INSTRUKCJA UŻYTKOWNIKA KONTA DOSTĘPOWEGO UMOŻLIWIAJĄCEGO KORZYSTANIE Z APLIKACJI INTERNETOWYCH GK KDPW

SPIS TREŚCI

I OTWARCIE KONTA DOSTĘPOWEGO

I.1. O koncie dostępowym

Aby korzystać z aplikacji internetowych do komunikacji elektronicznej z KDPW należy korzystać z przeglądarek internetowych zgodnych HTML5, z włączoną obsługą JavaScript oraz obsługą Cookies. Nie jest obsługiwana przeglądarka Internet Explorer – by poprawnie korzystać z aplikacji zalecamy nieużywanie tej przeglądarki niezależnie od aktualnej wersji.

Otwarcie konta dostępowego jest niezbędne do korzystania z aplikacji zarówno w środowisku produkcyjnym jak i testowym. Otwarcie konta jest bezpłatne.

Konto dostępowe pozwala na dostęp do wszystkich aplikacji GK KDPW, do których posiadacz konta uzyskał wcześniej dostęp. Uwierzytelnienie do danego konta dostępowego pozwala na przełączanie się między aplikacjami bez konieczności odrębnego uwierzytelniania się do każdej z nich.

W przypadku istnienia różnych polityk dostępu, w szczególności w przypadku przełączania się pomiędzy aplikacją wymagającą wyłącznie potwierdzenia podstawowym mechanizmem uwierzytelnienia (login i hasło), a aplikacją wymagającą dodatkowego potwierdzenia logowania z wykorzystaniem zaufanego urządzenia i aplikacji mobilnej KDPW Group Authenticator, użytkownik może zostać poproszony o powtórne uwierzytelnienie.

I.2. Żeby otworzyć konto dostępowe należy:

1. Na stronie logowania do wybranej usługi wybrać opcję „Zarejestruj się teraz”.
2. Podać swój adres e-mail. Adres ten będzie identyfikatorem konta dostępowego (loginem). W ramach otwartego konta nie będzie możliwości zmiany identyfikatora, co oznacza, że zmiana adresu e-mail będzie wymagała utworzenia nowego konta dostępowego.
3. Potwierdzić dostęp do adresu e-mail, będącego identyfikatorem konta. W tym celu należy użyć przycisku „Prześlij mi kod weryfikacyjny”, w wyniku czego na adres e-mail, będący identyfikatorem konta zostanie przekazany kod, który należy wprowadzić do formularza w aplikacji, a następnie wybrać przycisk „Zweryfikuj kod”.

Jeśli kod weryfikacyjny nie zostanie przesłany należy sprawdzić foldery dedykowane dla wiadomości typu Spam. Można także poprosić o powtórne wysłanie kodu, wybierając przycisk „Wyślij nowy kod”.

4. Wprowadzić hasło dostępowe utworzone zgodnie z podaną w formularzu instrukcją oraz podać swoje imię i nazwisko.
5. Wyrazić zgodę na przetwarzanie danych osobowych oraz potwierdzić zapoznanie się z klauzulą informacyjną, dotyczącą przetwarzania danych osobowych przez KDPW. Bez wykonania powyższych czynności otwarcie konta nie będzie możliwe.
6. Otworzyć konto poprzez wybranie przycisku „Utwórz”. Otwarcie konta potwierdzone zostanie przekierowaniem do strony logowania. Proces otwierania konta można anulować wybierając przycisk „Anuluj”.

