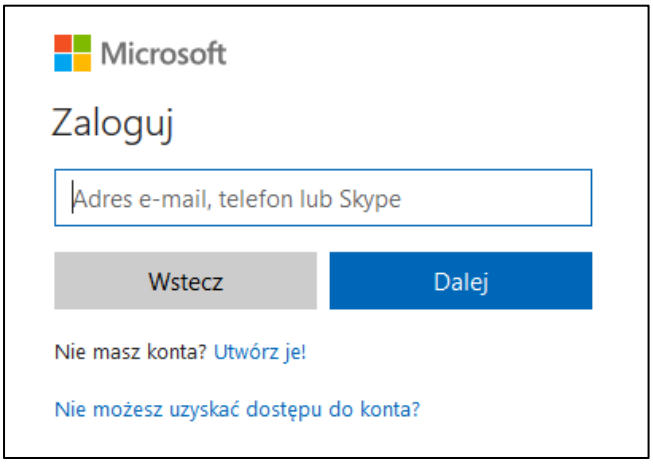
KONFIGURACJA WIELOSKŁADNIKOWEGO UWIERZYTELNIANIA

Konfigurowanie wieloskładnikowego uwierzytelniania

a. W celu konfiguracji wieloskładnikowego uwierzytelniania (MFA – Multi-factor authentication) należy wejść na stronę https://mfa.sgh.waw.pl i zalogować się do swojego konta SGH (Rys.1).

Rys. 1

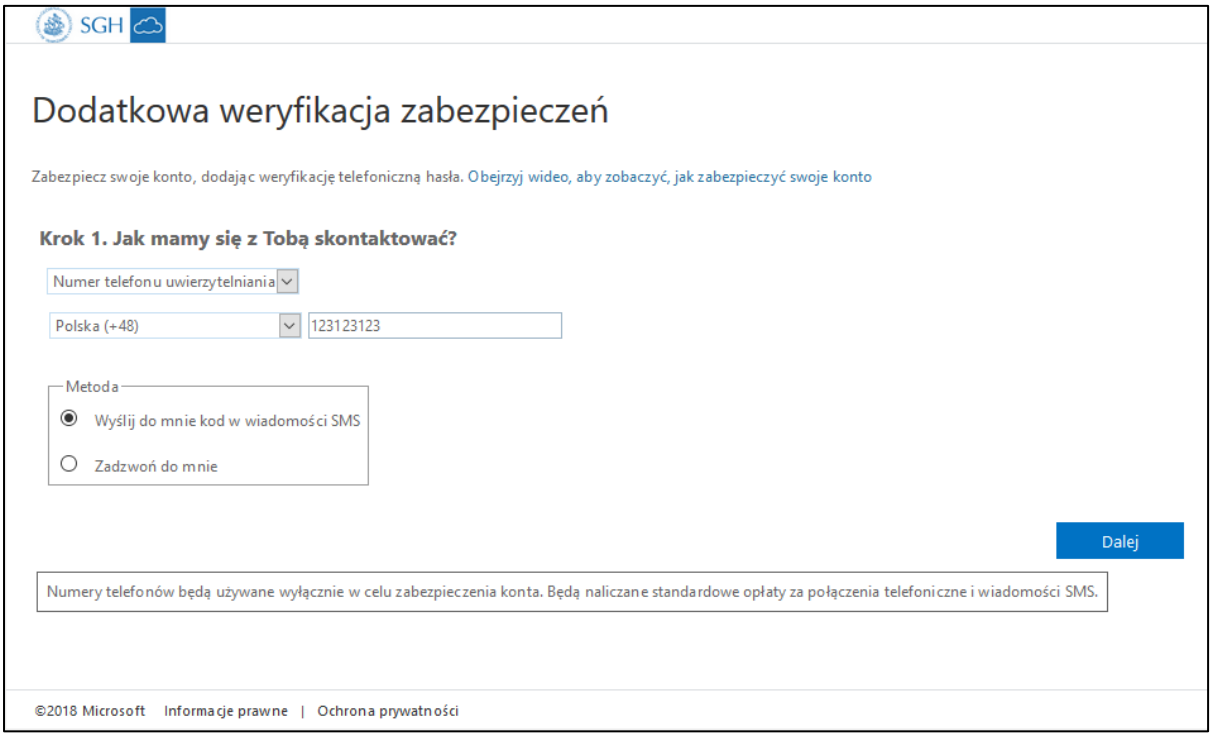


b. Po poprawnym zalogowaniu pojawi się poniższy widok. Wtedy należy wybrać niebieski przycisk *Skonfiguruj je teraz* (Rys.2).

