



Bank Polski

iPKO biznes –
ADMINISTRATOR'S GUIDE

Table of contents

Glossary.....	4
General Assumptions.....	5
System Login.....	6
First Login.....	6
Subsequent Login.....	9
Safe System Login.....	11
Context parameters.....	12
Setting context parameters.....	12
Accounts.....	12
Creating Account Authorization Patterns.....	12
Allocation of account authorization pattern.....	16
Group allocation to accounts.....	16
Single allocation to accounts.....	16
Group allocation to users.....	16
Single allocation to users.....	16
Creation of transaction signing pattern.....	16
Allocation of the Transaction signing pattern to accounts.....	16
Group allocation of the Transaction signing pattern to accounts.....	16
Single allocation of the Transaction Signing pattern to the account.....	17
Liquidity management.....	17
Naming of individual accounts.....	18
Services.....	18
Creating the Services patterns.....	20
Allocation of the Services patterns to users.....	22
Group allocation of the Services patterns to users.....	22
Single allocation of the Services patterns to the user.....	23
Users.....	18
Creation of Signature Classes.....	18
Allocation of Signature Classes to Users.....	19
Group allocation of Signature Classes to Users.....	19
Single allocation of Signature Classes to the User.....	20
Access restrictions.....	23
Access restricted to indicated computer IP addresses.....	23
Access management in predefined time frames.....	26
Limiting access to the iPKO biznes system via mobile application.....	27
Account Grouping.....	28
Creation of account groups.....	28
Allocation of accounts to groups.....	29
Account Grouping for Liquidity Management purposes.....	30

Defined Format Management.....	30
Format definition – template common fields.....	32
File Structure Setting.....	33
Format definition – fields typical for SPLIT and Tax Authorities.....	34
Operation title – SPLIT/Tax Office – floating-point formats.....	35
Operation title – SPLIT/Tax Authorities – fixed-point formats.....	35
Format definition – fields typical for the foreign transfer order.....	36
Whitelists.....	37
Creation of the white list.....	37
Allocation of the created white list to the accounts.....	38
Statement of accounts.....	39
Change of the content of the white list.....	39
Deletion of the white list.....	40
Transactional limits.....	41
Activation of limits.....	42
Change of user limits.....	42
Details of user limits.....	43
Group modification of user limits.....	44
Use of all of the available limit.....	44
Access channels and tokens.....	44
External Channels.....	46
List of accounts.....	47
Third Party Providers.....	48
List of CAF consents.....	49
List of AIS consents.....	49
Authorisation of changes.....	50
Temporary setup.....	50
iPKO biznes parameters setting by the Bank.....	53
Security.....	54
Internet Browser and Passwords.....	54
Secure logging (page address and certificate).....	54
Antivirus Software and E-mail Security.....	55
Firewall.....	55
E-mail Security.....	55
Prevention.....	55
Support for iPKO biznes System Users.....	56

Glossary

Client – an entity that has concluded an electronic banking service agreement with the Bank.

User – a proxy entitled to use electronic banking services, i.e. a person indicated by the Account Holder, entitled to access and use the accounts in the configuration specified by the Account Holder.

Administrator – a User acting on behalf of the Account Holder that manages the authorizations of Users granted by the Account Holder, or, if PKO Bank Polski SA is entrusted with the function of setting parameters for the authorizations of the Users indicated by the Account Holder – a User indicated by the Account Holder with the authorization to view context data,

Context – a set of accounts and the list of Users authorized to use those accounts in iPKO biznes,

Glossary Data – the data configured by the Administrator, defining relationships in the iPKO biznes system, namely: signature classes, account authorization patterns, services authorization patterns, transaction signing patterns.

Account patterns – a pattern with the list of account authorizations defined in the system. The Administrator may either create its own account authorization pattern or use the default authorization pattern on the website: full access, author, approver, view.

Services patterns – a pattern with the list of services authorization defined in the system. The Administrator may create its own services authorization pattern.

Signature Class – signature classes form the basis of the transaction signing pattern. There are four default signature classes on the website: Head, Manager, Accountant and President. It is also possible to create own signature classes. The signature classes are assigned to users.

Transaction Signing pattern – a pattern that allows to define what users, in what relationships and to what amount can authorize transactions in the account to which the transaction signing pattern is assigned.

General Assumptions

To be able to use the iPKO biznes electronic banking, it is required to:

- Sign the current/auxiliary account agreement.
- Sign the “iPKO biznes application” form.
- Have the “Identification Cards” signed by the Users who have not been using the Bank services so far.
- Collect the authentication tools and sign the “Tools Receipt Confirmation”.
- Remember the User ID,
- Have the access configured by the person indicated by the Account Holder as the Administrator (without system configuration, after logging into the system the Users will not be able to access the accounts), and at the request of the Account Holder, the Bank may assume the function of managing the rights of the Users and setting parameters of the iPKO biznes system, including the first setting of the system parameters. For the Bank to assume the function of parameters setting, a relevant form must be submitted to the Bank.

The Account Holder must indicate at least one User who will have the rights of the Administrator in the iPKO biznes system. If the access is configured and the rights are managed by the Bank, the Administrator representing of the company will have access to the context data only.

The tasks of the Administrator include:

- (optional – there are default tasks available) Creation of Signature Classes.
- (optional – there are default tasks available) Creation of specific account authorization pattern.
- Creation of specific Services patterns.
- Creation of Transaction signing patterns.
- Allocation of Signature Classes and Authorization Service Patterns to the Users.
- Allocation of Transaction Signing patterns to accounts and account authorization pattern to the Users.
- Allocation of Transaction Signing patterns to Services.
- (optional) activation of the service of waiting for funds,
- (optional) assigning names of accounts and setting sorting patterns,
- (optional) setting parameters of access restrictions to the iPKO biznes system, if necessary.

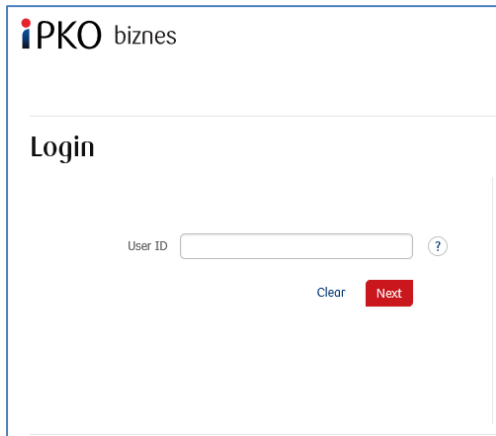
If all the above-mentioned activities are performed, other Users will be able to use the iPKO biznes system. To be able to commence the access configuration, the Administrator must log into the iPKO biznes system.

System Login

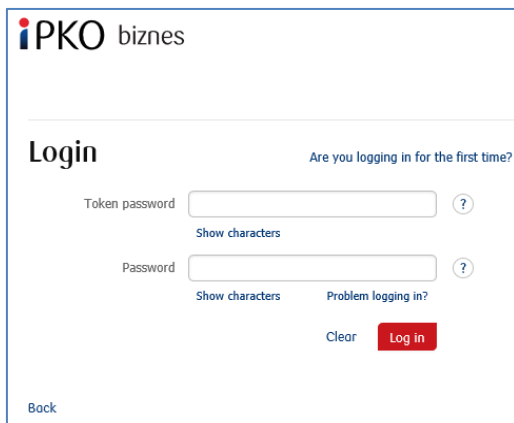
First Login

To use the iPKO biznes, enter the following address in the Internet browser: www.ipkobiznes.pl.

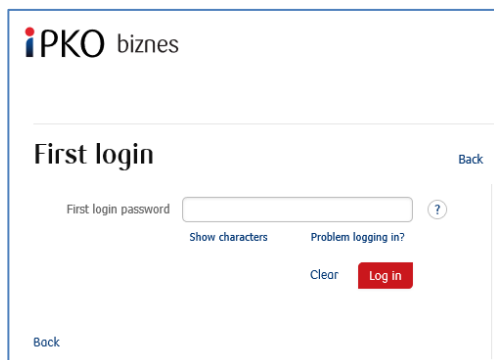
In the **User Id** field, enter the number given by the Bank employee and then select **Next**.



Once a valid User ID is entered, you will be taken to the next screen of the logon process. Select the link: [Are you logging in for the first time?](#)

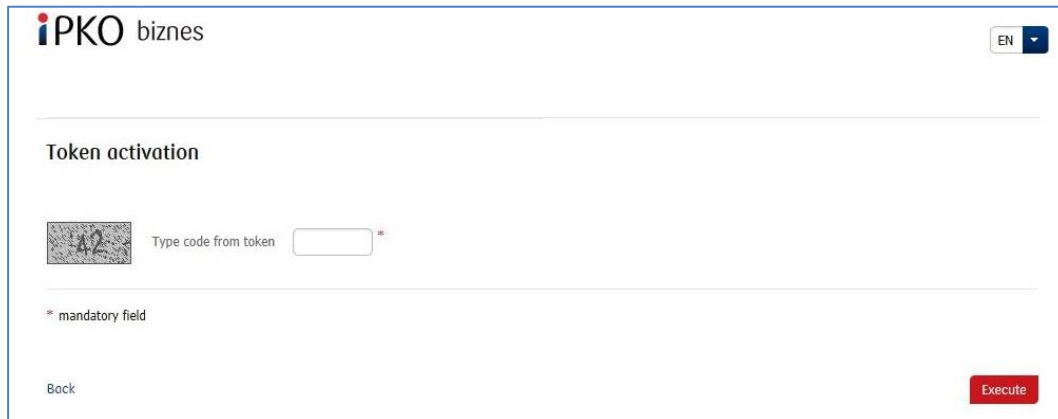


The **First Login** screen will be displayed.

