USER'S MANUAL: ACCESS ACCOUNT FOR KDPW GROUP ONLINE APPLICATIONS

TABLE OF CONTENTS

I OPENING AN ACCESS ACCOUNT 2

I.1. ABOUT ACCESS ACCOUNTS 2

I.2. TO OPEN AN ACCESS ACCOUNT: 2

I.3. TO LOG IN A KDPW APPLICATION USING AN EXISTING ACCESS ACCOUNT: 2

I.4. TO RECOVER ACCESS TO YOUR ACCOUNT IN CASE OF PASSWORD LOSS OR TO CHANGE THE PASSWORD TO YOUR ACCESS ACCOUNT: 3

I.5. TO LOG OUT OF THE KDPW APPLICATION: 3

II KDPW GROUP AUTHENTICATOR MOBILE APPLICATION 3

II.1. ABOUT THE APPLICATION 3

II.2. TO INSTALL THE KDPW GROUP AUTHENTICATOR MOBILE APPLICATION: 3

II.3. TO LINK AN ADDITIONAL ACCESS ACCOUNT WITH THE KDPW GROUP AUTHENTICATOR MOBILE APPLICATION: 4

II.4. TO DELETE AN ACCESS ACCOUNT LINKED TO KDPW GROUP AUTHENTICATOR MOBILE APPLICATION: 4

II.5. TO PROTECT THE KDPW GROUP AUTHENTICATOR APPLICATION AGAINST UNAUTHORISED USE: . 4

II.6. TO UNLOCK THE KDPW GROUP AUTHENTICATOR APPLICATION: 5

II.7. TO CHANGE YOUR PIN: 5

II.8. TO ENABLE OR DISABLE BIOMETRIC SECURITY FEATURES: 5

II.9. TO CONFIRM/REJECT AN OPERATION USING THE KDPW GROUP AUTHENTICATOR MOBILE APPLICATION: 5

II.10.TO RENAME A DEVICE: 6

III MANAGING TRUSTED BROWSERS 6

III.1. ABOUT MANAGING TRUSTED BROWSERS 6

III.2. TO VIEW THE LOG OF EVENTS ASSOCIATED WITH A PARTICULAR DEVICE/BROWSER: 7

III.3. TO DELETE A REGISTERED DEVICE OR A TRUSTED BROWSER: 7

III.4. TO CHANGE THE BROWSER NAME: 7

I OPENING AN ACCESS ACCOUNT

I.1. About access accounts

In order to use web applications for electronic communication with KDPW, users must use HTML5 compatible browsers with JavaScript and Cookies enabled. Internet Explorer is not supported; to use the application, we recommend that you do not use Internet Explorer regardless of its current version.

Opening an access account is necessary to use the application in both production and test environments. Opening an account is free of charge.

An access account allows access to all KDPW Group applications to which the account holder has previously been granted access. Authentication to a given access account allows switching between applications without having to separately authenticate to each of them.

In the case of different access policies, in particular when switching between an application requiring only authentication with the basic mechanism (login and password) and an application requiring additional authentication using a trusted device and the KDPW Group Authenticator mobile application, the user may be requested to authenticate again.

I.2. To open an access account:

1. On the login page for the selected service, select "Zarejestruj się teraz" (Register now).
2. Enter your e-mail address. The address will be the access account identifier (login). Once the account is opened, it is not possible to change the identifier, which means that changing your email address will require you to create a new access account.
3. Confirm access to the e-mail address which is the account identifier. To do this, use the "Prześlij mi kod weryfikacyjny" (Send a verification code) button. A code will be sent to the e-mail address, which is the account identifier. Enter the code in the application form and click "Zweryfikuj kod" (Confirm code).

If you do not receive the verification code, please check your Spam folder. You can also ask for the code to be resent by clicking the button "Wyślij nowy kod" (Send new code).

4. Enter an access password created according to the instructions given on the form and enter your first name and surname.
5. Accept the processing of personal data and confirm that you have read the information notice regarding the processing of personal data by KDPW. It is not possible to open an account without completing these steps.
6. Open an account by clicking the button "Utwórz" (Create). The opening of the account is confirmed by redirection to the login page. The account opening process can be cancelled by clicking the button "Anuluj" (Cancel).