I.3. Żeby zalogować się do aplikacji KDPW, przy użyciu uprzednio otwartego konta dostępowego, należy:

1. Wprowadzić do formularza na stronie aplikacji KDPW identyfikator użytkownika konta, którym jest adres e–mail podany przy otwieraniu konta, oraz hasło do konta dostępowego.
2. W przypadku aplikacji udostępnianych w ramach Portalu usług online.kdpw.pl, potwierdzić operację z wykorzystaniem aplikacji mobilnej KDPW Group Authenticator. Aplikacja powinna zostać zainstalowana oraz skonfigurowana z używanym w procesie logowania kontem dostępowym.
3. Ewentualnie zatwierdzić przeglądarkę użytą w procesie logowania jako zaufaną za pomocą aplikacji dostępnej pod adresem https://identity.kdpw.pl. Każde kolejne logowanie na komputerze lub urządzeniu mobilnym z wykorzystaniem przeglądarki, która została zarejestrowana jako zaufana nie wymaga potwierdzania przy użyciu aplikacji mobilnej KDPW Group Authenticator. Decyzja taka powinna być podjęta jedynie wobec przeglądarek na komputerze pozostającym pod kontrolą użytkownika i co do bezpieczeństwa której użytkownik ma zaufanie. Zarządzanie przeglądarkami oznaczonymi jako zaufane możliwe jest w aplikacji dostępnej pod adresem https://identity.kdpw.pl.

I.4. Żeby odzyskać dostęp do konta w przypadku utraty hasła albo zmienić hasło do konta dostępowego należy:

1. Wybrać przycisk „Nie pamiętasz hasła?”.
2. Podać identyfikator użytkownika konta, którym jest adres e-mail podanym przy otwieraniu konta.
3. Potwierdzić dostęp do adresu e-mail, będącego identyfikatorem konta. W tym celu należy użyć przycisku „Prześlij mi kod weryfikacyjny”, w wyniku czego na adres e-mail, będący identyfikatorem konta zostanie przekazany kod, który należy wprowadzić do formularza w aplikacji, a następnie wybrać przycisk „Zweryfikuj kod”.
4. Jeśli kod weryfikacyjny nie zostanie przesłany należy sprawdzić foldery dedykowane dla wiadomości typu Spam. Można także poprosić o powtórne wysłanie kodu, wybierając przycisk „Wyślij nowy kod”.
5. Podać nowe hasło i je potwierdzić.

I.5. Żeby wylogować się z aplikacji KDPW, należy:

1. Wybrać przycisk „Wyloguj” umieszczony w prawym górnym rogu ekranu.

Jeśli używana jest niewłaściwa przeglądarka, przycisk „Wyloguj” może być niewidoczny.

II APLIKACJA MOBILNA KDPW GROUP AUTHENTICATOR

II.1. O aplikacji

Aplikacja mobilna KDPW Group Authenticator (zwana dalej aplikacją mobilną lub aplikacją) wykorzystywana jest do bezpiecznego potwierdzania procesu uwierzytelniania użytkowników do konta dostępowego zdefiniowanego w KDPW oraz do potwierdzania wykonania wybranych operacji.

Aby korzystać z aplikacji mobilnej niezbędne jest posiadanie urządzenia mobilnego działającego w oparciu o systemy operacyjne Google (Android) lub Apple (iOS). W przypadku systemu Android

minimalną wersją systemu jest wersja 6.0 (Marshmallow). Dla systemu iOS minimalna wersja to 12.1. Urządzenia na których instalowana będzie aplikacja nie mogą mieć przełamanych zabezpieczeń.

Aplikacja na wskazane systemy udostępniana jest w autoryzowanych sklepach dla poszczególnych systemów operacyjnych:

- Aplikacja dla systemu Android w sklepie Google Play,
- Aplikacja dla systemu iOS w Sklepie Apple App Store.

II.2. Żeby zainstalować aplikację mobilną KDPW Group Authenticator należy:

1. Pobrać aplikację na urządzenie mobilne ze sklepu odpowiedniego dla systemu, z którego ono korzysta (Android lub iOS). Instalacja aplikacji może zostać wykonana tylko z autoryzowanego sklepu dla danego systemu.
2. Uruchomić aplikację oraz wybrać opcję „Rozpocznij rejestrację urządzenia" na ekranie powitalnym aplikacji, a następnie opcję „Zaloguj się w KDPW". Opcja przekieruje na stronę logowania do konta dostępowego KDPW.
3. Uwierzytelnić się (podać identyfikator i hasło) do konta dostępowego, które ma zostać powiązane z urządzeniem i instalowaną na nim aplikacją mobilną KDPW Group Authenticator. Konto dostępowe musi być wcześniej utworzone. Po poprawnym zalogowaniu na adres e-mail wskazany jako identyfikator konta dostępowego wysłany zostanie kod weryfikacyjny. Kod weryfikacyjny zostanie przesłany z adresu noreply@kdpw.pl. Jeżeli po kilku minutach wiadomość nie pojawi się w skrzynce odbiorczej, należy sprawdzić foldery z niechcianą pocztą (tzw. spam).
4. Potwierdzić powiązanie konta dostępowego z urządzaniem poprzez wprowadzenie otrzymanego kodu w polu Kod weryfikacyjny i wciśnięcie klawisza Potwierdź.
5. Skonfigurować zabezpieczenia aplikacji oraz wyrazić zgodę na otrzymywanie powiadomień. W ramach konfiguracji zabezpieczeń należy wybrać kod PIN oraz ewentualnie aktywować zabezpieczenia biometryczne. Zabezpieczenia te będą wykorzystywane do weryfikacji użytkownika w momencie potwierdzania operacji z wykorzystaniem aplikacji mobilnej KDPW Group Authenticator.

II.3. Żeby powiązać dodatkowe konto dostępowe z aplikacją mobilną KDPW Group Authenticator należy:

1. Wybrać opcję „Dodaj nowe konto" na ekranie ustawień aplikacji mobilnej. Aplikacja przekieruje użytkownika na stronę KDPW pozwalającą na uwierzytelnienie się do posiadanego konta dostępowego.
2. Uwierzytelnić się (podać identyfikator i hasło) do konta dostępowego, które ma zostać powiązane z urządzeniem i instalowaną na nim aplikacją mobilną KDPW Group Authenticator. Konto dostępowe musi być wcześniej utworzone. Po poprawnym zalogowaniu na adres e-mail wskazany jako identyfikator konta dostępowego wysłany zostanie kod weryfikacyjny. Kod weryfikacyjny zostanie przesłany z adresu noreply@kdpw.pl. Jeżeli po kilku minutach wiadomość nie pojawi się w skrzynce odbiorczej, należy sprawdzić foldery z niechcianą pocztą (tzw. spam).
3. Potwierdzić powiązanie konta dostępowego z urządzaniem poprzez wprowadzenie otrzymanego kodu w polu „Kod weryfikacyjny" i wciśnięcie klawisza „Potwierdź".
4. Potwierdzić wykonanie operacji z wykorzystaniem kodu PIN lub biometrii, w zależności od ustawionego w aplikacji mobilnej rodzaju zabezpieczeń.

II.4. Żeby usunąć konto dostępowe powiązane z aplikacją mobilną KDPW Group Authenticator należy:

1. Na ekranie aplikacji w zakładce Ustawienia w sekcji Konta wybrać opcję usunięcia konta (prezentowaną w postaci ikony kosza) przy odpowiednim koncie dostępowym.
2. Potwierdzić operację usunięcia z wykorzystaniem kodu PIN lub biometrii, w zależności od ustawionego w aplikacji mobilnej rodzaju zabezpieczeń. Jeżeli usuwane konto jest ostatnim kontem w aplikacji, aplikacja wróci do stanu po instalacji, wyświetlony zostanie ekran powitalny.

II.5. Zabezpieczenie aplikacji KDPW Group Authenticator przed nieuprawnionym użyciem:

1. Aplikacja zostanie zablokowana w przypadku, gdy wprowadzony będzie niepoprawny kod PIN 5 razy z rzędu. Zablokowana aplikacja informuje o tym fakcie użytkownika za pomocą dedykowanego komunikatu.
2. W momencie zablokowania urządzenia, na adresy e-mail kont dostępowych powiązanych z urządzeniem wysyłany jest komunikat o zablokowaniu urządzenia. Komunikat zostanie przesłany z adresu noreply@kdpw.pl. Jeżeli po kilku minutach wiadomość nie pojawi się w skrzynce odbiorczej, należy sprawdzić foldery z niechcianą pocztą.