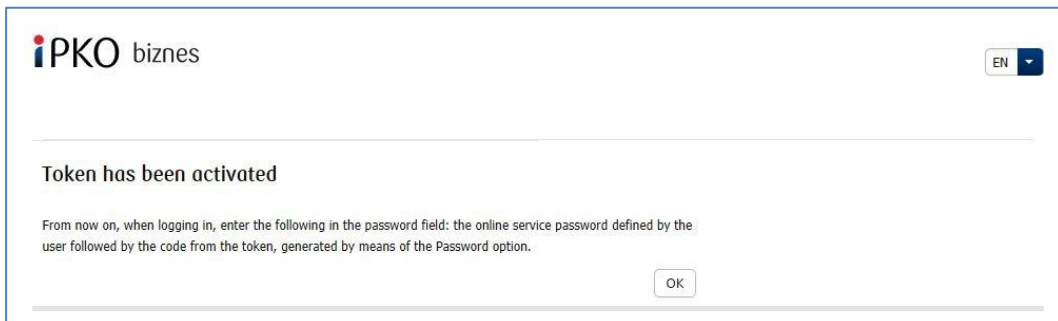


In the **First Login** field enter the first system logon password (access password) provided by the Bank employee or sent by SMS and then access by clicking **Log in**.

After the **Log in** button is clicked, you will be asked to activate the token. Enter the token response for a given operation code and click **Execute**.



You will receive confirmation of the token activation.



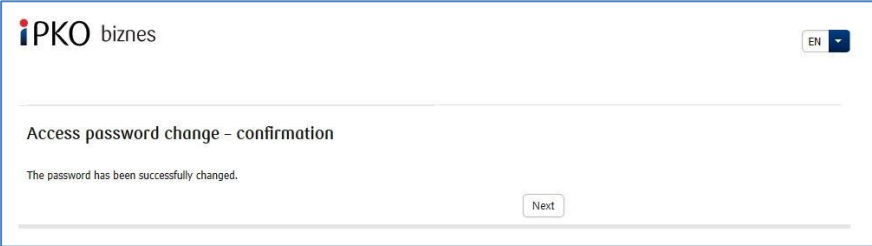
Click **OK**, and you will be moved to the **access password** change screen.



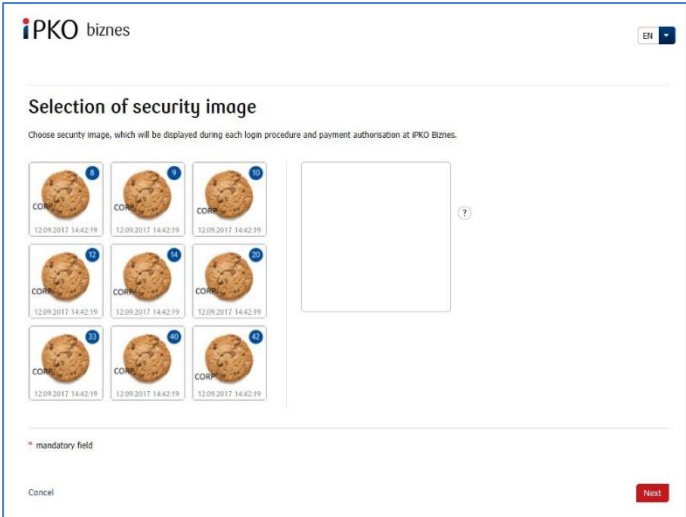
Fill in the following fields on the **Access password change** screen:

- **First login password** – repeat the first system logon password (access password) provided by the Bank employee or sent in the form of SMS to your mobile phone number.
- **New password** – enter the password selected by you. The password shall contain 8 to 16 alphanumeric characters (digits and/or letters and special characters: `!@#\$\$%^&*()_+={}|:;',.<>?`). The password cannot contain Polish letters (e.g. "ł", "ś"). Remember that password is case sensitive.
- **Retype password** – repeat the password selected by you.

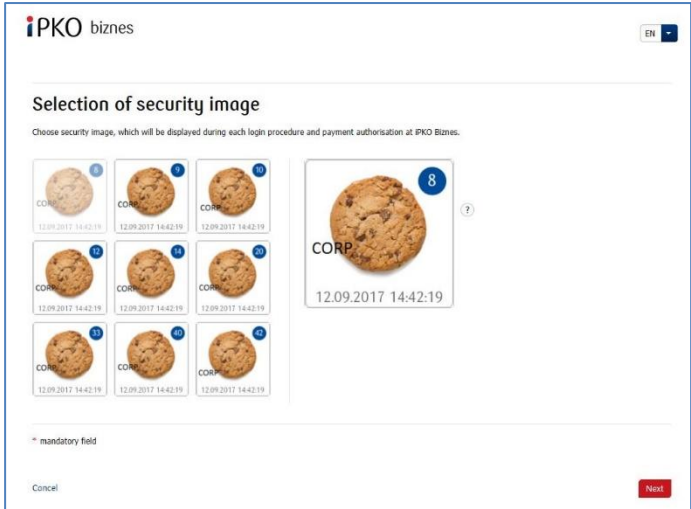
Once the correct data is entered and the **Log in** button is clicked, you will receive the access password change confirmation.



Once you click the **Next** button, a screen will appear where you will be prompted to select a **Security Image** (this document contains examples of images. REMEMBER! Images are unique and will not repeat on the website).



Select the image on this screen by clicking the selected item (this document contains examples of images. REMEMBER! Images are unique and will not repeat on the website) and then click **Next**.



NOTE! During the selection of the image the system does not ask for any code from the authentication tool. Please remember your image – from that moment it will be displayed whenever you log in and authorize access to the iPKO biznes website.

When the previous step is confirmed by clicking **Next**, you will be moved to the security image confirmation screen. Click **Next** to finally approve the selection and be able to use the website.



- the security image will be displayed during each subsequent system logon and authorisation – check every time whether the image displayed corresponds to the image selected by you and whether there is date and time displayed that correspond to the current data in the following format: DD.MM.YYYY (day.month.year) HH: MM: SS (hour.minute.second), e.g. 01.01.2016 23:59:59,
- you can change the image at any time. To change it log into new website of iPKO biznes, select “Settings” tab and then “Access Channels” and “Security Image”. To change the image, you must **provide** the code from the authentication tool,
- the presentation of the security image does not apply to the iPKO biznes mobile website and the “old” version of the iPKO biznes website.

Note!

If, when logging into the website, you have any doubts as to your image or the data presented (date and time displayed on the image are not consistent with current data), stop the logon process or authorisation immediately and contact the Corporate Customer Service Centre. Consultants are available at: +48 61 855 94 94 or 801 36 36 36 (charged according to the operator's tariff). The helpline is available from Monday to Friday, from 8:00 a.m. to 6:00 p.m.; e-mail: ipkobiznes@pkobp.pl.

NOTE! User ID and password are also used to activate the phone service. To activate the service, call the HELPLINE.

Subsequent Login

The screen and the logon process will be as follows:

Step 1. Enter the User ID at www.ipkobiznes.pl. This screen changes because it will contain only one mandatory field, i.e. the field for entering the User ID. Enter the User ID in the field and then click **Next**.

iPKO biznes

Login

User ID ?

Clear

Step 2. Logging after selecting the security image. The first step (and screen) of the logon process does not change. The second screen presents the image selected by you above the field for entering the Token Password and the Password. Then, after you are moved to the next screen, check whether the image displayed corresponds to the image selected by you when logging into the new website for the first time. After entering data in the Token Password and Password fields, click **Log in**.

Login ? Are you logging in for the first time?

Security image

Token password ?

Show characters

Password ?

Show characters Problem logging in?

Clear

Back

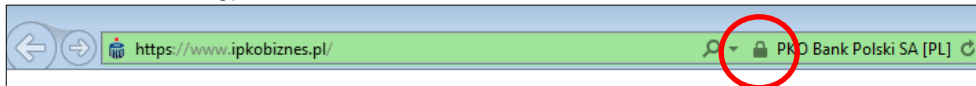
Safe System Login

1. Always enter the Bank's website address manually.

2. Check whether the website's address in the browser window is as follows: <https://www.ipkobiznes.pl>

3. Check whether there is a closed padlock icon somewhere within the browser window.

Depending on the browser, the icon may appear in the address bar or in the status bar in the bottom of the screen. The padlock icon indicates that the webpage is protected by the security certificate and the connection is encrypted.



4. Check whether the security certificate is correct. The certificate data are available in the browser, usually under “Properties” option in the “File” menu. After clicking the “Certificates” button, check both “General” and “Certification path” option.

To access the certificate data, you can also double click the padlock icon. After clicking it, you will see certificate details indicating that it has been issued for <https://www.ipkobiznes.pl> domain.

You can also learn from them that the certificate has been purchased by PKO Bank Polski.

5. When logging into the Bank's website, never use links of unknown origin, included in e-mails and SMS messages, or on websites which are not owned by the Bank.

6. Do not share your login data (client number, access passwords) with other persons, do not share them at the request of third parties.

7. Verify the information presented by the Bank regarding the date and time of the last correct login and the last failed login attempt – if any inaccuracies are identified, report it.

If the appearance of the logon page seems suspicious to you, BEFORE YOU LOG IN, contact the helpline at **801 36 36 36** (toll free for national calls, other calls charged according to the operator's tariff) or **+48 61 855 94 94** (for international and mobile calls; calls charged according to the operator's tariff).

Context parameters

Setting context parameters

When selecting the Administration link (right upper corner of the main menu), the Administrator is able to configure the context parameters such as, among others: Context name, Duplicate verification, Lock on modification of operations from file, Checksum verification, Session duration, Accounts sort order.

