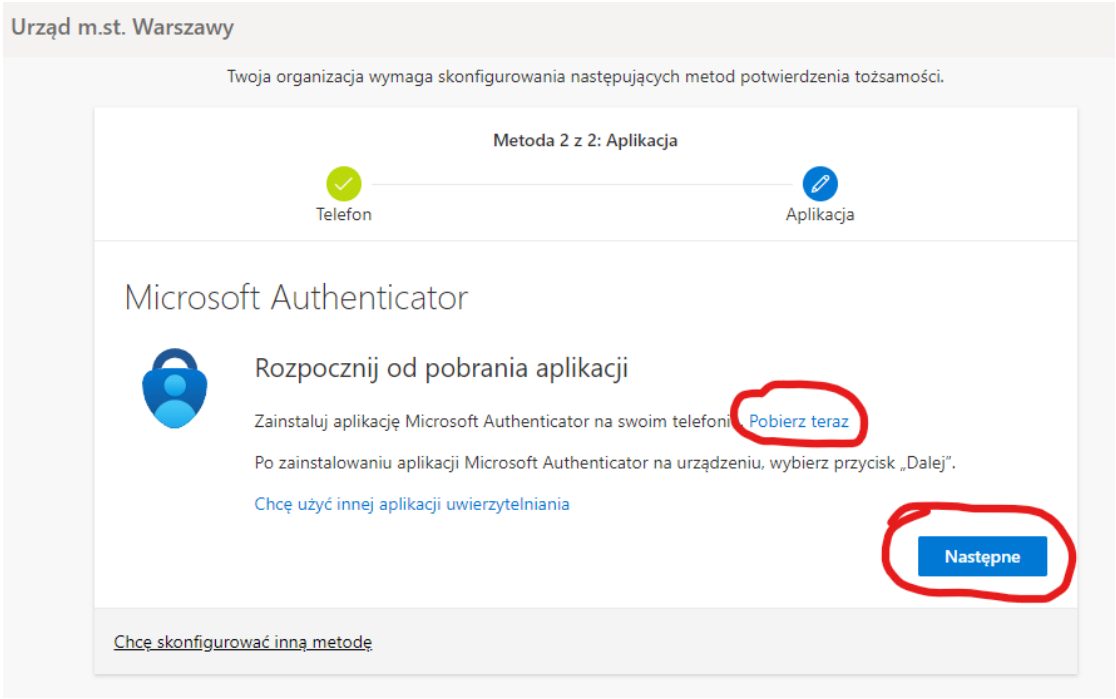
Potwierdzanie aplikacją mobilną

W poprzednim kroku system poprosił o pobranie aplikacji. Możesz ją pobrać klikając na polecenie Pobierz teraz.

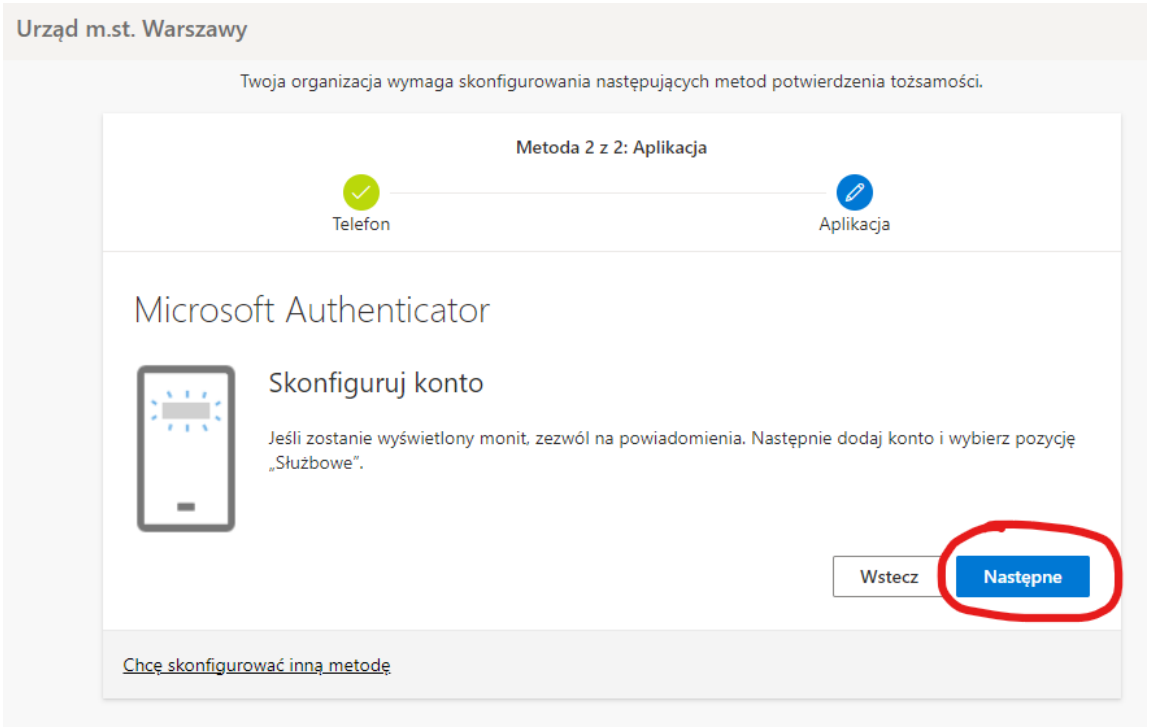
Kliknięcie w to polecenie przeniesie Cię na stronę Microsoft na której będą dostępne kody QR dla odpowiedniej wersji systemu urządzenia, na którym chcesz zainstalować aplikację. Możesz zeskanować kod QR urządzeniem lub na urządzeniu otworzyć sklep i zainstalować aplikację ze sklepu.