I.3. To log in a KDPW application using an existing access account:

1. Enter the account user identifier which is the e-mail address provided when opening the account and enter the password for the access account into the form on the KDPW application page.
2. In the case of applications made available within the Services Portal online.kdpw.pl, confirm the operation using the KDPW Group Authenticator mobile application. The application should be installed and configured with the access account used in the login process.

3. Alternatively, designate the browser used in the login process as a trusted browser using the application available at https://identity.kdpw.pl. Each subsequent login on a computer or mobile device using the browser which has been designated as trusted does not require authentication using the KDPW Group Authenticator mobile application. Such a decision should only be made in relation to browsers on a computer under the user's control whose security the user trusts. Browsers designated as trusted can be managed in the application available at https://identity.kdpw.pl.

I.4. To recover access to your account in case of password loss or to change the password to your access account:

1. Click the button "Nie pamiętasz hasła?" (Forgot your password?).
2. Enter your account user identifier which is the email address provided when opening the account.
3. Confirm access to the e-mail address which is the account identifier. To do this, click the button "Prześlij mi kod weryfikacyjny" (Send a verification code) and a code to be entered in the application form will be sent to the e-mail address which is the account identifier. Next, click "Zweryfikuj kod" (Confirm code).
4. If you do not receive the verification code, please check your Spam folder. You can also ask for the code to be resent by clicking the button "Wyślij nowy kod" (Send new code).
5. Enter and confirm your new password.

I.5. To log out of the KDPW application:

1. Click the button "Wyloguj" (Logout) at the top right of the screen.

If the wrong browser is used, the button "Wyloguj" (Logout) may not be visible.

II KDPW GROUP AUTHENTICATOR MOBILE APPLICATION

II.1. About the application

The KDPW Group Authenticator mobile application ("mobile application" or "application") is used to securely confirm the authentication process of users to the access account defined in KDPW and to confirm the execution of selected operations.

To use the mobile application, you need to have a mobile device with the Google (Android) or Apple (iOS) operating system. In case of the Android system, the lowest supported system version is 6.0 (Marshmallow). For iOS, the lowest supported version is 12.1. Devices on which the application is to be installed must have their security features intact.

The application for those systems is available in authorised stores for the respective operating systems:

- Application for Android in the Google Play store (it is necessary to have a Google account to download the application),
- Application for iOS in the Apple App Store.

II.2. To install the KDPW Group Authenticator mobile application:

1. Download the application to the mobile device from the store depending on the device's operating system (Android or iOS). The application can only be installed from an authorised store for the respective system.

2. Launch the application and select the option “Rozpocznij rejestrację urządzenia” (Start device registration) on the welcome screen of the application. Next, select the option “Zaloguj się w KDPW” (Log in to KDPW). It will redirect you to the KDPW access account login page.
3. Authenticate (enter the ID and password) to the access account which is to be linked to the device and the KDPW Group Authenticator mobile application to be installed on it. The access account must have been previously created. After successfully logging in, a verification code will be sent to the e-mail address provided as the access account identifier. The verification code will be sent from the address noreply@kdpw.pl. If the message does not appear in your inbox within a few minutes, please check your Spam folder.
4. Confirm that the access account is to be linked to the device by entering the code in the field “Kod weryfikacyjny” (Verification code) and clicking the button “Potwierdź” (Confirm).
5. Configure the security features of the application and agree to receive notifications. In the security configuration, set a PIN and activate biometric security features as required. The security features will be used to authenticate the user when confirming operations using the KDPW Group Authenticator mobile application.