Company name: DPT CORPORATION
DPT CORPORATION

User name: MARCIN MOBILNY
User ID: 2507622

Messages 1 Settings Administration

Time remaining to session timeout: 25:22

Transactions Accounts Cards Loans & deposits Cash Analysis Applications e-Gov EN

Administration / Context parameters Collapse My short-cuts

Context parameters Accounts Users Services Access restrictions New

Whitelists Transactional limits File formats Access channels and tokens External channels

Context parameters

[PDF Administrator's guide](#) [HTML Context configuration form](#)

Context name	DPT CORPORATION	User data	MARCIN MOBILNY
Context ID	67098	User ID	2507622
Company number	64931469	Signature class	PREZES

Context parameters

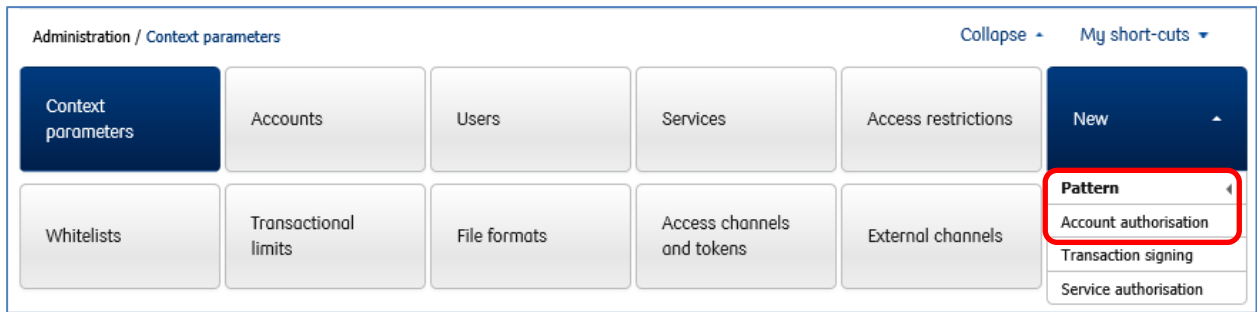
Awaiting funds availability	Inactive	Session duration	20 minutes
Execution of Split Payment despite insufficient funds in VAT account	Yes	Language version	PL – Polish version (default)
Duplicate verification	Inactive	Accounts sort order	Default (currency, type, account number)
Lock on modification of operations from file	Inactive	Access to context for external entities	Non-active
Checksum verification	Transactions - Inactive File exchange - Inactive		

Edit

Accounts

Creating Account Authorization Patterns

As a standard, in the iPKO biznes system there are four Account Authorization Patterns: Full Access, View, Creation, Sing-off. The Administrator can create their own account authorization patterns – to do so, the Administrator has to select the “New” tile and select the “Account Authorization” from a drop-down list. The “New account authorization pattern” will appear on the screen.



NOTE! The Operation Sign-off Pattern does not apply to the operation of creation, modification or termination of the term deposit. To perform these operations, the User must have the relevant authorization.

When defining a new Account authorization pattern, the Administrator should indicate the set of rights in iPKO biznes system that can be used by the User with a given pattern allocated to them.

Consequences of activation of individual functions in the Account authorization pattern:

Full access - checking of this field activates (check) all rights under all sections

Account details - checking of this field activates (check) all rights under the "Account Details" section.

Account Details - the User holding such a right has access to the account data: account name, account number, account interest rate, funds available, accounting balance and the frequency of statement generation (completion of the order) and the date of the next statement.

Book balance and funds available in account - the User holding such a right has access to information on the account balance and funds available.

Account History - the Client can view the history of the transactions selected for a given account and download a document with the transactions found as Excel, PDF and CSV files.

Statements, documents downloaded from the website - this function allows to order, download and print statements as PDF files. No special download rights are required to download the statements. The User will be able to download a summary with the data available to the User on the screen.

File reports - by checking this box, you can:

order and download standard, daily reports in MT940 (**NOTE!** In the reports generated in the MT940 format the Bank does not make available the regarding a given payment instruction including the amount of the original operation, the currency of the original operation, the exchange rate, the settlement amount and currency), Elixir and Kontakt format. The reports from the accounts linked to a loan present transactions for the period starting on 01.01.2018, provided that the reports are available from the date of making the account available in the iPKO biznes channel, which means that it is not possible to present reports for the period before the date of making the account available in the iPKO biznes system.

These reports facilitate cooperation with financial and accounting systems.

Sending of history by fax - relevant transactions found in the "Account History", can be sent one by one by fax or email. This function works only if the "Account History View" function is enabled.

Blocks in account - function available after selecting the "Account" menu, "Funds blocked" tile, "Funds not cleared" and "Seizures under legal processes" tab.

Search for transaction and bundles - allows to search for transactions and batches by set criteria and filters applied.

Term deposits - checking of this field activates (check) all rights under the "Term Deposits" section.

List of term deposits - this function allows to view deposits available within the context.

Details of term deposits – the User with the rights to view details of the deposit can obtain, inter alia, the following information: deposit account number and name, accounting balance, deposit duration, set-up and expiry date and interest rate of the deposit.

Deposit opening – The User with access to a given function is able to set up the deposit through the iPKObiznes system. Authorisation is not required to set up a deposit.

Modification of term deposit parameters and management of automatic deposit sessions – this function allows to change the method of managing interest or funds after the expiry of the deposit or to change the automated deposit session. Changes can be also made to the deposit renewal options. Authorisation is not required to change the deposit parameters.

Early withdrawal of term deposit – this function allows to withdraw funds from the deposit account before the end of the contractual period. As a result, the interest payable is lost either in whole or in part. Authorisation is not required to terminate the deposit.

Trusted counterparties (Payments) and standing orders – checking of this field activates (check) all the rights under the “Trusted counterparties and standing orders” section.

List of trusted beneficiaries (Payments) – the User with such rights can see the list of defined payments with the payment name, number of the debited account, details of the beneficiary and payment title. However, the User cannot modify, create or delete the payment.

Creation, modification and removal of trusted domestic counterparty – it requires sign-off and relevant rights to the account, from which the payment is defined, i.e. at least the following rights: “Payment creation, modification and removal” and “List of trusted beneficiaries”.

Creation, modification and removal of trusted tax-related counterparty – it requires sign-off and relevant rights to the account, from which the payment is defined, i.e. at least the following rights: “Payment creation, modification and removal” and “List of trusted beneficiaries”.

Creation, modification and removal of trusted Social Security Institution counterparty – it requires sign-off and relevant rights to the account, from which the payment is defined, i.e. at least the following rights: “Payment creation, modification and removal” and “List of trusted beneficiaries”.

Transfer order to trusted domestic counterparty (Payments) – the payment does **NOT REQUIRE** any sign-off, although relevant rights to the account are required, i.e. at least the following rights “Transfer order to trusted domestic counterparty (Payment)” and “List of trusted beneficiaries (Payment)”.

Transfer order to trusted tax-related counterparty (Payments) – the payment does **NOT REQUIRE** any sign-off, although relevant rights to the account are required, i.e. at least the following rights “Transfer order to trusted tax-related counterparty (Payment)” and “List of trusted beneficiaries (Payment)”.

Transfer order to trusted counterparty Social Security Institution (Payments) – the payment does **NOT REQUIRE** any sign-off, although relevant rights to the account are required, i.e. at least the following rights “Transfer order to trusted counterparty Social Security Institution (Payment)” and “List of trusted beneficiaries (Payment)”.

Transfer order to trusted foreign counterparty (Payments) – the payment does **NOT REQUIRE** any sign-off, although relevant rights to the account are required, i.e. at least the following rights “Transfer order to trusted foreign counterparty (Payment)” and “List of trusted beneficiaries (Payment)”.

NOTE! The transfer to a trusted counterparty is transfer to a counterparty where the accounts of the sender and receiver (trusted counterparty) are permanently defined. The authorization code is not required to make a transfer to the trusted counterparty.

List and details of standing orders – presents all standing orders defined in electronic access channels. The following information is presented in the list: date of the next payment, name and address of the counterparty, the number of the account from which the order is executed, the counterparty's account number, the type and parameters of the order and the amount and currency of the order. Additionally, in the

standing order “Details” function the following can be viewed: method of payment (regular or SORBNET) and the calendar (i.e. the date of the next payment, the method of payment and the order end date).

Creation, modification and removal of regular standing order – the creation, modification and removal of regular standing order requires the sign-off and relevant right to the account, i.e. at least the following: “List and details of standing orders” and “Creation, modification and removal of regular standing order”.

Creation, modification and removal of foreign standing order – the creation, modification and removal of foreign standing order requires the sign-off and relevant right to the account, i.e. at least the following: “List and details of standing orders” and “Creation, modification and removal of foreign standing order”.

Creation, modification and removal of Split standing order – the creation, modification and removal of Split standing order requires the sign-off and relevant right to the account, i.e. at least the following: “List and details of standing orders” and “Creation, modification and removal of Split standing order”.

Creation, modification and removal of tax-related standing order – the creation, modification and removal of tax-related standing order requires the sign-off and relevant authorization to the account, i.e. at least the following: “List and details of standing orders” and “Creation, modification and removal of tax-related standing order”.

Creation, modification and removal of standing order to Social Security Institution – the creation, modification and removal of standing order to Social Security Institution requires the sign-off and relevant authorization to the account, i.e. at least the following: “List and details of standing orders” and “Creation, modification and removal of standing order to Social Security Institution”.

Ordering of transaction – checking of this field activates (check) all authorizations under the “Transaction order” section.

One-time transfer order – an order to make a domestic, one-time transfer and a domestic bundle transfer,
Issue new split payment – the User can, depending on their set-up and signing authorization, place a Split payment.

Own account transfer order – it is a quick transfer of funds between own accounts held in PKO Bank Polski within one context.

Tax transfer order – the User can make a transfer to the Tax Authorities depending on their set-up and signing authorization.

Order of transfer to Social Security Institution – the User can make a transfer to Social Security Institution depending on their set-up and signing authorization.

Direct debit order – the User can define a direct debit order depending on their set-up and signing authorization.