Na telefonach służbowych Urzędu Miasta aplikacja Microsoft Authenticator jest już zainstalowana.

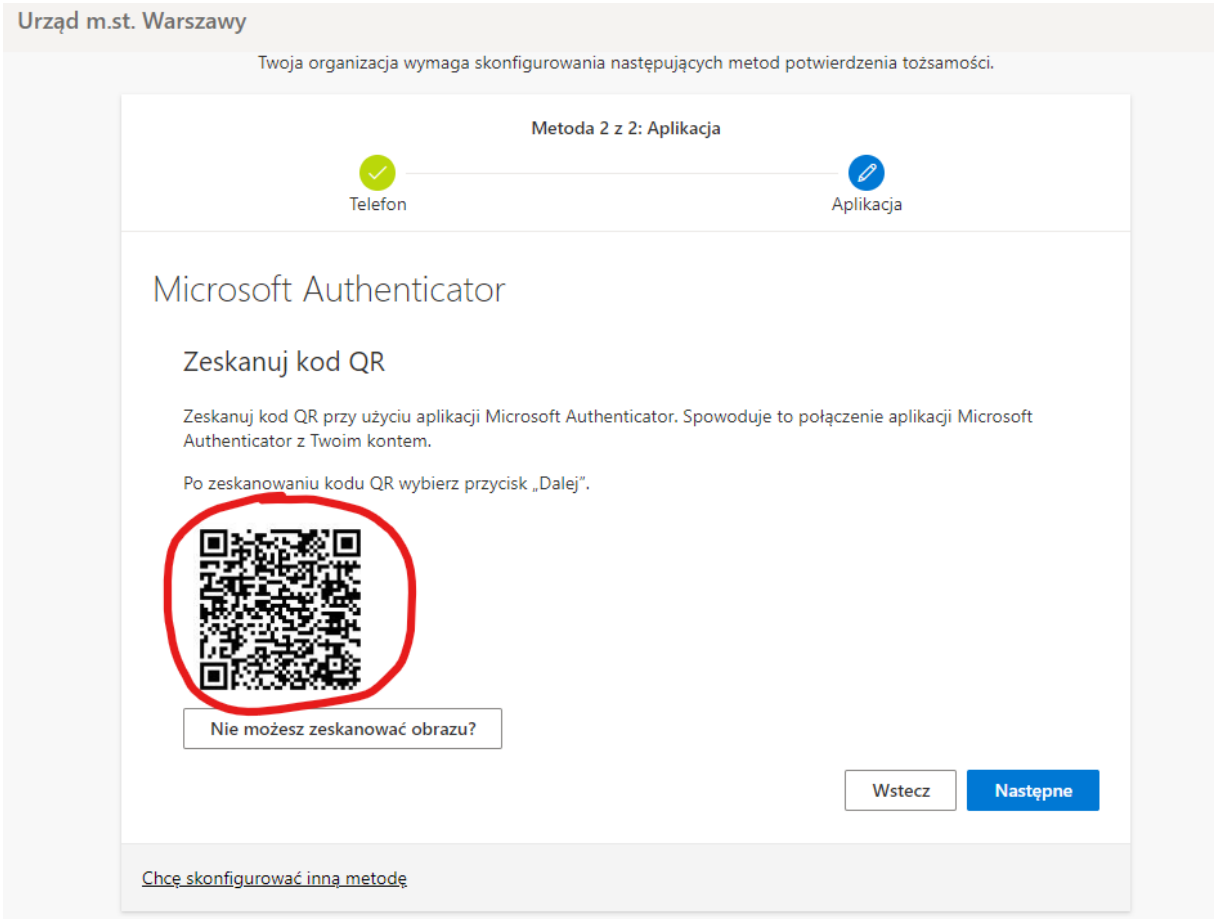
Po zainstalowaniu aplikacji kliknij polecenie Następne:



Teraz pojawi się okno Skonfiguruj konto. Postępuj z komunikatami wyświetlanymi na stronie. Potem kliknij w przycisk Następne:

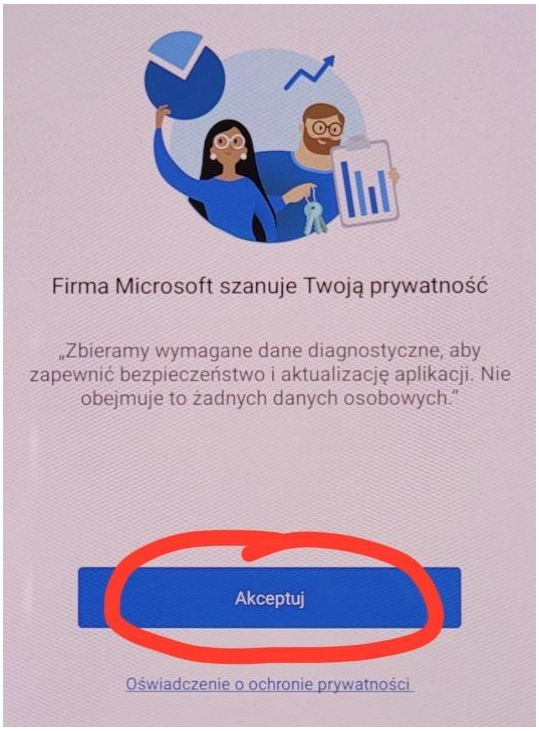


Pojawi się kolejne okno z kodem QR do zeskanowania urządzeniem przenośnym na którym konfigurujesz aplikację do uwierzytelniania logowania (kod ważny jest przez około 30 sekund, potem proces trzeba będzie przejść od nowa):

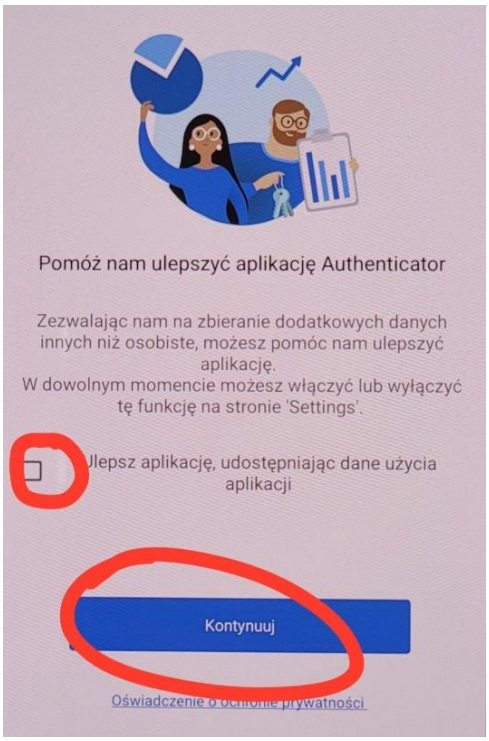


Uruchom na urządzeniu przenośnym (telefon/tablet) aplikację Microsoft Authenticator. Poszukaj wśród ikonek na ekranie telefonu lub tabletu następującej ikonki:

Po uruchomieniu aplikacji pojawi się ekran dotyczący prywatności. Zapoznaj się z zasadami ochrony prywatności i zaakceptuj je przyciskiem Akceptuj:



W kolejnym kroku aplikacja poprosi Cię o zgodę na zbieranie danych na temat korzystania z aplikacji (bez danych osobistych). Ma to na celu stałe ulepszanie aplikacji przez producenta. Ta zgoda nie jest jednak wymagana, więc nie musisz jej zaznaczać. Wybór należy do Ciebie. Bez względu na to czy zaznaczysz zgodę czy nie aby przejść dalej kliknij przycisk Kontynuuj:

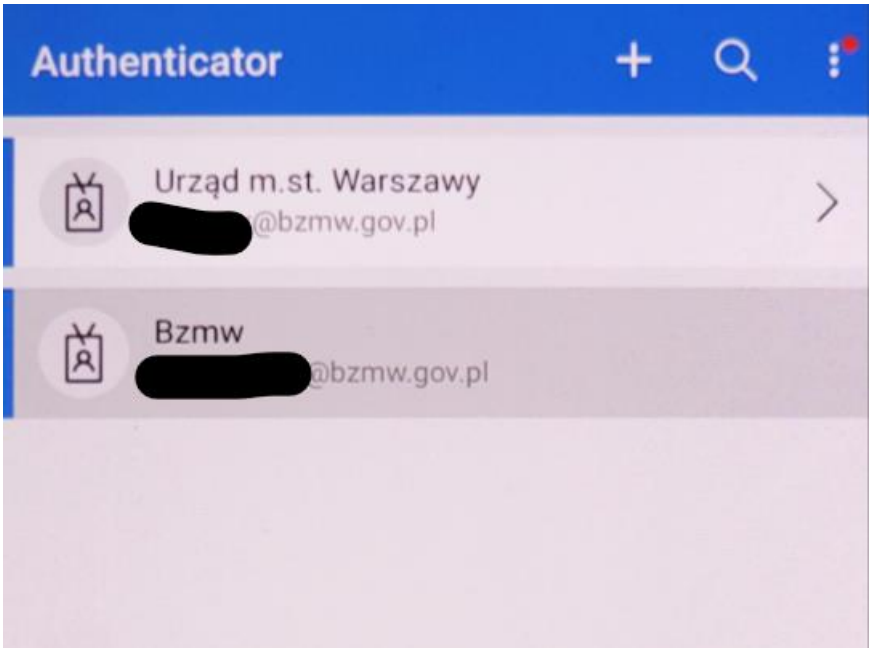


Następnie system poprosi Cię o dodanie konta. Możesz dodać różne konta, zarówno służbowe jak i prywatne. Aplikację możesz wykorzystać do uwierzytelniania wieloskładnikowego zarówno do usług służbowych jak i prywatnych (np. prywatne konto mailowe, aplikacje społecznościowe, itp.). Nikt z urzędu nie ma dostępu do listy kont, które masz zapisane w aplikacji. Konfigurację przeprowadzimy na przykładzie konta służbowego.

Wybierz polecenie Zeskanuj kod QR:

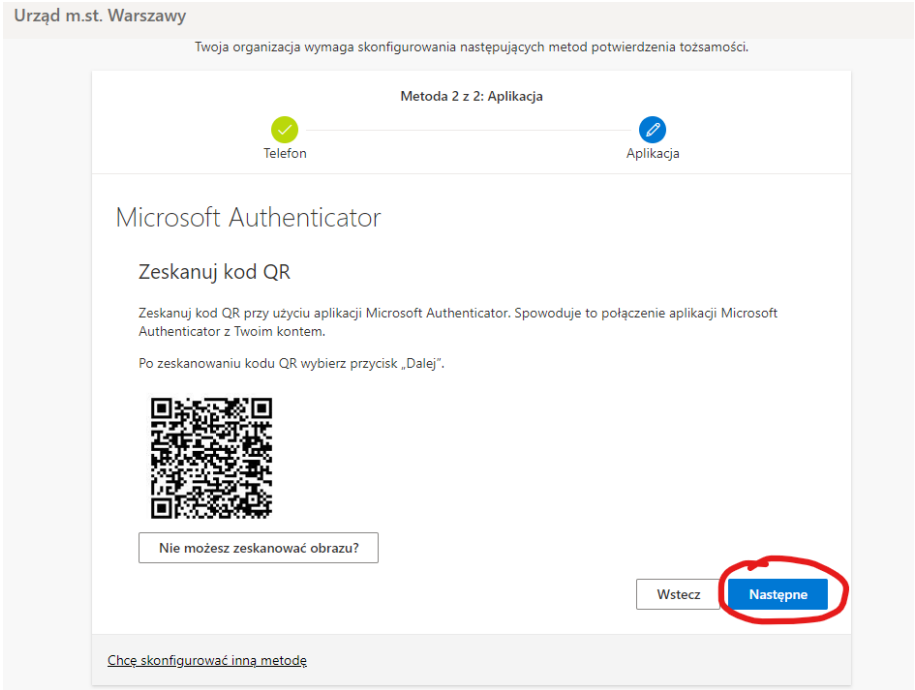
W urządzeniu przenośnym uruchomi się aparat. Zezwól aplikacji na korzystanie z aparatu i zrób zdjęcie kodu, który wyświetla się na ekranie komputera.

Po zeskanowaniu, Twoje konto doda się do aplikacji potwierdzającej logowanie:

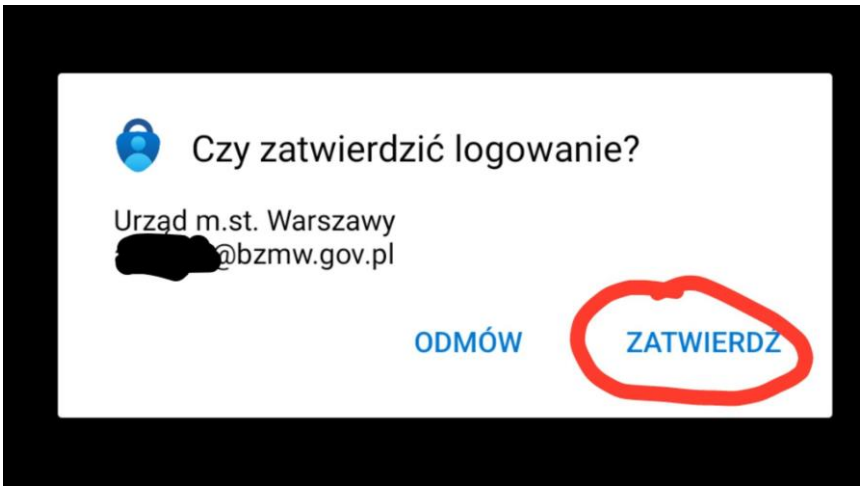


Jednocześnie włączona została blokada aplikacji Microsoft Authenticator. Jest to ta sama blokada jak a została wykorzystana w telefonie do blokowania ekranu np. odcisk palca lub kod PIN.

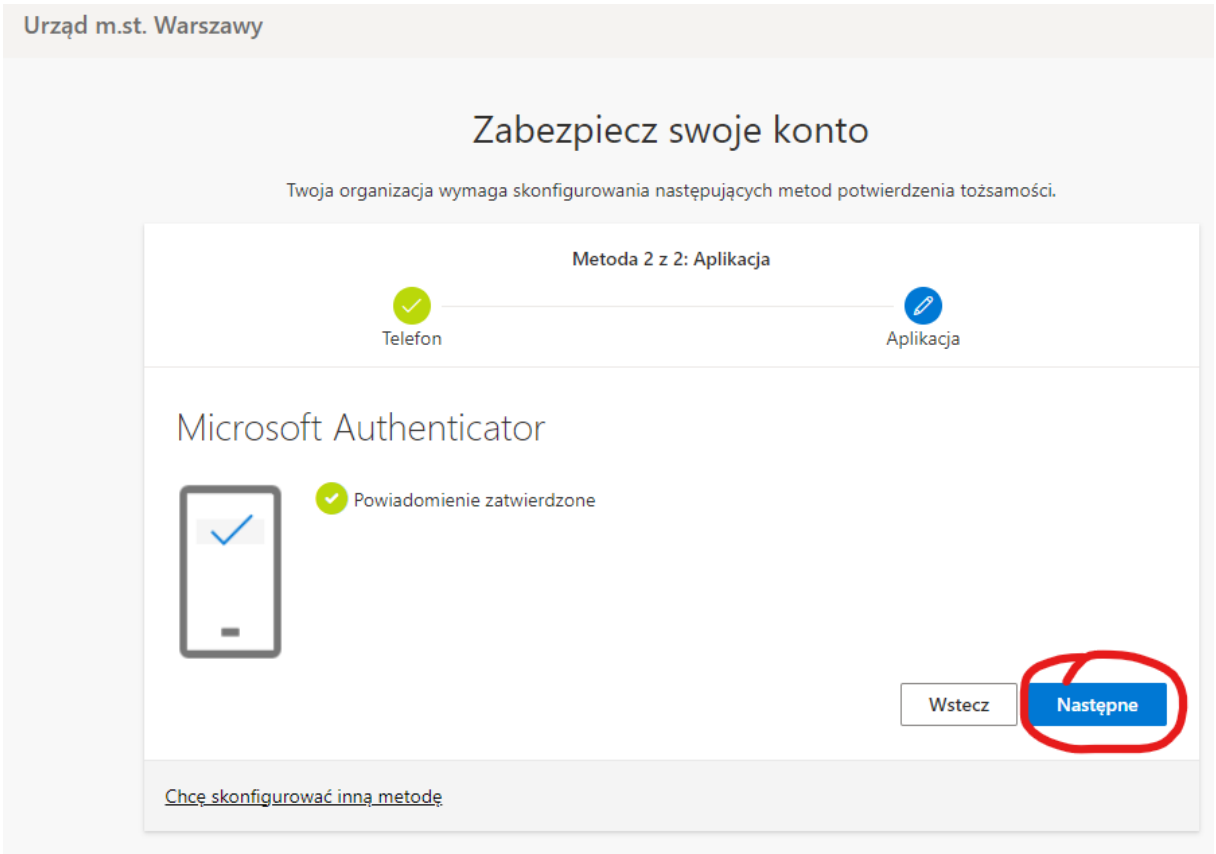
Na ekranie komputera kliknij przycisk Następne:



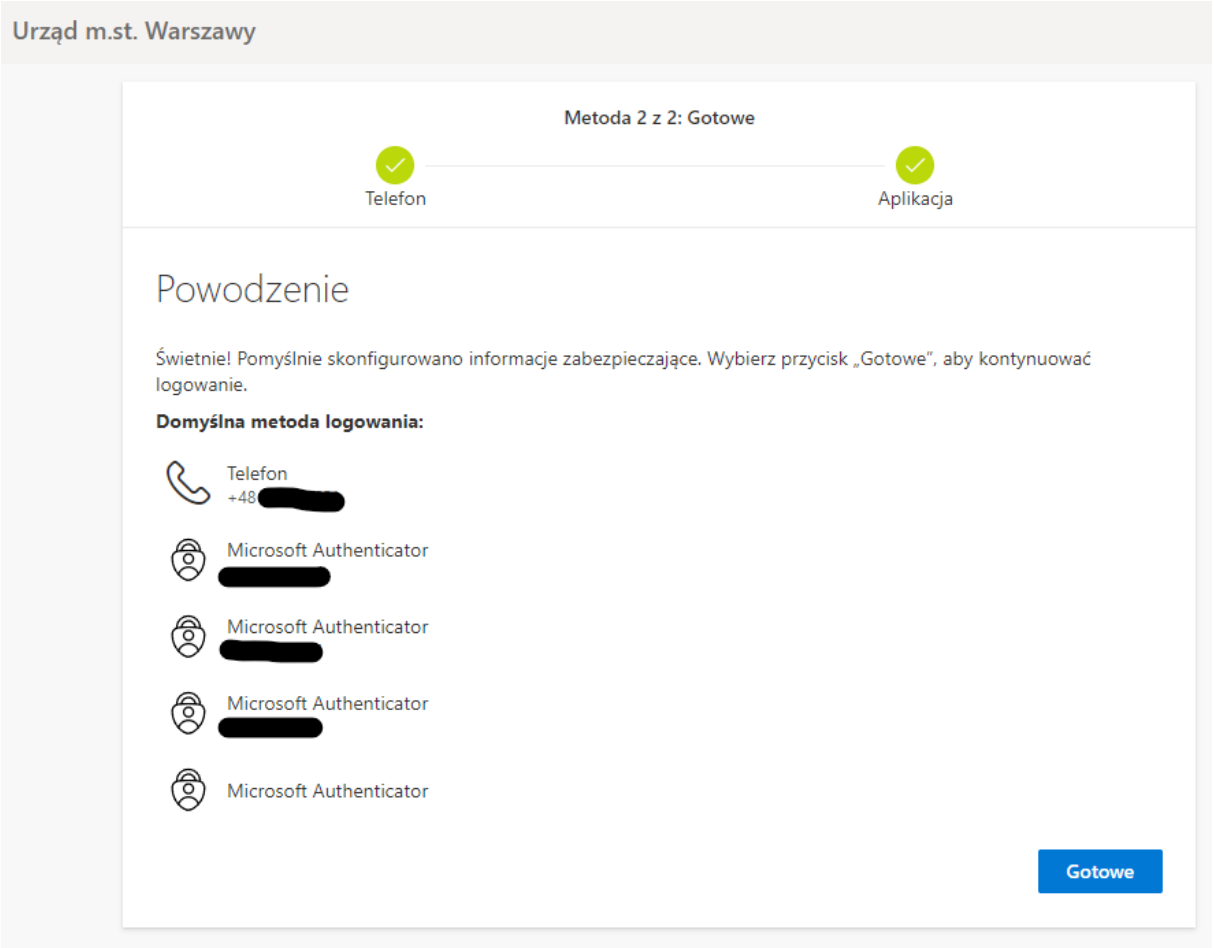
Na urządzeniu przenośnym pojawi się prośba o zatwierdzenie logowania:



Należy je zatwierdzić. W tym momencie usługa została ustawiona.