II.6. Żeby odblokować aplikację KDPW Group Authenticator należy:

1. Na ekranie aplikacji wybrać zakładkę Ustawienia i w sekcji Bezpieczeństwo wybrać opcję Odblokuj aplikację.
2. Wybrać konto, które ma być użyte w procesie odblokowywania. Opcja przekieruje na stronę logowania do konta dostępowego KDPW.
3. Uwierzytelnić się (podać identyfikator i hasło) do konta dostępowego. Po poprawnym zalogowaniu na adres e-mail wskazany jako identyfikator konta dostępowego wysłany zostanie kod weryfikacyjny. Kod weryfikacyjny zostanie przesłany z adresu noreply@kdpw.pl. Jeżeli po kilku minutach wiadomość nie pojawi się w skrzynce odbiorczej, należy sprawdzić foldery z niechcianą pocztą (tzw. spam).
4. Potwierdzić operację odblokowania poprzez wprowadzenie otrzymanego kodu w polu „Kod weryfikacyjny" i wciśnięcie klawisza „Potwierdź".
5. Ponownie skonfigurować kod PIN. Proces odblokowania automatycznie wyłączy wykorzystanie biometrii, jeśli było ono wcześniej aktywowane. W przypadku gdy użytkownik zamierza wykorzystywać biometrię niezbędne jest aktywowanie tej opcji w ramach ustawień aplikacji.

II.7. Żeby zmienić kod PIN należy:

1. Wybrać opcję „Zmień kod PIN" dostępną na ekranie ustawień aplikacji mobilnej w sekcji Bezpieczeństwo.
2. Wprowadzić aktualny kod PIN w sekcji Obecny kod PIN oraz podać nowy PIN w sekcji Nowy kod PIN. Nowy kod, dla zapewnienia poprawności wprowadzonych wartości należy podać dwukrotnie, przy czym jego ustawienie będzie możliwe tylko w przypadku stwierdzenia zgodności obu wartości.

   Żeby zmienić kod PIN bez podawania aktualnego kodu należy odinstalować i ponownie zainstalować aplikację.
3. Potwierdzić zmianę wciskając przycisk Ustaw PIN. Wprowadzenie zmian zostanie potwierdzone dedykowanym komunikatem. Po wprowadzeniu zmiany automatycznie wyłączone zostanie wykorzystanie biometrii, jeśli było ono wcześniej aktywowane. W przypadku gdy użytkownik

zamierza wykorzystywać biometrię niezbędne jest aktywowanie tej opcji w ramach ustawień aplikacji.

II.8. Żeby włączyć lub wyłączyć wykorzystanie zabezpieczeń biometrycznych należy:

1. Dotknąć przełącznika Zabezpieczenia biometryczne, umiejscowionego na ekranie ustawień aplikacji w sekcji Bezpieczeństwo. Jeśli przełącznik jest w kolorze szarym zabezpieczenia biometryczne są nieaktywne, w przeciwnym razie są one aktywne.
2. Wyłączenie korzystania z zabezpieczenia biometrycznego nie wymaga dodatkowego potwierdzenia. Po wyłączeniu wykorzystania biometrii, do potwierdzania operacji wymagane będzie podanie poprawnego kodu PIN.
3. Włączenie zabezpieczenia biometrycznego wymaga podania ważnego kodu PIN, który został ustanowiony w aplikacji. Po włączeniu biometrii wszystkie operacje będą potwierdzane z jej wykorzystaniem, a podanie kodu PIN nie będzie wymagane.