Issue new split direct debit – the User can define a Split direct debit order depending on their Split transfer set-up and signing authorization.

Foreign transfer order – the User can, depending on their set-up and signing authorization, place a foreign transfer order (in a foreign currency or in PLN).

Creation, details, modification of a collective bundle – the User can set up bundles booked collectively and can view details of such bundle.

Release of authorized operations – the User can dispatch transactions or batches of transfers already authorized by the required persons.

Removal of non-authorized transaction and cancellation of pending ones – the function requires appropriate account authorizations, i.e. at least “Removal of non-authorized transaction and cancellation of pending ones” and “Searching for bundles and transactions”. By selecting the “Transactions” option in the top menu, the User may search on the list of transactions for the transactions with the following status “To be signed off, dispatched” or “Pending” and delete/cancel them.

A new Account authorization pattern will be added to the list of available Account Authorization Patterns.

Allocation of account authorization pattern

Allocation of account authorization pattern to the Users within the context. The pattern can be allocated in 4 ways:

Group allocation to accounts

Under “List of accounts” section (in the “Accounts” tile), indicate the accounts, use the Group functions option and then select “Modify authorization pattern” in the drop-down list and in the list provided below select the user and Account Authorization Patterns (“Selection of the authorization patterns” -> “Select pattern” from the drop-down list). The method allows to allocate the indicated account patterns to many accounts and users.

Single allocation to accounts

Under “List of accounts” section (in the “Accounts” tile) use the “Modify authorization pattern” function available next to every account and then in the next screen select the users and the Account Authorization Pattern. The method allows to allocate the authorization pattern to one account to many users.

Group allocation to users

Under “List of users” section (in the “User” tile), indicate the users by using the Group functions option and select “Change account authorization pattern” in the drop-down list. In the list below select the accounts and the authorization pattern. The method allows to allocate the indicated account patterns to many accounts and users.

Single allocation to users

Under “List of users” section (in the “Accounts” tile) use the “Details” function available next to every user. On the screen select the “Change account authorization pattern” function under group functions. The “Change account authorization pattern” webpage will be displayed where you can define the pattern of authorizations for the accounts which can be accessed by a given user. The method allows to allocate to one user the authorization pattern to many accounts.

Creation of transaction signing pattern

The Transaction signing pattern defined who and on what conditions can authorize a transaction/service ordered from a given account. The signature classes created earlier shall be used to create the Transaction signing pattern. For example: if 2 signatures of different classes are required in the Transaction signing pattern, then 1 signature of the Accountant class and 1 signature of the Head class is created. When defining the pattern, the Administrator can define additional rules for transaction limit authorization, for example - two signatures of, for example, Head class are required to authorize the transaction in the amount of up to PLN 1,000,000.

Allocation of the Transaction signing pattern to accounts


The created Transaction signing pattern shall be allocated to accounts/services. They shall be allocated under “Accounts” -> “List of accounts” or “Services” -> “List of services”. The Transaction Signing pattern can be allocated to accounts or services following either the procedure for group allocation or single allocation. Apart from a default pattern it is also possible to allocate a fixed pattern. It is pattern that will apply only in the defined period. After the end of that period, the default pattern will apply again.

Group allocation of the Transaction signing pattern to accounts

It is possible to allocate the Transaction signing pattern to several accounts at the same time. To allocate the same Transaction signing pattern to several or all accounts, on the “List of accounts” in the context check the accounts to which the same Transaction signing pattern is to be allocated. Then select the Group functions option, and select “Modify transaction signing pattern” from the drop-down list.

On the next screen, select from the drop-down list the Transaction Signing pattern that will apply to all accounts checked by you earlier within the context. It is also possible to allocate a fixed pattern.

Group modification of transaction signing pattern

 Administrator's guide

List of accounts

Account name	Account number	Transaction signing pattern	
		Default	Term
CURRENT ACCOUNT	15 1020 5561 0000 3902 0327 8843 PLN	1 reka	None
CURRENT ACCOUNT	60 1020 5561 0000 3202 0607 2849 PLN	1 reka	None
CURRENT ACCOUNT	16 1020 5561 0000 3402 0607 2864 PLN	1 reka	None

Default pattern:

Term pattern:

From:

[Back](#) [Execute](#)

The group allocation of the Transaction Signing pattern to the account requires a sign-off.

Single allocation of the Transaction Signing pattern to the account

It is also possible to allocate the Transaction Signing Pattern separately to every account. This option allows to allocate different Transaction Signing Pattern to individual accounts within one context. To allocate the Transaction Signing pattern to one account in the context, find this account on the “List of accounts” in the context of (Accounts - > List of accounts) and then select the “Modify transaction signing pattern” function. On the next screen, select from the drop-down list a relevant Transaction Signing pattern. You can also select a fixed pattern.

The single allocation of the Transaction Signing pattern to the account requires a sign-off.

Liquidity management

The liquidity management panel allows you to display accounts not only from your own context, but also from other contexts.

NOTE! For the account to be displayed in the “Liquidity Management” panel, it has to be allocated to at least one group used for the Liquidity Management panel. For details of the allocation of accounts to groups see the chapter in the guide regarding account grouping.

The dependency indicated above can be used to configure the availability of a given account in the Liquidity Management panel. For example, a payroll account can be excluded from presentation by not allocating it to any group of accounts used in the Liquidity Management panel.

This is particularly important because every User with the Liquidity Management right can view the history of all accounts configured in the Panel. The right to view the history in the Liquidity Management panel does not depend on the Account Authorization Patterns used in the basic module (“Account” section and “Transaction”).

The right to the “Liquidity Management” panel is included in the Services patterns.

Naming of individual accounts

The account naming is not an obligatory element of the configuration process, but only an extra option at the stage of access configuration by the Administrator at the company. The name assigned by the Bank by default corresponds to the type of a given account, e.g. a current account, auxiliary account. It is recommended to name the accounts in particular when the function of account sorting by name is to be used.

Account naming in the iPKO biznes makes it easier to manage and identify the accounts. It is a convenient function for Clients who hold many accounts or need to have them group additionally (e.g. PLN accounts, FX account, payroll accounts).

NOTE! All Users see the same name of the account in the context. The same account cannot have different names that depend on the User who log into the system. The account names have to be unique. The accounts can be named in the "Account" tile "List of accounts"->„Account details”->”Rename”-> “Modification of account name” function.

Users

Creation of Signature Classes

The Administrator should create Signature Classes that they will use, in subsequent configuration steps, when defining the Transaction Signing Patterns. The Signature Classes are used to “group” Users to easily create transaction sign-off rules that apply at the company. As a standard, there are four Signature Classes in iPKO biznes system:

- Dyrektor (Head),
- Kierownik (Manager),
- Księgowy (Accountant),
- Prezes (President).

The Administrator can add a new Signature Class. To define another class, select the “New” tile and then “Signature Class” function.

The screenshot displays the 'New signature class' configuration interface. At the top, there is a navigation bar with several menu items: 'Context parameters', 'Accounts', 'Users', 'Services', 'Access restrictions', 'Whitelists', 'Transactional limits', 'File formats', 'Access channels and tokens', 'External channels', and a 'New' dropdown menu. The 'New' menu is currently open, showing options: 'Pattern', 'Signature class', 'Whitelist', 'File format', and 'Zgoda CAF'. Below the navigation bar, the main content area is titled 'New signature class'. It features a PDF icon and the text 'Administrator's guide'. There is a text input field for 'Signature class name' with a character count of '0 / 35 Characters'. Below this, there is a section titled 'List of users' with an 'Expand section' link. At the bottom left, there is a 'Back' button, and at the bottom right, there is a red 'Execute' button.

The new signature class will be added to the list of signature classes available after selecting the “Users” tile and the “Signature Class” tab. In addition, for all the Signature Classes shown in the list of “Signature Classes” list, it is possible to change the name (“Edit” function) or delete (“Delete” function) a given signature class from the list.

Allocation of Signature Classes to Users

The Signature Classes created earlier shall be assigned to individual Users. The Signature Classes can be allocated under the “Users” tile. The “List of Users” is displayed on the first screen. The Signature Classes can be allocated in groups or one by one.

Group allocation of Signature Classes to Users

If there is a group of Users who are to have the same Signature Class, it is recommended to use the option of group allocation of the Signature Classes to Users.

To allocate the same Signature Class to the Users, check individual persons in the “List of Users” and then select the Group Function option and the select the “Change signature class” option in the drop-down list.

The Signature Class for the selected Users shall be selected from the drop-down list.

The screenshot shows a web interface with a top navigation bar containing tiles for 'Context parameters', 'Accounts', 'Users' (selected), 'Services', 'Access restrictions', and 'New'. Below this are more tiles: 'Whitelists', 'Transactional limits', 'File formats', 'Access channels and tokens', and 'External channels'. A secondary navigation bar includes 'List of users' (selected), 'Signature classes', 'Account authorisation patterns', and 'Service authorisation patterns'. The main content area is titled 'List of users' and features a PDF icon for 'Administrator's guide'. A 'Group functions' dropdown menu is open, with 'Change signature class' highlighted in red. Below the dropdown is a table with the following data:

Group functions	ID	Administrator	Signature class	Service authorisation pattern	Functions
Change signature class					
Change account authorisation pattern					
Change service authorisation pattern	4924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)	PEŁNY DOSTĘP DO USŁUG	[View] [Edit] [Add] [Delete]

Group modification of signature class


PDF Administrator's guide

List of users

User	User ID	Administrator	Signature class
ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)

Selection of signature class

Existing class New class

Select class 

- None
- DYREKTOR
- KIEROWNIK
- KSIĘGOWY

Back Execute

Single allocation of Signature Classes to the User

If the User is to have a separate Signature Class, the following shall be:
 follow the same procedure as for the group allocation of the Signature Class, but select only one User,
 or
 on the first screen in the “List of users” submenu in the context check the selected person and the select the “Change signature class” function.