II.3. To link an additional access account with the KDPW Group Authenticator mobile application:

1. Select the option “Dodaj nowe konto” (Add new account) on the mobile application settings screen. The application will redirect you to the KDPW website where you can authenticate to your access account.
2. Authenticate (enter the ID and password) to the access account which is to be linked to the device and the KDPW Group Authenticator mobile application to be installed on it. The access account must have been previously created. After successfully logging in, a verification code will be sent to the e-mail address provided as the access account identifier. The verification code will be sent from the address noreply@kdpw.pl. If the message does not appear in your inbox within a few minutes, please check your Spam folder.
3. Confirm that the access account is to be linked to the device by entering the code in the field “Kod weryfikacyjny” (Verification code) and then click the button “Potwierdź” (Confirm).
4. Confirm the operation with your PIN or biometrics depending on the type of security features set in the mobile application.

II.4. To delete an access account linked to KDPW Group Authenticator mobile application:

1. On the application screen, in the tab “Ustawienia” (Settings) in the section “Konta” (Accounts), select the option to delete the account (trash bin icon) next to the relevant access account.
2. Confirm the deletion with your PIN or biometrics depending on the type of security features set in the mobile application. If the account to be deleted is the last account in the application, the application will reset to the after-installation status and the welcome screen will be displayed.

II.5. To protect the KDPW Group Authenticator application against unauthorised use:

1. The application will be locked if an incorrect PIN code is entered 5 times in a row. The locked application will notify the user with a dedicated message.
2. When the device is locked, a lock message is sent to the email addresses of the access accounts linked with the device. The message will be sent from the address noreply@kdpw.pl. If the message does not appear in your inbox within a few minutes, please check your Spam folder.

II.6. To unlock the KDPW Group Authenticator application:

1. On the application screen, select the tab “Ustawienia” (Settings) and click the option “Odblokuj aplikację” (Unlock app) in the section “Bezpieczeństwo” (Security).
2. Select the account to be used in the unlocking process. The option will redirect to the KDPW access account login page.
3. Authenticate (enter the ID and password) to the access account. After successfully logging in, a verification code will be sent to the e-mail address provided as the access account identifier. The verification code will be sent from the address noreply@kdpw.pl. If the message does not appear in your inbox within a few minutes, please check your Spam folder.
4. Confirm the unlocking operation by entering the code in the field “Kod weryfikacyjny” (Verification code) and then click the button “Potwierdź” (Confirm).
5. Reset the PIN. The unlock process will automatically disable biometrics if previously enabled. If the user intends to use biometrics, it is necessary to enable this option in the application settings.

II.7. To change your PIN:

1. Select the option “Zmień kod PIN” (Change PIN) available on the mobile application settings screen in the section “Bezpieczeństwo” (Security).
2. Enter the current PIN in the section “Obecny kod PIN” (Current PIN) and enter a new PIN in the section “Nowy kod PIN” (New PIN). The new PIN must be entered twice to ensure the correctness of the entered values, and it can only be set if the two values match.

   To change the PIN without entering the current PIN, uninstall and reinstall the application.
3. Confirm the change by clicking the button “Ustaw PIN” (Set PIN). The change will be confirmed by a dedicated message. Once the change has been made, biometrics will automatically be disabled if previously enabled. If the user intends to use biometrics, it is necessary to enable this option in the application settings.

II.8. To enable or disable biometric security features:

1. Touch the switch “Zabezpieczenia biometryczne” (Biometric security) located on the application settings screen in the section “Bezpieczeństwo” (Security). If the switch is grey, biometric security is disabled, otherwise it is active.
2. To disable biometrics, you are not required to make any additional confirmation. After biometrics has been disabled, a valid PIN is required to confirm operations.
3. To enable biometric security, you need to enter the PIN which has been set in the application. Once biometrics is enabled, all operations will be confirmed using biometrics and PIN entry will not be required.

II.9. To confirm/reject an operation using the KDPW Group Authenticator mobile application:

1. Select the relevant notification in the notification screen in the application. If you don’t see the notification you want, you can refresh the screen by touching it and then dragging your finger down. You can also select the relevant notification from the list of notifications available in your phone’s operating system. Selecting the notification will take you to the screen “Potwierdzenie operacji” (Operation confirmation).

2. Make sure that the notification is correct by checking its content and the date it was generated. Each notification has a specific validity period presented on the screen. Once the time limit for confirmation has been exceeded, it will no longer be possible.
3. Confirm/reject the operation by clicking the appropriate button for the selected notification and then confirm by entering the PIN or using biometric security (depending on the settings).