II.9. Żeby potwierdzić/odrzucić operację z wykorzystaniem aplikacji mobilnej KDPW Group Authenticator należy:

1. Wybrać właściwe powiadomienie na ekranie powiadomień w aplikacji. Jeśli na ekranie nie widać oczekiwanej informacji, można go odświeżyć dotykając go, a następnie przeciągnąć palec do dołu. Odpowiednie powiadomienie można tez wybrać korzystając z listy powiadomień dostępnej w systemie operacyjnym telefonu. Wybranie powiadomienia spowoduje przejście do ekranu „Potwierdzenie operacji".
2. Zweryfikować poprawność powiadomienia poprzez zapoznanie się z jego treścią i z datą jego wygenerowania. Każde z powiadomień ma określony czas ważności, prezentowany na ekranie. Po przekroczeniu czasu przewidzianego na akceptację nie będzie ona możliwa.
3. Potwierdzić/Odrzucić operację poprzez kliknięcie odpowiedniego przycisku dla wybranego powiadomienia, a następnie zatwierdzić wprowadzając kod PIN lub zabezpieczenie biometryczne (zależnie od ustawionej opcji).

II.10. Żeby zmienić nazwę urządzenia należy:

1. Przejść do ekranu ustawień w aplikacji mobilnej, do sekcji Nazwa urządzenia. W ramach tej sekcji wyświetlona jest nazwa, pod którą urządzenie jest identyfikowane w serwisach KDPW. Jeśli nazwa urządzenia nie została ustalona, używana jest nazwa fabryczna urządzenia.
2. Wybrać opcję „Zmień nazwę urządzenia".
3. Wprowadzić nową nazwę urządzenia i zatwierdzić przyciskiem „Zmień". Nazwa urządzenia może zawierać tylko litry, cyfry, spację i myślniki (-). Maksymalna długość nazwy urządzenia to 64 znaki.
4. Potwierdzić wykonanie operacji kodem PIN lub zabezpieczeniem biometrycznym (zależnie od ustawionej opcji).

III ZARZĄDZANIE PRZEGLĄDARKAMI OZNACZONYMI JAKO ZAUFANE

III.1. O zarządzaniu przeglądarkami oznaczonymi jako zaufane

Aplikacja dostępna pod adresem identity.kdpw.pl wykorzystywana jest do zarządzania przeglądarkami i urządzeniami zaufanymi, stanowiącymi drugi czynnik w procesie uwierzytelniania do konta dostępowego, które umożliwia korzystanie z aplikacji internetowych KDPW.

Urządzenie uwierzytelniające jest to urządzenie mobilne, na którym zainstalowana i skonfigurowana została aplikacja KDPW Group Authenticator. Takie urządzenie wraz z aplikacją służą do potwierdzania operacji logowania do konta dostępowego KDPW oraz potwierdzania wykonania wybranych operacji w aplikacjach KDPW.

Zaufane przeglądarki są to przeglądarki internetowe zarejestrowane przez posiadacza konta dostępowego jako zaufane i pozostające pod jego kontrolą. Użycie zaufanej przeglądarki stanowi dodatkowy czynnik uwierzytelniania w procesie potwierdzenia operacji logowania do konta dostępowego KDPW. Rejestracja przeglądarki jako zaufanej możliwa jest jedynie po uwierzytelnieniu do konta dostępowego z wykorzystaniem urządzenia uwierzytelniającego.

Aplikacja do zarządzania przeglądarkami oznaczonymi jako zaufane dostępna jest pod adresem https://identity.kdpw.pl, a dostęp do niej odbywa się z wykorzystaniem konta dostępowego do usług KDPW.

Dostęp do aplikacji do zarządzania przeglądarkami oznaczonymi jako zaufane wymaga użycia dodatkowego mechanizmu uwierzytelnienia, jakim jest potwierdzenie operacji logowania z wykorzystaniem aplikacji mobilnej KDPW Group Authenticator. Jeśli użytkownik nie posiada skonfigurowanego urządzenia uwierzytelniającego skojarzonego z kontem dostępowym, niezbędne jest wcześniejsze pobranie i skonfigurowanie aplikacji KDPW Group Authenticator.