Services

Creating the Services patterns

The Services patterns defines the rights/activities a given User can hold/perform in the iPKO biznes system as regards the services available. There are no predefined Authorization Service Patterns on the iPKO biznes website. When defining them, the Administrator has to create a new pattern, depending on the scope of activities the User is to perform in the iPKO biznes system.

The following service authorizations can be defined in the iPKO biznes system:

Counterparty database:

Access to counterparty database,
 Creation, modification and removal of trusted domestic beneficiary.

The “Counterparty database” service allows to create (and import), modify and delete counterparties. The absence of rights to this service means that the User can view and use the counterparty database but cannot manage it. The Transaction Signing pattern is **not** allocated to the “Counterparty database” service because the database management does not require authorisation.

File exchange:

The “file exchange” service is not connected with the access to the account. The file exchange function allows the User to access files dispatched and received within the entire context. The “File exchange” service allows to dispatch and receive files to and from the Bank. There is a Transaction signing pattern allocated to the “File exchange” service; however, **it not possible to set up the transaction limit** as part of the Transaction signing pattern.

Prepaid cards:

Reposting of funds.

Card management within a business,

Credit cards:

Card management within a business,

Card cancellation and ordering,

Modification of card limits.

Charge cards:

Card management within a business,

Card cancellation and ordering,

Modification of card limits.

Debit cards:

Card management within a business,

Card cancellation and ordering,

Modification of card limits.

Liquidity Management

The liquidity management panel is dedicated to Clients with a complex organizational structure, with many instances of the iPKO biznes Internet banking system.

Liquidity Limits Management

The Liquidity Limits Management module in iPKO biznes is dedicated to corporate clients with access to the account balance consolidation service (Real Cash Pooling or Consolidated Account).

Reporting module

Administration of reporting module

The Reporting module (customized reports) is a service that enables an authorized person to define any structure of output files. It is designed to create customized reports, e.g. reports required to feed accounting systems or define customized file formats. A module based on the transactions posted on the account allows to quickly obtain a file that complies with the expected output parameters.

External bank accounts

MT101 request for transfer search

MT101 request for transfer order

Applications

Applications List – list of all applications on the website,

Accounts applications – a permit to open and close auxiliary accounts,

Internet banking applications – the right to add and delete users in iPKO biznes (only with the User role).

Applications for cards – the right to order debit, prepaid, charge, credit cards (depending on the agreement signed)

Applications for cards – the right to order debit, prepaid, charge, credit cards (depending on the agreement signed)

Other online applications - the right to submit other applications regarding Cash, Accounts, Settlements, Cards, Loans and iPKO biznes.

The module enables authorized users to submit applications online. Just as in the case of other functions of iPKO biznes, there are separate rights to view, submit and sign the applications.

All authorizations shall be configured under the “Services patterns” related to the users. Remember that by modifying existing Service authorization patterns, all users using this pattern will have access to the application.

<input type="checkbox"/> Applications	<input type="checkbox"/> Access	<input type="checkbox"/> Creation	<input type="checkbox"/> Signing
Applications List	<input type="checkbox"/>		
Accounts applications		<input type="checkbox"/>	<input type="checkbox"/>
Internet banking applications		<input type="checkbox"/>	<input type="checkbox"/>

Allocation of the Services patterns to users

The Authorization Service Patterns created earlier shall be assigned to individual Users. The Authorization Service Patterns can be allocated under the “Users” tile. The “List of Users” is displayed on the first screen. The Authorization Service Patterns can be allocated in groups or one by one.

Group allocation of the Services patterns to users


If there is a group of Users who are to have the same Services patterns, it is recommended to use the option of group allocation of the Service authorization patterns to Users.

To allocate the same Services patterns to a group of Users, check individual persons in the “List of Users” on the first screen and then select the “Group Function” option and then select the “Change service authorization pattern” option in the drop-down list.

The screenshot shows a navigation menu with 'Users' selected. Below it, there are several tabs: 'List of users', 'Signature classes', 'Account authorisation patterns', and 'Service authorisation patterns'. The 'List of users' tab is active, displaying a table of users. A dropdown menu is open over the table, with 'Change service authorisation pattern' highlighted in red. The table has columns for ID, Administrator, Signature class, Service authorisation pattern, and Functions.

ID	Administrator	Signature class	Service authorisation pattern	Functions
4924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)	PEŁNY DOSTĘP DO USŁUG	[Icons]

Group change of service authorisation pattern

 Administrator's guide

List of users

User	User ID	Administrator	Service authorisation pattern
ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.	PELNY DOSTĘP DO USŁUG

Existing pattern New pattern

Select pattern: PELNY DOSTĘP DO USŁUG

Back Execute


The allocation of the Services patterns to Users requires a sign-off.

Single allocation of the Services patterns to the user

If the User is to have a separate Services patterns, use the option of the single allocation of the Services patterns. Follow the same procedure as for the group allocation of the Services patterns, but select only one User or on the "List of Users" on the first screen check a person and then select the "Modification of service authorization pattern" function.

On the next screen, select a relevant Services patterns from the drop-down list.

Modification of service authorisation pattern

 Administrator's guide

User: ANNA WANNA
 User ID: 1954924
 Administrator: Yes, allowed to change own authorisation permissions.
 Service authorisation pattern: PELNY DOSTĘP DO USŁUG

Existing pattern New pattern

Select pattern: PELNY DOSTĘP DO USŁUG

Back Execute

The allocation of the Services patterns to the User requires a sign-off.

Access restrictions

The iPKO biznes access restriction option is not an obligatory element of the configuration process, but an extra option at the stage of access configuration by the Administrator at the company.

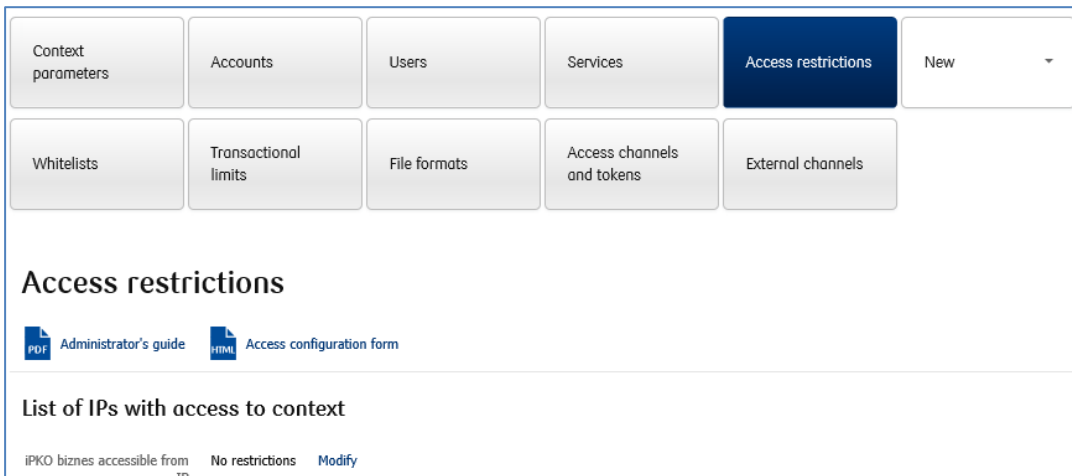
Access restricted to indicated computer IP addresses

In the iPKO biznes system, the Administrator representing the Company or the Bank's employee can indicate IP addresses from which specific Users of the context will be able to log into the system. It means that it will not be possible to log into a given context from IP addresses other than those indicated by the person when setting the parameters of the context, and it is also possible to introduce customized settings for the users.

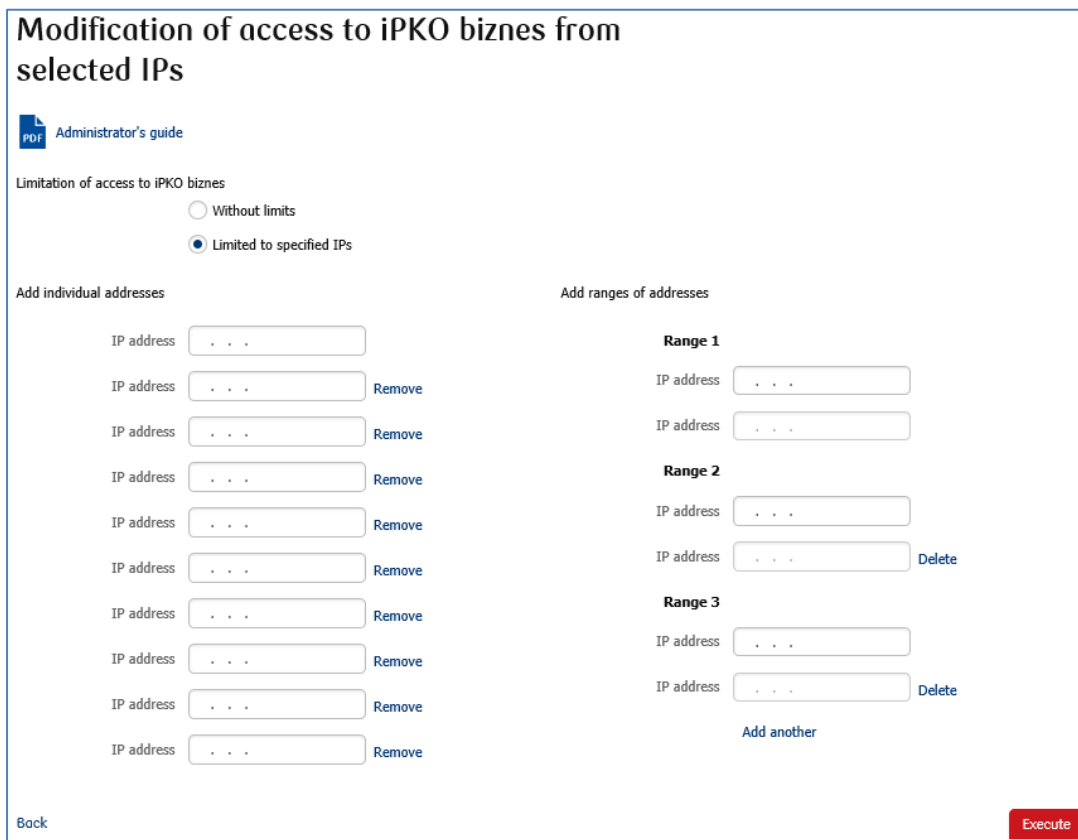
In addition, there is an option in the iPKO biznes system that allows to limit the period during which the context is available to specific Users. This function allows to limit the User access in time, i.e. to enable access during specific hours: from-to, on days: business days, Saturday, Sunday, public holidays.