Rys. 2

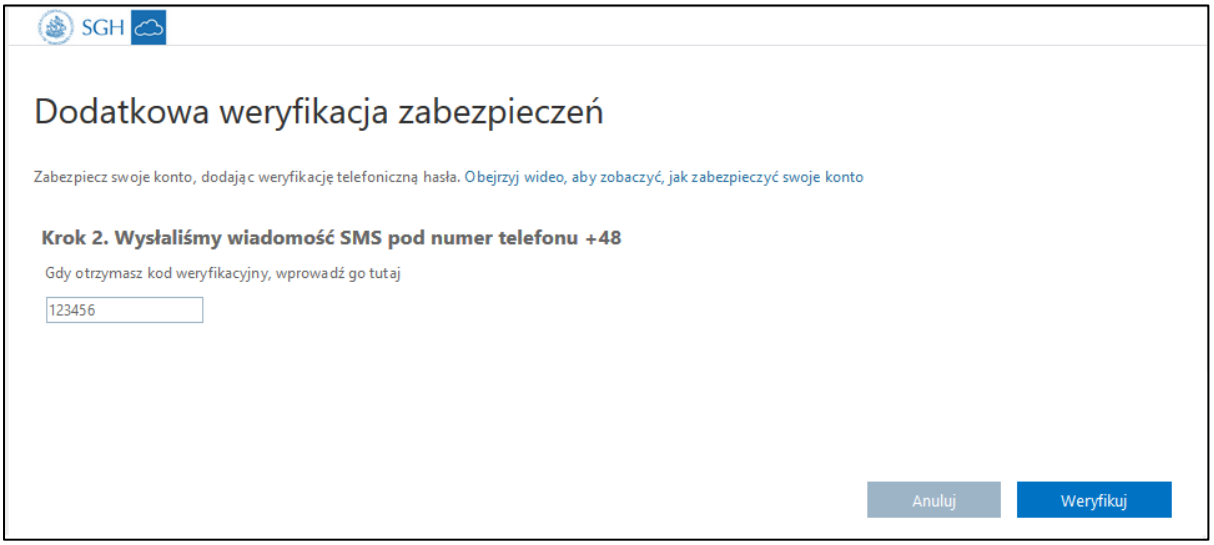
c. W kolejnym kroku należy uzupełnić dane kontaktowe, które posłużą do konfiguracji dwuskładnikowego uwierzytelniania (Rys.3).

Rys. 3

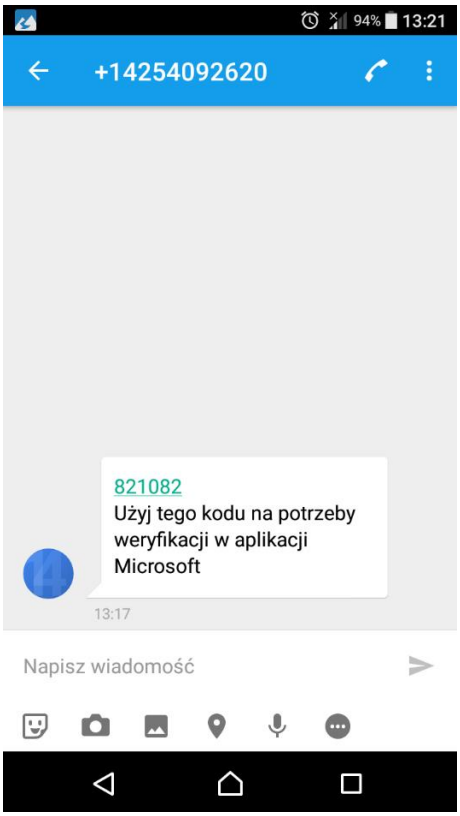


d. Po wybraniu przycisku *Dalej* przejdziemy do kolejnego kroku (Rys.4), w którym należy podać kod otrzymany w wiadomości SMS (Rys.5).