II.10. To rename a device:

1. Go to the settings screen in the mobile application and go to the section "Nazwa urządzenia" (Device name). This section shows the name by which the device is identified in KDPW services. If no device name has been set, the factory name of the device is used.
2. Select the option "Zmień nazwę urządzenia" (Rename device).
3. Enter the new device name and confirm by clicking "Zmień" (Change). A device name can only contain letters, digits, spaces, and dashes (-). The maximum length of a device name is 64 characters.
4. Confirm the operation with the PIN or using biometric security (depending on the settings).

III MANAGING TRUSTED BROWSERS

III.1. About managing trusted browsers

The application available at identity.kdpw.pl is used to manage browsers and trusted devices which are the second authentication factor for an access account used with KDPW web applications.

An authentication device is a mobile device on which the KDPW Group Authenticator application has been installed and configured. Together with the application, the device is used to confirm logging in to a KDPW access account and to confirm the execution of selected operations in KDPW applications.

Trusted browsers are web browsers designated by the access account holder as trusted browsers which are under the user's control. A trusted browser is an additional authentication factor in the confirmation process of logging in the KDPW access account. A browser can only be designated as trusted after authentication to the access account using an authentication device.

The application for managing browsers designated as trusted is available at https://identity.kdpw.pl and can be accessed using a KDPW services access account.

Access to the application for managing browsers designated as trusted requires an additional authentication factor: the confirmation of the login using the KDPW Group Authenticator mobile application. If the user does not have a configured authentication device linked with the access account, it is necessary to download and configure the KDPW Group Authenticator application first.

The application for managing browsers designated as trusted presents information concerning trusted devices linked with a given access account which provide an additional authentication factor for the access account. A list of trusted browsers and authentication devices is presented in separate tabs.

Browsers are described by a set of attributes which allow them to be identified and verified as trusted. The set of attributes includes:

- Browser name defined by the user
- Type of browser
- Date and time when the browser was added as trusted
- Date and time and IP address of last use

Authentication devices are described by the following attributes:

- Device name defined by the user in the KDPW Group Authenticator mobile application
- Application instance identifier
- Date and time the device was added to the access account
- Date and time of last use

III.2. To view the log of events associated with a particular device/browser:

1. Go to the appropriate tab of the application for managing browsers designated as trusted, available at https://identity.kdpw.pl, depending on whether the event log is for an authentication device or a trusted browser.
2. Locate the correct device/browser from the list, bearing in mind that the list may contain multiple entries.
3. Select the option "Rejestr zdarzeń" (Event log) available as a button for a given item on the list, located on the right side. The event log window contains:
   - device information (name, identifier) / browser information (name, type),
   - sorting and filtering options for the list (sorting is only possible by date and time),
   - event list,
   - buttons for paging the results.

III.3. To delete a registered device or a trusted browser:

1. Go to the appropriate tab of the application for managing browsers designated as trusted, available at https://identity.kdpw.pl, depending on whether you want to delete an authentication device or a trusted browser.
2. Locate the correct device/browser from the list, bearing in mind that the list may contain multiple entries.
3. Select the option "Usuń" (Delete) available as a button for a given item on the list, located on the right side.
4. Confirm the deletion by clicking "Usuń urządzenie" (Delete device) or "Usuń przeglądarkę" (Delete browser). To cancel, select "Anuluj" (Cancel).

III.4. To change the browser name:

1. Go to the tab "Zaufane przeglądarki" (Trusted browsers) in the application for managing browsers designated as trusted available at https://identity.kdpw.pl.
2. Locate the correct browser from the list, bearing in mind that the list may contain multiple entries.
3. Select the option "Zmień nazwę" (Rename) available as a button for a given item on the list, located on the right side.
4. Enter a name in the field "Nowa nazwa przeglądarki" (New browser name). Once confirmed, the name will be displayed in the list of trusted browsers to better identify it.
5. Confirm by clicking "Zapisz" (Save). To cancel, select "Anuluj" (Cancel).