There are two methods for limiting the access to the iPKO biznes system from specific IP addresses:

1. select the “Access restrictions” tile -> „List of IPs with access to context”-> iPKO biznes accessible from IP -> “No restrictions” “Modify” button.



Then the “Modification of access to iPKO biznes from selected IPs” option will be displayed on the screen with two available “Limitation of access to iPKO biznes” sub-options: “Without limits” and “Limited to specified IPs”. It is possible to indicate max. 10 IP addresses from which users can access/log into the iPKO biznes website. The change will apply to all users in the context.



2. select “Access restriction” tile -> „User’ access”. The user access from the selected IP can be changed one by one or in groups.
 - a. to change access from the IP address for one user, selected this user from the list of users.

Users' access

Group functions ▾

<input checked="" type="checkbox"/>	User User ID	Hours of accessibility	Weekdays	Public holidays	Access status	IP availability	Access by mobile application	Functions
<input checked="" type="checkbox"/>	ANNA WANNA 1954924	No restrictions	No restrictions	No restrictions	Active	Context default	Default for context	Modify access from IP

Then deselect the “Modify access from IP” function by the selected user. The screen “Modification of access from user’s IP” will be displayed. It is possible to limit access to a maximum of 10 IP addresses.

Modification of access from user's IP

Administrator's guide

User ANNA WANNA
User ID 1954924
Administrator Yes, allowed to change own authorisation permissions.

Limitation of access to iPKO biznes

Without limits
 Limited to specified IPs

Add individual addresses

IP address

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

IP address Remove

Add ranges of addresses

Range 1

IP address

IP address

Add another

Back Execute

- b. to change the access from the IP address for a group of users, on the screen “User Access” check the selected users, and then select “Group Functions” option, and select “Modify access from IP” from the drop-down list.

Users' access

Group functions ▾

Modify term access


Modify access from IP

Change access from mobile application

	Weekdays	Public holidays	Access status	IP availability	Access by mobile application	Functions
1954924	No restrictions	No restrictions	Active	Context default	Default for context	

The screen “Group modification of access from IP addresses of users” will be displayed. Check the “Limitation of access to iPKO biznes” “Limited to specified IPs” radio button and then enter appropriate IP addresses. Do not enter dots between the digits. The system adjusts the format of the sequence of digits. It is possible to enter max. 10 IP addresses for which the user’s access will be limited.

Group modification of access from IP addresses of users

 Administrator's guide

Selected users 1

[Collapse list](#)

User	User ID	Administrator
ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.

Limitation of access to iPKO biznes

Without limits
 Limited to specified IPs

Add individual addresses

IP address

IP address [Remove](#)

IP address [Remove](#)

IP address [Remove](#)

IP address [Remove](#)

[Add another](#)

Add ranges of addresses

Range 1

IP address

IP address

[Add another](#)

[Back](#) [Execute](#)


For Clients who plan to entrust the Bank with the iPKO biznes system parameters setting, the iPKO biznes offers the option of printing the “iPKO biznes system access configuration request – access restrictions”.

Access management in predefined time frames

There is a function in the iPKO biznes system that allows to limit the period during which the context is available to specific Users. This change allows to limit the User access in time, i.e. to enable access during specific hours: from-to, on days: business days, Saturday, Sunday, public holidays. To do so, select “Modify term access” for a specific User.

Then, a table will be displayed on the screen where you can determine specific restrictions for this User.

Modification of user's term access in iPKO biznes

 Administrator's guide

User ANNA WANNA

User ID 1954924

Administrator Yes, allowed to change own authorisation permissions.



Access hours No restrictions From / to (hours) from : to :

Business days [v](#)

Saturday [v](#)

Sunday [v](#)

Public holidays [v](#)

Access status Active Blocked until further notice Locked until From  To 

[Back](#) [Execute](#)

The iPKO biznes system availability can be set for several Users in the “Group functions”, ”Modify term access” option.

Users' access

Group functions
 Modify term access
 Modify access from IP
 Change access from mobile application

	Weekdays	Public holidays	Access status	IP availability	Access by mobile application	Functions
1954924	No restrictions	No restrictions	Active	Context default	Default for context	

Group modification of term access for users

Administrator's guide

Selected users 1

Collapse list

User name User ID	Administrator	Hours of accessibility	Weekdays	Public holidays	Access status
ANNA WANNA 1954924	Yes, allowed to change own authorisation permissions.	No restrictions	No restrictions	No restrictions	Active

Access hours No restrictions From / to (hours) from 00 : 00 to 23 : 59

Business days

Saturday

Sunday

Public holidays

Access status Active Blocked until further notice Locked until From ____ : ____ To ____ : ____

Back Execute

Limiting access to the iPKO biznes system via mobile application

The iPKO biznes system offers an option for context access management in the mobile application.

Administration / Access restrictions / Access to context through mobile application Collapse - My short-cuts ▾

Context parameters	Accounts	Users	Services	Access restrictions	New ▾
Whitelists	Transactional limits	File formats	Access channels and tokens	External channels	

iPKO biznes change of access by mobile application

iPKO biznes accessible from mobile application

Available Unavailable

Back Execute

Account Grouping

The account grouping function can be used for two purposes:
to group accounts in the “Accounts” and “Transactions” sections,
to group accounts in the “Liquidity Management” panel.

The account grouping is a two-stage process. First you have to create groups, and then allocate accounts to them.

Creation of account groups

To create a group of accounts, after logging into the system select the “Settings” link (upper right corner of the panel), then “My profile” tile, select the “List of accounts” tab and then the “Group Management” link.

The screenshot shows the top navigation bar of the iPKO biznes system. On the left is the logo. In the center, the company name is 'DPT CORPORATION' and the user name is 'MARCIN MOBILNY'. On the right, there are links for 'Messages', 'Settings' (highlighted with a red box), and 'Administration'. Below the navigation bar is a menu with options: Transactions, Accounts, Cards, Loans & deposits, Cash, Analysis, Applications, e-Gov, and a language selector set to 'EN'.

The screenshot shows the 'My profile' settings page. At the top, there are several navigation tiles: 'Access channels', 'Access password', 'Authorisation tool', 'My profile' (selected), and 'Mobile applications'. Below this, the 'Settings' section is active, with 'List of accounts' highlighted in a red box. The main content area is titled 'My profile' and contains three sections: 'Default account in forms', 'Default transaction parameter values', and 'Default import parameters'. Each section has various input fields and dropdown menus for configuration. At the bottom right, there is a red 'Execute' button.

Settings [List of accounts](#)

List of accounts

Group functions ▼ [Managing groups](#)

<input type="checkbox"/>	Account name	Account number	Favourite account	Group of accounts
<input type="checkbox"/>	CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN	<input type="checkbox"/>	Add
<input type="checkbox"/>	ZPŚS	07 1020 5561 0000 3802 0991 5291 PLN	<input type="checkbox"/>	Add
<input type="checkbox"/>	VAT ACCOUNT	97 1020 5561 0000 3102 0991 5275 PLN	<input type="checkbox"/>	Add

[Execute](#)

Enter the target group name in the “Group name” field, select the “Create group” button and then “Save”.

Managing groups ✕

Group name [Create group](#)

0 / 30 Characters

*** Mandatory field**

[Cancel](#) [Save](#)

Managing groups ✕

Group name [Create group](#)

0 / 30 Characters

▼ ▲ ✕ ↻ Grupa1

*** Mandatory field**

[Cancel](#) [Save](#)

Allocation of accounts to groups

To allocate account to the group, select the “List of accounts” tab. To allocate the accounts to the group, check all or selected accounts on the list (using the checkboxes) and then use one of the following options:

- add accounts one by one – if the accounts checked are to be allocated to different groups, indicate the group for every account separately.
- add in groups – if the accounts checked are to be allocated to the same groups.

Settings [List of accounts](#)

List of accounts

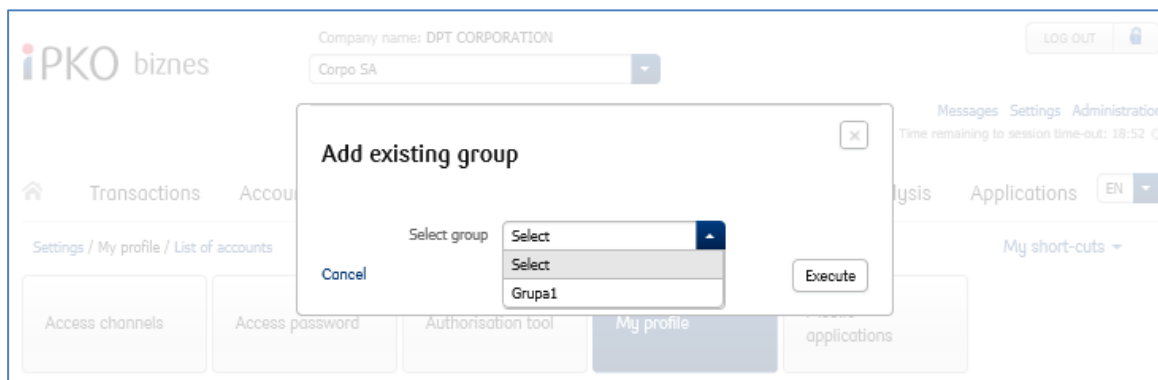
Group functions ▼ Managing groups

<input type="checkbox"/>	Account name	Account number	Favourite account	Group of accounts
<input type="checkbox"/>	CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN	<input type="checkbox"/>	Add
<input type="checkbox"/>	ZPŚS	07 1020 5561 0000 3802 0991 5291 PLN	<input type="checkbox"/>	Add
<input type="checkbox"/>	VAT ACCOUNT	97 1020 5561 0000 3102 0991 5275 PLN	<input type="checkbox"/>	Add

[Execute](#)

NOTE! The changes collectively overwrite the existing settings, so the accounts will be allocated only to the groups selected on the group allocation screen.