Rys. 4

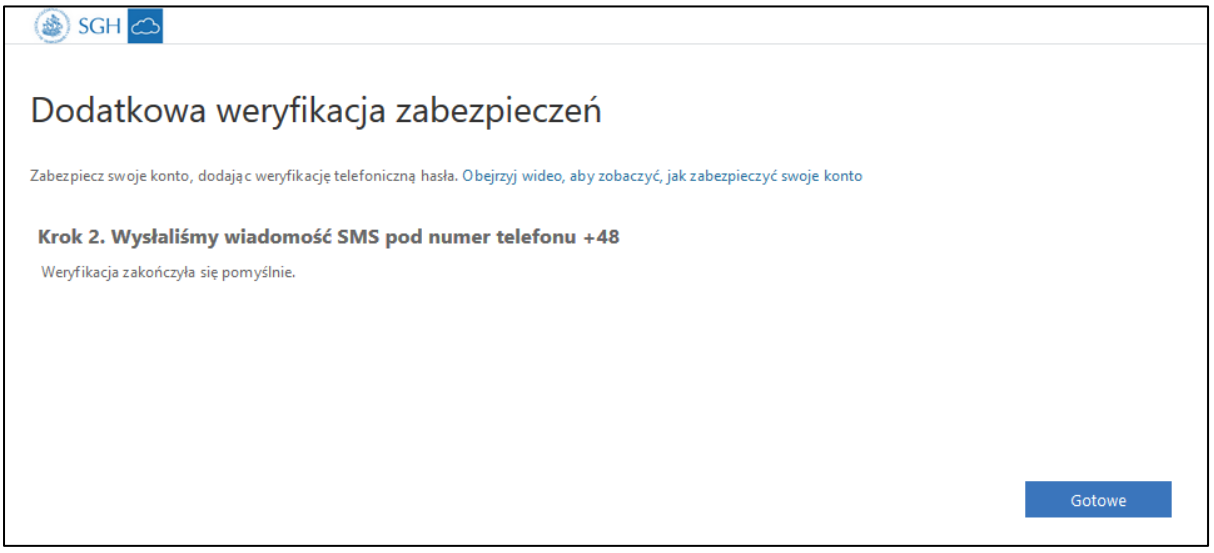


Rys. 5



e. Po zweryfikowaniu poprawności kodu, konfiguracja dwuskładnikowa zostanie zakończona - pojawi się komunikat *Weryfikacja zakończyła się pomyślnie* (Rys.6).

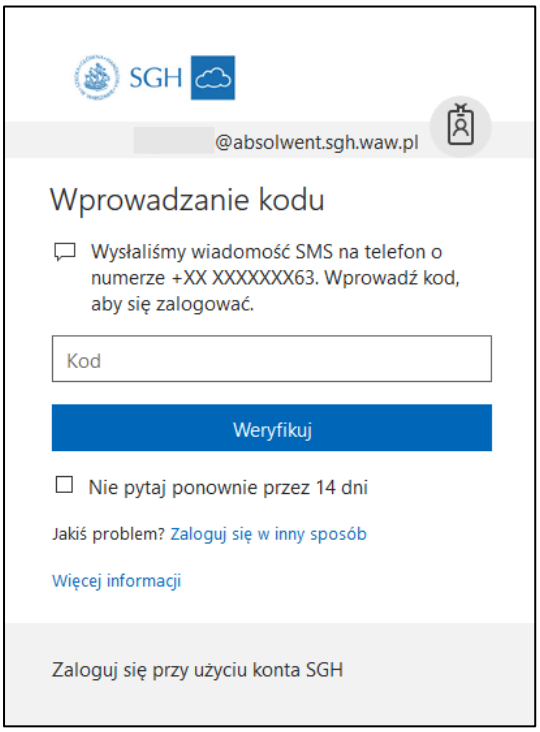
Rys. 6



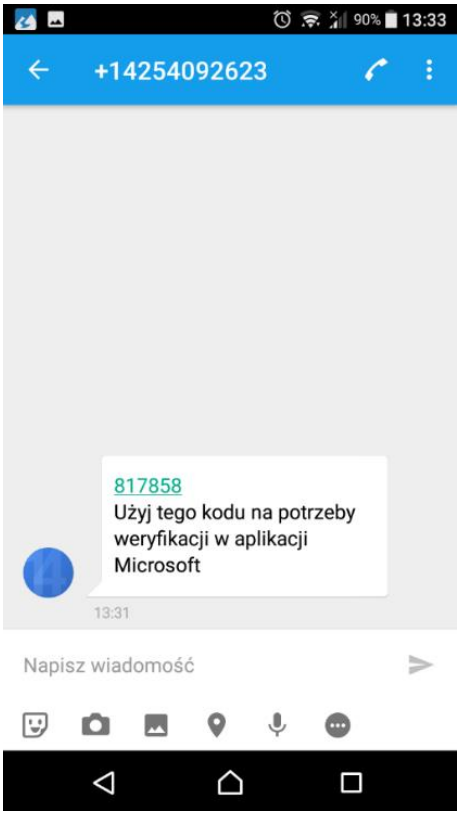
Pierwsze logowanie

a. Po skonfigurowaniu dodatkowej weryfikacji zabezpieczeń, pojawi się okienko z prośbą o wpisanie kodu (Rys.7), który otrzymamy w wiadomość SMS (Rys.8).