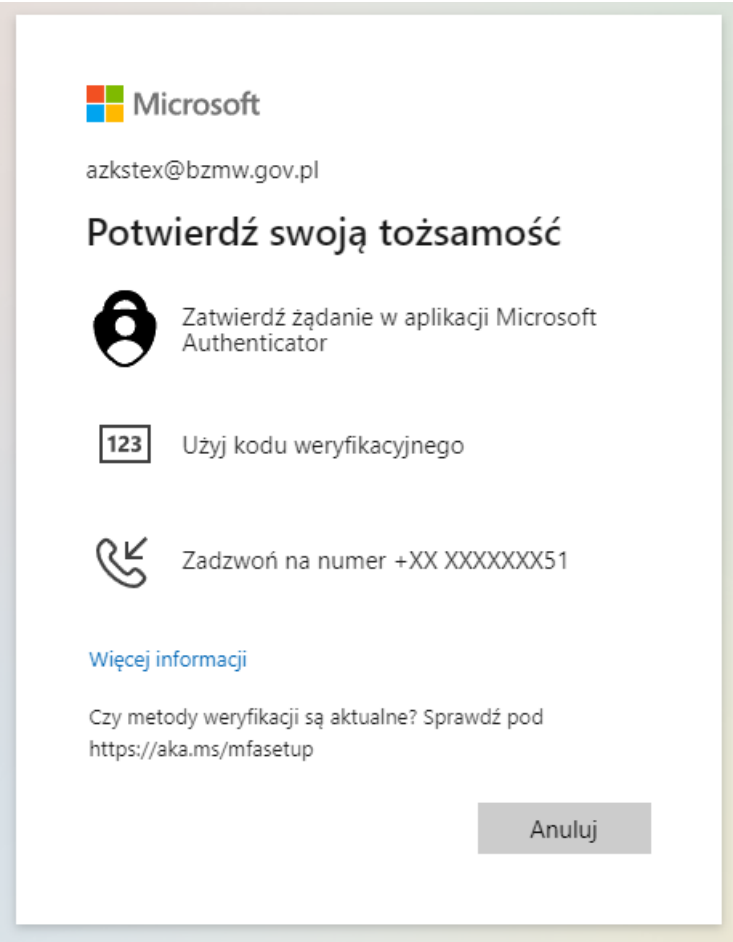
Po kliknięciu polecenia Następne zostanie wyświetlona lista wszystkich metod uwierzytelnienia jakie są przypisane do Twojego konta.



Potwierdzanie logowania do usług Microsoft 365 i innych, które takiego uwierzytelnia będą wymagały, jest możliwe za pomocą połączenia telefonicznego lub aplikacji mobilnej.

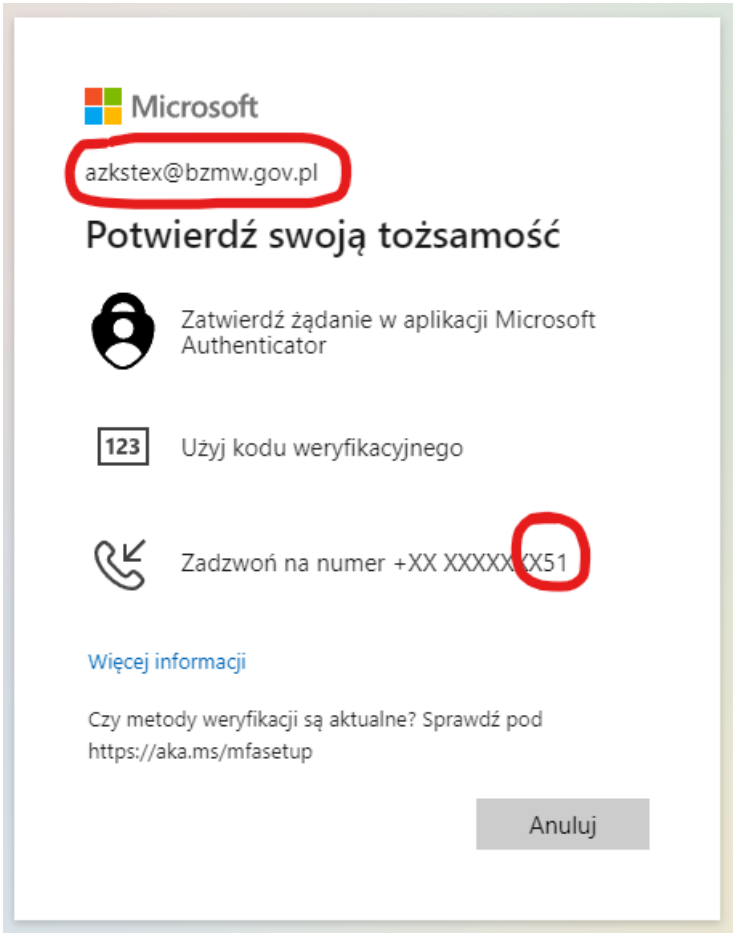
Kolejne logowania

Podczas kolejnych logowań po wpisaniu loginu i hasła pojawi się od razu okno Potwierdź swoją tożsamość. Aby skorzystać z potwierdzania telefonicznego wybierz polecenie Zadzwoń na numer +XX XXXXXXXXX. Jeśli chcesz skorzystać z aplikacji mobilnej wybierz polecenie Zatwierdź żądanie w aplikacji Microsoft Authenticator (ewentualnie w innej, jeśli nie korzystasz z aplikacji Microsoft). Możesz też użyć kodu weryfikacyjnego, który generowany jest również w aplikacji mobilnej



Jeśli wybierzesz połączenie telefoniczne, to odbierz telefon i zatwierdź logowanie przyciskiem # na klawiaturze telefonu.