Select the “Add” option on the allocation screen and indicate the group to which the accounts are to be allocated.



Account Grouping for Liquidity Management purposes

In the “Liquidity Management” panel there is an option for the allocation of group to accounts from other contexts. For this to be possible, the parameters must be first set by the Bank. To allocate the group to the accounts from other contexts, use the “Context name” field on the “Account Group” page.

NOTE! For the account to be displayed in the “Liquidity Management” panel, it has to be allocated to at least one group used for the Liquidity Management panel. For details of the allocation of accounts to groups see the chapter in the guide regarding account grouping.

Defined Format Management

The functionality is available in the Administration module → New tile → Drop down list → File format – domestic transfer; File format – foreign transfer; File format – domestic counterparty; File format – foreign counterparty.

As shown on the screen above, the User with administrator rights will be able to choose one from 4 available templates. The User without administrator rights will only have passive information about the formats defined

in the context (if any). After selecting from the drop-down list the file format that we want to create, the new format creation process will commence. The process is described in the next chapter.

The screenshot shows the iPKO biznes system interface. At the top, the company name is 'DPT CORPORATION' and the user is 'MARCIN MOBILNY'. The navigation menu includes 'Transactions', 'Accounts', 'Cards', 'Loans & deposits', 'Cash', 'Analysis', 'Applications', and 'e-Gov'. The sidebar contains a 'New' dropdown menu with options for 'File format', 'File format – domestic transfer', 'File format – foreign transfer', 'File format – domestic Counterparty', and 'File format – foreign Counterparty'. The main content area is titled 'Context parameters' and contains a table of parameters and an 'Edit' button.

Context name	DPT CORPORATION	User data	MARCIN MOBILNY
Context ID	67098	User ID	2507622
Company number	64931469	Signature class	PREZES

Awaiting funds availability	Inactive	Session duration	20 minutes
Execution of Split Payment despite insufficient funds in VAT account	Yes	Language version	PL – Polish version (default)
Duplicate verification	Inactive	Accounts sort order	Default (currency, type, account number)
Lock on modification of operations from file	Inactive	Access to context for external entities	Non-active
Checksum verification	Transactions - Inactive File exchange - Inactive		

[Edit](#)

All formats created will be displayed on the “List of file formats” page.

The screenshot shows the iPKO biznes administration interface. At the top, the company name is DPT CORPORATION and the user is MARCIN MOBILNY. The navigation menu includes Transactions, Accounts, Cards, Loans & deposits, Cash, Analysis, Applications, and e-Gov. The 'File formats' tile is highlighted in the dashboard. Below the dashboard, the 'List of file formats' page is displayed, featuring a table with the following data:

Format name	Format type	Status	Functions
Wlasny	Domestic transfer	Active	

The following functions will be available next to every format:

- “Details” – a page displaying information about the format, including the options available: Change status, Change, Delete or Print.
- “Modify” – allows to modify the format created earlier,
- “Modify status” – allows to start and end the publication of the format in the context. Inactive status means that format created will not be available for Users on the file import screen even though it is defined in the context.
- “Delete” – allows to delete a format.

Format definition – template common fields

After using one of the templates available on the drop-down list in the “New” tile, the format definition process will start.

Field name	Description
Format name	Text field of 35 characters. The name has to be unique within the context and, at the same time, different from the names of the existing basic and additional formats.
Use other format settings	The option allows you to copy the settings of another format already defined in the context. If this option is used, the system opens an additional screen with the list of available formats.

Code page	The change of the code page from the default value "Detect automatically" will result in the situation where the code page will be set automatically to that indicated in the format when the User selects a given format during import. It is recommended to keep the "Detect automatically" option unless there are problems with Polish diacritic characters.
Decimal separator of amount	Specify the amount separator used in the file. The files with the amounts expressed in Polish grosz can be also supported.
Date format	If the date field is used in the file, specify the date format.
Date separator	Field available if the date format has been specified. Specify if and if yes, then that kind of separator is used in the date field.
Cut too long contents in text fields	The option is dedicated to text fields, such as "Operation details", "Counterparty Details" – for the files with too many characters in these fields (over 140) the system will import the file and delete all the characters over the said limit (the field ending characters will be deleted). For fixed-point files, first the filling-in characters will be recognized and then the length of proper data will be verified and, if necessary, any excess data will be deleted.
File type	Specify whether the file is a fixed-point or variable point file.
Separator of fields in file	Enter the character or a sequence of characters (max. 5) that are used as file field separators. Note: data separator is the field displayed for the floating-point files only.
Text qualifier	If the file uses a text qualifier, you may specify a character or a sequence of characters (max. 5). The qualifier should start and end the text field. No separate pairs of qualifiers should be used for sub-fields. Note: text qualifier is the field displayed for the floating-point files only.
Separator in multi-row fields	The option is dedicated for text fields, such as "Operation details", "Counterparty details" – if the file uses a sub-field separator, you can specify it in the format and then file division into lines will be preserved during import. Note: separator in many-line fields is the field displayed for the floating-point files only.
Removal of character	The function allows to indicate a character or a sequence of characters to be ignored during import to the system. Note: the characters indicated for deletion cannot be used in the format as the format structure elements. For example, a character used also as the field separator in the file cannot be deleted. When using this function make sure that the file remains in compliance with the file format.
Modification of character	The function allows to indicate a character or a sequence of characters to be replaced with other character/a sequence of characters during import to the system. Note: the characters indicated for replacement cannot be used in the format as the format structure elements. For example, a character used also as the field separator in the file cannot be replaced. When using this function make sure that the file remains in compliance with the file format.
File has header	If the file has a header, check the option and enter the number of header lines in the file (counted from the top of the file). Header data will be ignored during import.
File has footer	If the file has a footer, check the option and enter the number of footer lines in the file (counted from the bottom of the file). Footer data will be ignored during import.

File Structure Setting

The file structure is set by copying the layout of fields in the file to be imported.

There are three checkboxes in the bottom section of the page:

Ungroup the field "Transaction Title",

Ungroup the field "Counterparty's name and address",

Split payment.

The function is dedicated to formats where many-line fields files are not used for the counterparty details or transaction details items.

If this function is used, the 140-character text fields (4x35 characters) is replaced with 4 separate fields, each of 35 characters.

The fields which can be used to create the forms are on the left. The format under construction is on the right – it has mandatory fields by default.

File structure

Ungroup field "Transaction details"

Ungroup field "Counterparty name and address"

Split Payment

Available fields

Transfer type

Payment date

Currency

Originator's references

Ignored field

Add >

Add all >>

Remove <

Delete all <<

File structure

Payment amount

Originator account number

Counterparty account number

Counterparty name and address

Transaction title

Up

Down

Example of record

Payment amount;Originator account number;Counterparty account number;Counterparty name and address;Transaction title

When defining the format use the add/delete option ("Add", "Add All" / "Remove", "Delete All"). They allow to add or delete fields in the structure created. To define the sequence of fields, specify the field in "File structure" and the use the "Up" and "Down" options. For fixed-point files you can also specify the length by each field.

There is an additional function available at the bottom of the screen: "Example of record" showing the current setting of the format parameters, taking into account the field separator and the sequence of fields in the format. For fixed-point files, in addition the length will be displayed next to each field.

After creating the format, define the status on the confirmation screen (the "Active" format will be available to the User, the "Inactive" format will be saved, but it will not be published). The operation has to be authorized with the token code.

Format definition – fields typical for SPLIT and Tax Authorities

To be able to use the format when placing transfer orders of SPLIT type and to the Tax Authorities, it is **necessary** to use the "Transfer type" field in the format. When the field is move to the "File structure" section, an additional window will appear:

File structure
Gross amount
VAT amount
Originator account number
Counterparty account number
Counterparty name and address
Invoice number
Counterparty ID
Transaction title
Transfer type

Up Down

Defining value of „Transfer type“ field

Regular transfer [Add](#)

Transfer to Tax Office [Add](#)

Split Payment [Add](#)

In the “Transfer type’ field value definition” field indicate the value with which the lines will be marked in the file with regular transfer, SPLIT payment and transfers to the Tax Office.

For example – as seen on the screen – if value “1” is entered in the “Transfer type” field, the system will interpret this file line as a regular transfer. If value “2” is entered in the field, all such lines will be interpreted as a transfer to the Tax Office, and the value “53” will mean that it is the SPLIT payment.

Operation title – SPLIT/Tax Office – floating-point formats

It is required that specific data be included in the operation details (transfer title) in the imported file, as per the ELIXIR standard. Full information on how to define such a title for floating-point files, is available on the iPKO biznes logon page, in the “iPKO biznes ELIXIR-O Input File Structure” file. After selecting the “Split Transfer” file structure, the transaction title will be divided into additional separate fields with the invoice number, Counterparty ID, gross amount and VAT amount.