Rys. 7

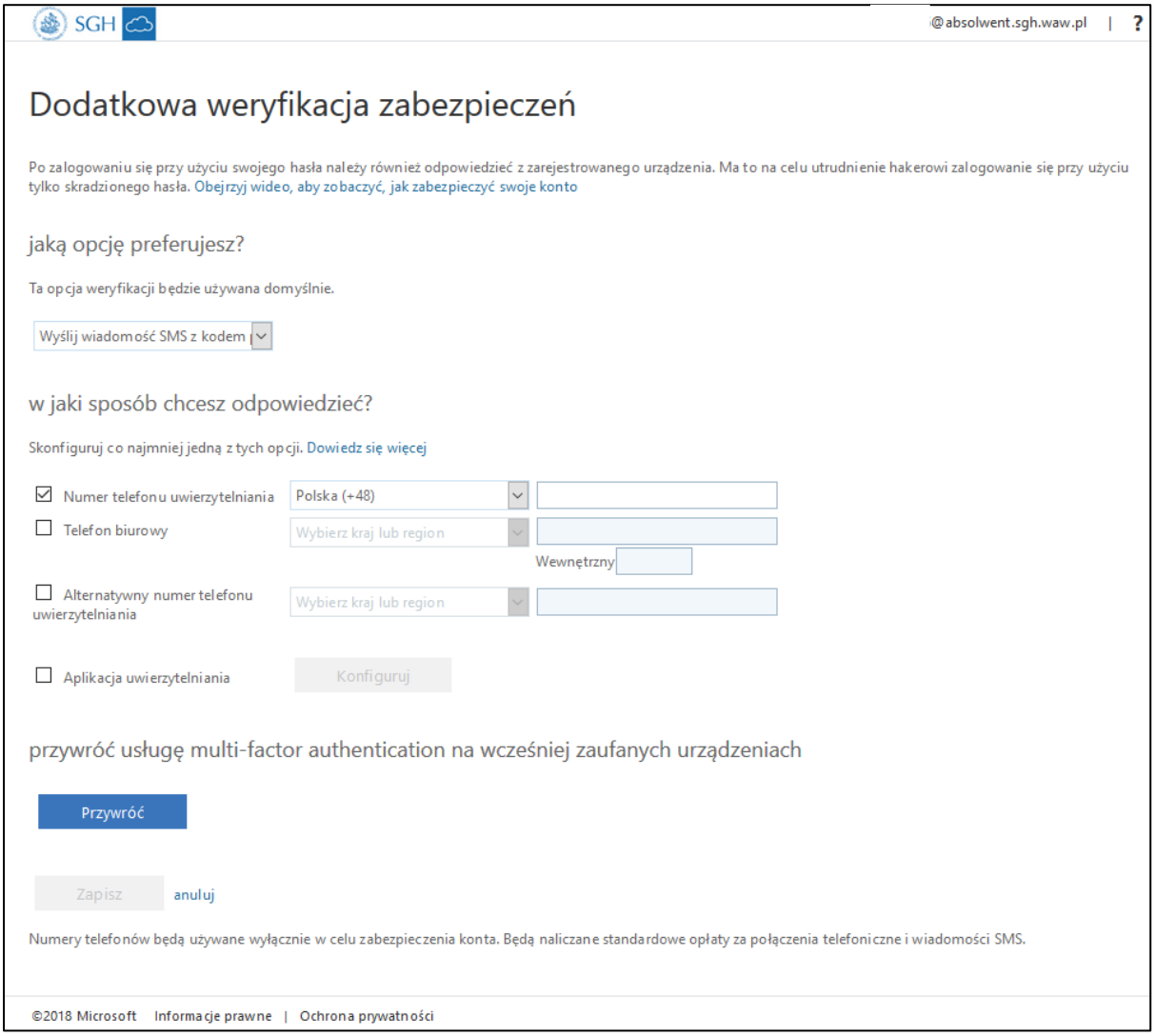


Rys. 8



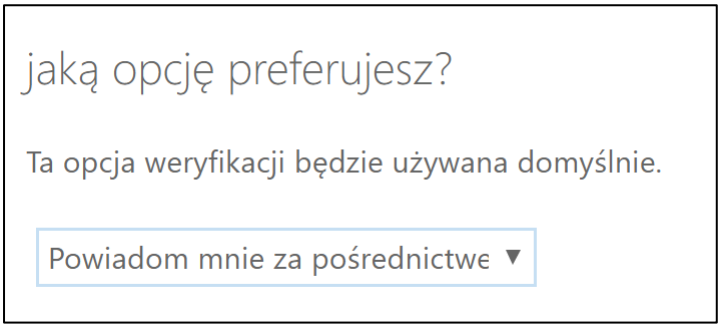
b. Po wpisaniu kodu i kliknięciu *Weryfikuj* pojawi się poniższy widok (Rys.9)

Rys. 9

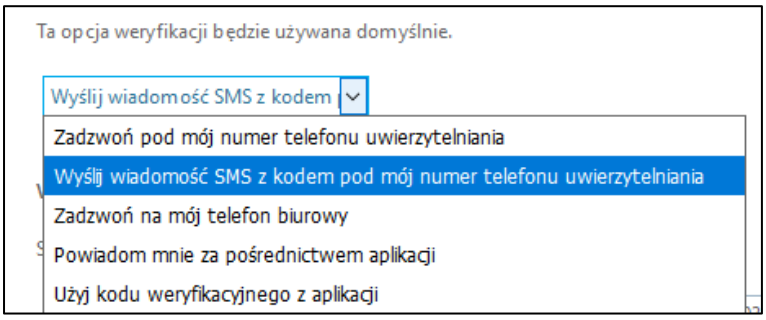


Po rozwinięciu opcji „***jaką opcję preferujesz?***” (Rys. 10), możemy wybrać domyślny sposób weryfikacji. Oznacza to, że podczas logowania będziemy proszeni o potwierdzenie swojej tożsamości poprzez właśnie ten sposób weryfikacji. Jednakże, jeśli nie będziemy mogli z niego skorzystać, możliwe będzie potwierdzenie swojej tożsamości poprzez inny sposób weryfikacji skonfigurowany na etapie *Dodatkowej weryfikacji zabezpieczeń* (Rys. 11).

Rys. 10



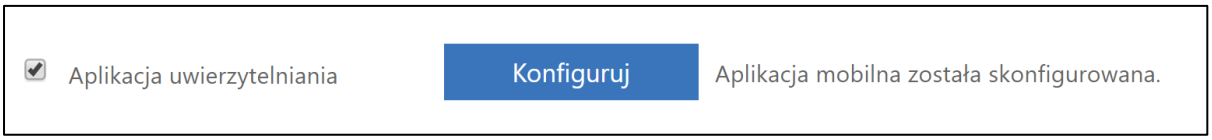
Rys. 11



Opcja "***w jaki sposób chcesz odpowiedzieć?"*** pozwala na skonfigurowanie różnych opcji uwierzytelniania. Dostępne warianty to:

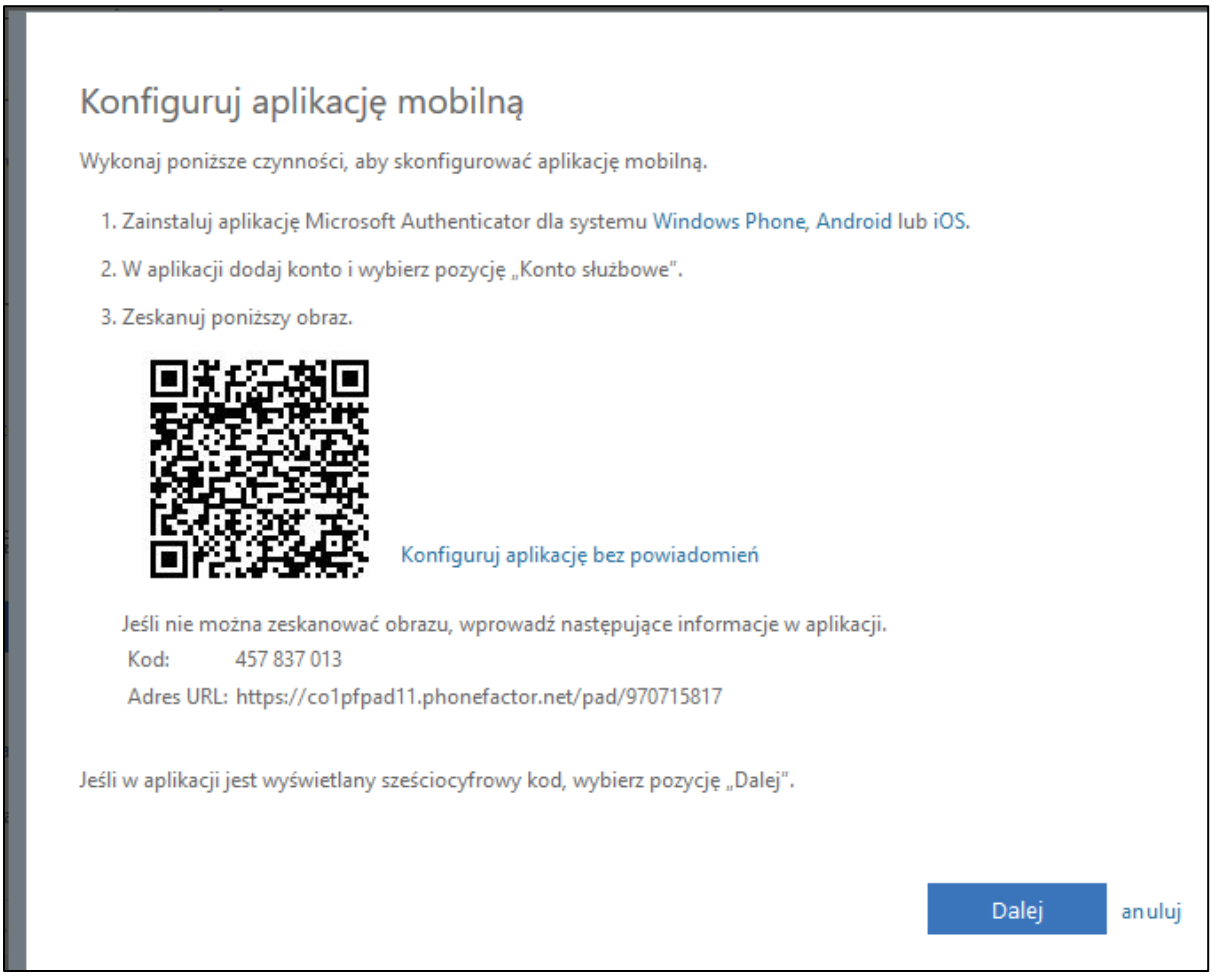
- *Numer telefonu uwierzytelniania* - w tym miejscu dodajemy numer telefonu, na który chcemy otrzymywać SMS z kodem uwierzytelniania
- *Telefon biurowy* – dane do tej opcji są pobierane automatycznie z książki adresowej SGH
- *Alternatywny numer telefonu uwierzytelniania* - dodatkowy numer telefony, na który możemy otrzymać kod SMS do uwierzytelniania
- *Aplikacja uwierzytelniania (Microsoft Authenticator)* – pozwala na potwierdzanie tożsamości poprzez aplikację mobilną na służbowym lub prywatnym telefonie komórkowym. Po wybraniu tej opcji należy pamiętać o skonfigurowaniu aplikacji na telefonie wybierając przycisk *Konfiguruj* (Rys. 12). Aplikację można pobrać w sklepie Google Play lub App Store.

Rys. 12



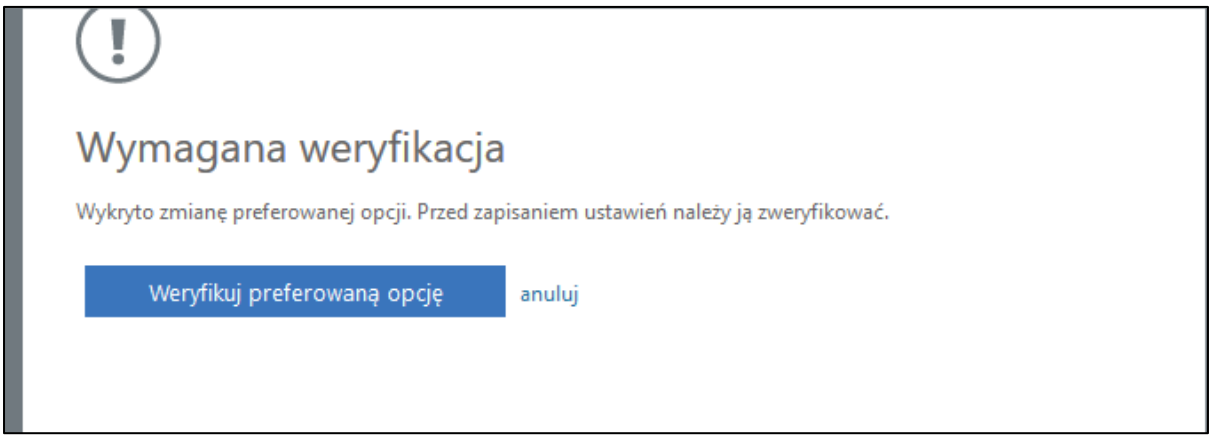
Po wybraniu opcji *Konfiguruj*, przejdziemy do okienka z instrukcją, jak skonfigurować aplikację na telefonie (Rys. 13). Następnie należy postępować zgodnie z podaną instrukcją.