W aplikacji do zarządzania przeglądarkami oznaczonymi jako zaufane prezentowane są informacje związane z zaufanymi i skojarzonymi z danym kontem dostępowym urządzeniami, zapewniającymi dodatkowy mechanizm uwierzytelniania do konta dostępowego. Na odrębnych zakładkach prezentowana jest lista zaufanych przeglądarek oraz urządzeń uwierzytelniających.

Przeglądarki opisywane są przez zestaw atrybutów pozwalających na ich identyfikację oraz weryfikację jako zaufane. W skład zbioru atrybutów wchodzą:

- Nazwa przeglądarki definiowalna przez użytkownika
- Typ przeglądarki
- Data i godzina dodania do konta przeglądarki jako zaufanej
- Data i godzina oraz Adres IP ostatniego użycia

Urządzenia uwierzytelniające opisywane są przez następujące atrybuty:

- Nazwa urządzenia definiowalna przez użytkownika z poziomu aplikacji mobilnej KDPW Group Authenticator
- Identyfikator instancji aplikacji
- Data i godzina dodania urządzenia do konta dostępowego
- Data i godzina ostatniego użycia

III.2. Żeby wyświetlić rejestr zdarzeń skojarzonych z danym urządzeniem/przeglądarką należy:

1. Przejść do właściwej zakładki aplikacji do zarządzania przeglądarkami oznaczonymi jako zaufane dostępnej pod adresem https://identity.kdpw.pl w zależności od tego czy rejestr zdarzeń ma dotyczyć urządzenia uwierzytelniającego czy zaufanej przeglądarki.
2. Odszukać właściwe urządzenie/przeglądarkę z wyświetlonej listy, mając na uwadze, że lista może zawierać wiele pozycji.
3. Wybrać opcję „Rejestr zdarzeń” dostępną w formie przycisku dla danej pozycji na liście, zlokalizowanego po prawej stronie. Okno rejestru zdarzeń zwiera:
   - informacje o urządzeniu (nazwa, identyfikator) / przeglądarce (nazwa, typ),
   - opcje sortowania oraz filtrowania listy (sortowanie możliwe jest jedynie po dacie i godzinie),
   - listę zdarzeń,
   - przyciski stronicowania wyników.

III.3. Żeby usunąć zarejestrowane urządzenie lub przeglądarkę zaufaną należy:

1. Przejść do właściwej zakładki aplikacji do zarządzania przeglądarkami oznaczonymi jako zaufane dostępnej pod adresem https://identity.kdpw.pl w zależności od tego czy operacja usuwania ma dotyczyć urządzenia uwierzytelniającego czy zaufanej przeglądarki.
2. Odszukać właściwe urządzenie/przeglądarkę z wyświetlonej listy, mając na uwadze, że lista może zawierać wiele pozycji.
3. Wybrać opcję „Usuń" dostępną w formie przycisku dla danej pozycji na liście, zlokalizowanego po prawej stronie.
4. Potwierdzić operację usunięcia klikając przycisk „Usuń urządzenie" lub „Usuń przeglądarkę". W przypadku rezygnacji należy wybrać opcję „Anuluj".

III.4. Żeby zmienić nazwę przeglądarki należy:

1. Przejść do zakładki „Zaufane przeglądarki" aplikacji do zarządzania przeglądarkami oznaczonymi jako zaufane dostępnej pod adresem https://identity.kdpw.pl.
2. Odszukać właściwą przeglądarkę z wyświetlonej listy, mając na uwadze, że lista może zawierać wiele pozycji.
3. Wybrać opcję „Zmień nazwę" dostępną w formie przycisku dla danej pozycji na liście, zlokalizowanego po prawej stronie.
4. Wprowadzić własną nazwę w polu „Nowa nazwa przeglądarki". Po zatwierdzeniu, nazwa ta będzie prezentowana na liście zaufanych przeglądarek pozwalając lepiej zidentyfikować daną pozycję.
5. Potwierdzić operację klikając przycisk „Zapisz". W przypadku rezygnacji należy wybrać opcję „Anuluj".