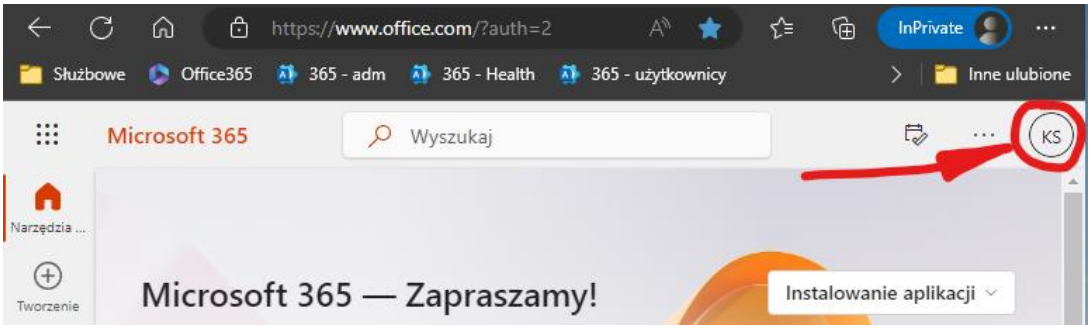
Podczas logowania zwróć uwagę na następujące elementy: nazwa konta służbowego – powinna być wyświetlona nazwa naszego konta oraz w numerze telefonu dwie ostatnie cyfry powinny być zgodne z cyframi naszego numeru telefonu.



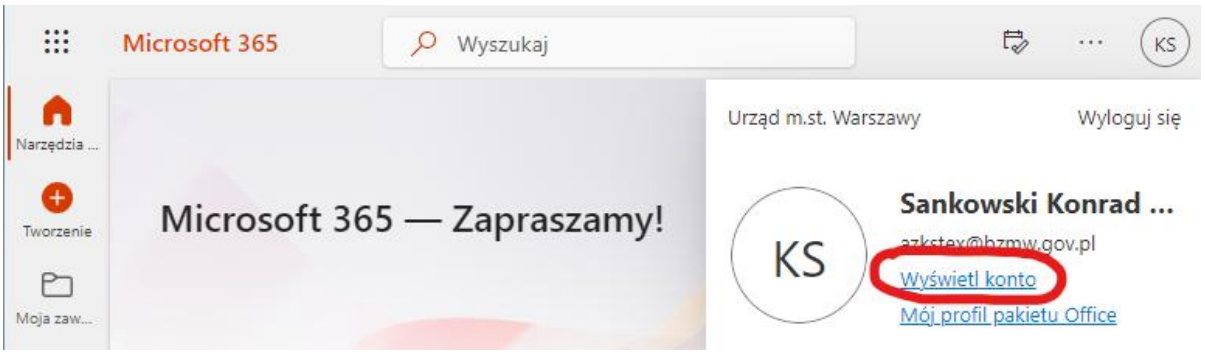
Samodzielna zmiana numeru telefonu i metody uwierzytelniania

W każdej chwili możesz samodzielnie zmienić zarówno domyślną metodę uwierzytelniania jak i numer telefonu. Przyda się to szczególnie wtedy gdy nie będziesz mieć np. możliwości odebrać połączenia na telefonie stacjonarnym lub gdy zmienisz numer (np. przy okazji zmiany komórki w której pracujesz).

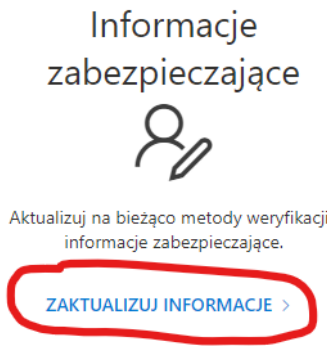
Żeby zmienić metodę uwierzytelniania lub numer telefonu musisz przede wszystkim zalogować się do swojego konta w usłudze Microsoft 365. Najlepiej zrobić to poprzez stronę https://office.com. Będąc na tej stronie kliknij na ikonę profilową ze swoim zdjęciem lub inicjałami w prawym, górnym rogu strony:



W oknie, które się otworzy kliknij polecenie Wyświetl konto:



Spowoduje to otwarcie strony z Ustawieniami Twojego konta służbowego w usłudze Microsoft 365. W karcie Informacje zabezpieczające kliknij polecenie Zaktualizuj informacje:



W kolejnym oknie zobaczysz listę metod, które masz zapisane do uwierzytelniania logowania. Możesz tu dodać lub usunąć metodę logowania a także zmienić aktualny numer telefonu. Jeśli zajdzie taka potrzeba, np. stracisz urządzenie, na którym masz zapamiętane logowanie, możesz wylogować się ze wszystkich urządzeń, które posiadasz. Zapobiegnie to dostanie się osobom nieuprawnionym do danych.