Rys. 13



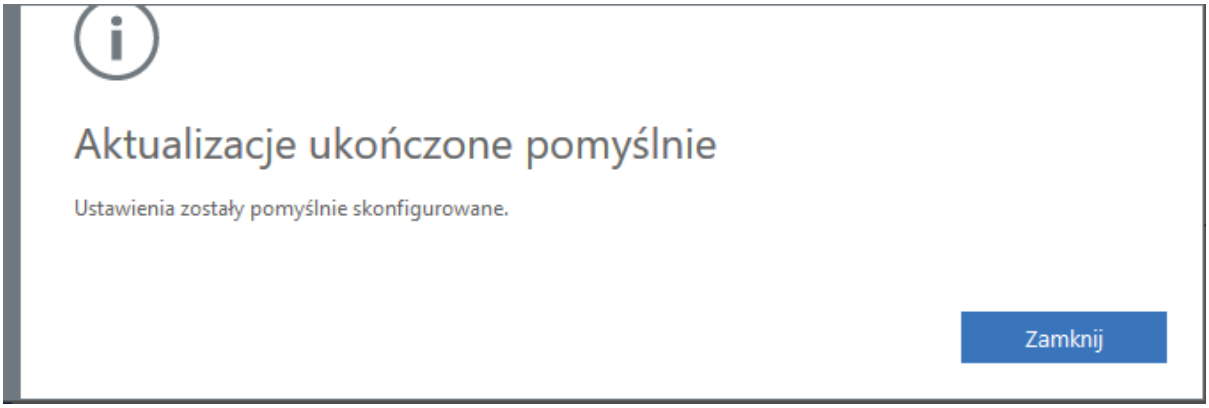
Po wykonaniu kolejnych kroków oraz wybraniu opcji *Dalej* pokaże się poniższy komunikat (Rys. 14). Należy kliknąć *Weryfikuj preferowaną opcję* i postępować zgodnie ze wskazówkami.

Rys. 14



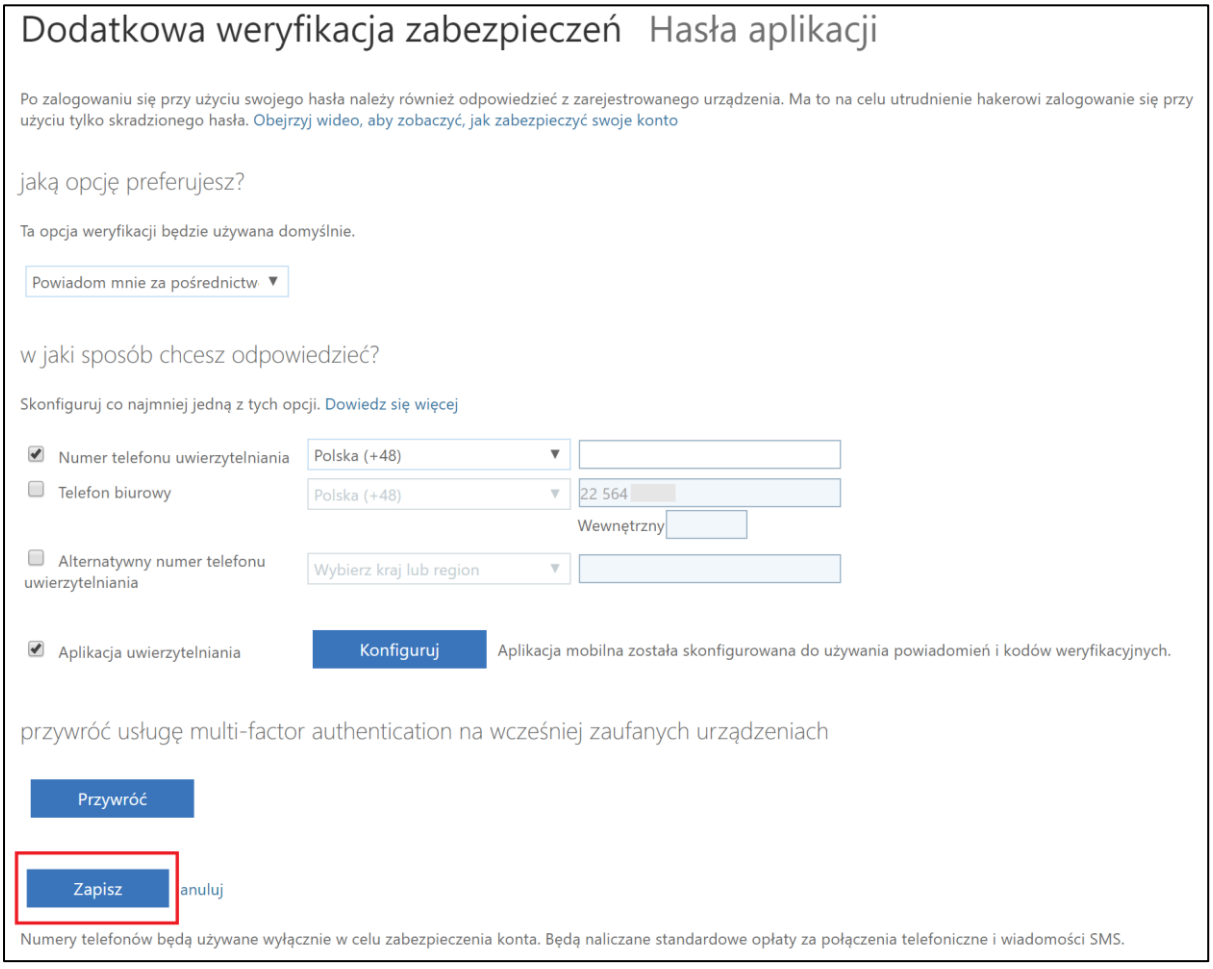
Po pomyślnym zakończeniu weryfikacji, pojawi się komunikat *Aktualizacje ukończone pomyślnie* (Rys. 15). Na zakończenie konfiguracji opcji *Aplikacja mobilna* należy kliknąć *Zakończ*.

Rys. 15



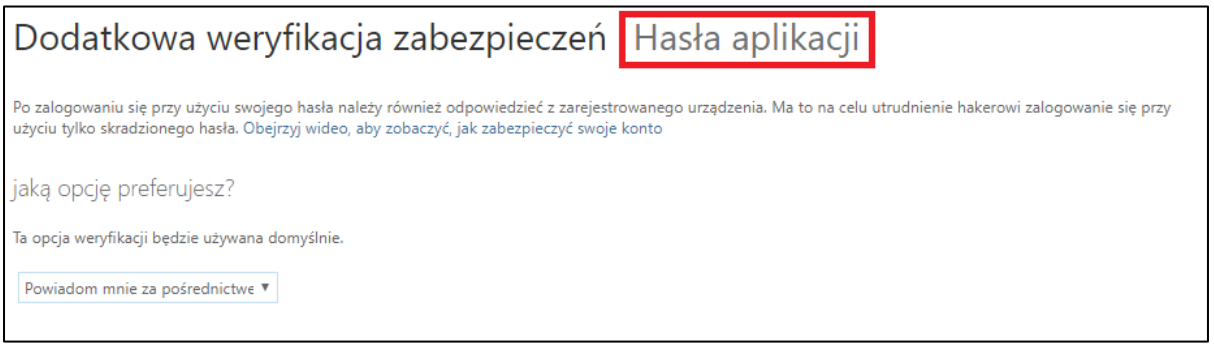
Po zakończeniu konfiguracji opcji uwierzytelniania dwuskładnikowego, należy zapisać wprowadzone ustawienia wybierając w lewym dolnym rogu przycisk *Zapisz* (Rys. 16).

Rys. 16



Uwaga! Jeśli korzystają Państwo z pocztowych aplikacji natywnych na urządzeniach mobilnych, mogą one wymagać dodatkowego potwierdzenia. W zakładce *Hasła aplikacji* (Rys. 17) znajdą Państwo instrukcję, jak wygenerować hasło do aplikacji natywnych (Rys. 18).

Rys. 17



Rys. 18