Operation title – SPLIT/Tax Authorities – fixed-point formats

Sub-field separators shall not be used for fixed-point formats. The structure for the Tax Office in fixed-point files is the same as in the floating-point files, formats, without the use of sub-fields (there is no need to move to the new data field, if the limit of 35 characters is exceeded). After selecting the “Split Payment” structure, the transaction title will be divided into additional separate fields with the invoice number, Counterparty ID, gross amount and VAT amount.

Format definition – fields typical for the foreign transfer order

For a foreign format, it is necessary to define the glossary for the “Fee instructions” field.

Similarly, as in the case of the SPLIT payment orders and transfer orders to the Tax Office, there is an additional window under the file structure where you have to define your own values or use the default settings.

For example – as seen on the screen – if in a given operation in the file, value “1” is entered in the “Fee instructions” field, it means that a given transfer is to be imported with the cost clause set as “SHA”, “2” means “BEN”, whereas “3” means “OUR”.

Cost clauses:

SHA – the sender pays the costs of the sender’s bank and the beneficiary pays the costs of other banks,

BEN – the beneficiary pays the costs of the sender’s bank and other banks,

OUR – the sender pays the costs of the sender’s bank and other banks,

The screenshot shows a software interface for defining file structure fields. A list of fields is shown on the left, with 'Fee instructions' selected. Below the list are 'Up' and 'Down' buttons. A dialog box titled 'Defining content of field 'Fee instructions'' is open, showing three options: SHA, BEN, and OUR, each with an 'Add' button.

Field
File structure
Payment amount
Currency
Originator account number
Counterparty account number
Counterparty name and address
Transaction title
Beneficiary bank SWIFT/ ABA code
Beneficiary bank country
Fee account
Fee instructions

Up Down

Defining content of field 'Fee instructions'

SHA SHA Add

BEN BEN Add

OUR OUR Add

Whitelists

The Whitelist of Counterparties function allows to define the lists of counterparties, which, after allocation to the accounts, will prevent any transactions to accounts which are not included in the white list.

Basic assumptions:

Depending on the configuration, the white lists may be defined at the level of iPKO biznes (by the administrator) or by the Bank following an appropriate instruction.

It will be possible to import the white list from the file.

There are 2 types of white lists: domestic and foreign.

Once defined, the white list is allocated to the account.

If the white list is allocated to the account, at the stage of the operation set-up, sign-up and dispatch (release of the authorized transaction) it will be verified whether the account to be credited is on the list of accepted accounts. If the result of the verification is negative, the system will prevent the operation.

Creation of the white list

To create the white list, select the “New” tile. The following options are available in the drop-down list: “New list” and “Import from the file”. The “New list” option is selected. A “New white list” is displayed on the output screen.

If the white list of counterparties is created manually, the editable screen will be displayed with the “Name” and “Type” fields, where you enter the name of the white list and define the list type (Domestic/Foreign) and with “Account” and “Counterparty Name” columns.

New whitelist

Name *

Type *

Counterparty accounts

Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>
Account <input type="text"/>	Counterparty name <input type="text"/>

[Add another](#)

[Back](#) [Execute](#)

To import the white list, select its type, provide the name and indicate the file location. Then the selected file will be sent to the bank server, where its content will be analysed and if the result is correct, the list will be created. Then allocate this list to the selected accounts.

Import from file

Name *

Type *

Code page *

Select file *





The creation of a white list requires confirmation with the token code.

Allocation of the created white list to the accounts

The created white lists shall be assigned to the accounts. They are allocated at the level of the “Whitelists” tile > “Whitelists Counterparties” by selecting the “Assign” function in the list of accounts next to the selected account.

Whitelists Counterparties List of accounts

Whitelists Counterparties

Identifier	Name	Type	Functions
4164	Domestic1	Domestic	   

When the “Assign” function is selected, the screen with the accounts available for selection will be displayed. To confirm the selection, enter the token reply for the indicated operation code.

Assignment of whitelist

Name Domestic1
Type Domestic
Identifier 4164

Accounts selection

<input type="checkbox"/>	Account name	Account
<input type="checkbox"/>	CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN
<input type="checkbox"/>	ZFŚS	07 1020 5561 0000 3802 0991 5291 PLN
<input type="checkbox"/>	VAT ACCOUNT	97 1020 5561 0000 3102 0991 5275 PLN

Counterparty accounts Collapse section ▾

Account	Counterparty name
09 1020 5561 0000 3102 0013 4312	T1
26 1020 5561 0000 3202 0296 0052	T2

[Back](#)

Assignment of whitelist - confirmation

Name Domestic1
Type Domestic
Identifier 4164

Accounts selection

No whitelisted accounts from context

Counterparty accounts

To expand the list, use the "Expand section" function

Expand section ▾



* Mandatory field

[Back](#)

[Authorise](#)

Similarly, the allocation of the white list to the accounts can be deleted by selecting the "Assign" option and not indicating any accounts and then by confirming this operation with the token code.

NOTE! Only one domestic and one foreign white list can be allocated to the account.

NOTE! If the account is not allocated to the created white list, it will be possible to prepare the transfer order to any beneficiary at the basic module level.

Statement of accounts

To view the white lists that apply to the accounts, select the "Whitelists" tile and then the "List of accounts" tab. The screen with accounts will be displayed, broken down by types of white lists (Domestic List / Foreign list).

Whitelists Counterparties		List of accounts	
Account name	Account	Domestic list	International list
CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN	None	None
ZFŚS	07 1020 5561 0000 3802 0991 5291 PLN	None	None
VAT ACCOUNT	97 1020 5561 0000 3102 0991 5275 PLN	None	None

Change of the content of the white list

After selecting the "Whitelists" tile, the "Whitelists counterparties" tab, the "Change" function becomes available and is displayed by every account to which the white list is allocated. This function allows to modify the content of details of the beneficiaries (Account and Counterparty name).

Change of whitelist

Name Domestic1
Type Domestic
Identifier 4164

Counterparty accounts

Account: <input type="text" value="09102055610000310200134312"/>	Counterparty name: <input type="text" value="T1"/>
Account: <input type="text" value="26102055610000320202960052"/>	Counterparty name: <input type="text" value="T2"/>

[Add another](#)

Whitelisted accounts from context Collapse section ▾

No whitelisted accounts from context

[Back](#)

On the editable screen displayed you can make changes to the existing accounts of the counterparties or add new ones by selecting the “Add next” option. To confirm the changes enter the token code.

NOTE! If the white list is modified, the changes will apply to all accounts to which a given white list is allocated.

Change of whitelist - confirmation



Name Domestic1
Type Domestic
Identifier 4164

Counterparty accounts

Account	Counterparty name
09 1020 5561 0000 3102 0013 4312	T1
26 1020 5561 0000 3202 0296 0052	T2

Whitelisted accounts from context Expand section ▾

To expand the list, use the "Expand section" function





Security image Type code from token

* Mandatory field

[Back](#)

Deletion of the white list

To delete the white list, select the “Delete” option on the right side of the entry and confirm this operation with the token code.

Whitelists Counterparties		List of accounts	
Whitelists Counterparties			
Identifier	Name	Type	Functions
4164	Domestic1	Domestic	   

NOTE! If the white list allocated to the accounts is deleted, it means that all restrictions for these accounts as regards the transactions with the defined list of beneficiaries are removed. It will be possible to send transactions to any account.

Removal of whitelist



Name Domestic1
Type Domestic
Identifier 4164

Counterparty accounts

Account	Counterparty name
09 1020 5561 0000 3102 0013 4312	T1
26 1020 5561 0000 3202 0296 0052	T2

Whitelisted accounts from context

To expand the list, use the "Expand section" function [Expand section ▾](#)

Security image   Type code from token *

* Mandatory field

[Back](#) [Execute](#)

Transactional limits

These limits determine the maximum amount for which individual users can authorize transfers within a specified period.

Basic assumptions:

- Possible dates: daily, weekly, monthly,
- Limits are expressed in PLN,
- The limits are linked to the account and the user,
- The limit shall be used at the time of sign-off. The limit period is counted from the first authorisation till the end of the limit period. Daily limit is counted by the end of the day, weekly – by the end of Sunday, monthly – by the end of the last day of the month. If the transaction is moved to edition or deleted, the limit use is also removed.

Transaction limits cannot be set for VAT accounts and technical accounts linked to the loan.

Activation of limits

To activate the transaction limits select the “Transactional limits” tile.

The screenshot shows the iPKO biznes user interface. At the top, the company name is 'DPT CORPORATION' and the user is 'MARCIN MOBILNY' with ID '2507622'. The navigation menu includes 'Transactions', 'Accounts', 'Cards', 'Loans & deposits', 'Cash', 'Analysis', 'Applications', and 'e-Gov'. The 'Transactional limits' tile is highlighted in the 'Administration / Transactional limits' section. Below the tiles, the 'Transactional limits' page is displayed, showing a table of users with their respective limits.

Group functions	User	Identifier	Administrator	Signature class	Functions
<input type="checkbox"/>	MARCIN MOBILNY	2507622	Yes, allowed to change own authorisation permissions.	PREZES (ID 233111)	

The list of context users is displayed on the page. The limits can be defined for each user individually (“Modify” function next to each user) or in groups with the use of “Group functions” > “Group modification of limits”. To make a group change first check the users (by ticking the checkboxes) who are to have the same set of limits.

This screenshot shows the 'Transactional limits' page with the 'Group modification of limits' option selected. The table below shows a user 'ANNA WANNA' with ID '1954924'. The 'Functions' column for this user has a red box highlighting the 'Modify' icon (an 'X' in a square).

Group functions	User	Identifier	Administrator	Signature class	Functions
<input type="checkbox"/>	ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)	

Change of user limits

On the limit change screen define the expected limit for every account separately. The limit is expressed in PLN therefore the FX and foreign transactions will be converted according to the valid exchange rate. The list shows the accounts to which the user holds the right.

Change of user limits



Administrator's guide

User ANNA WANNA
 User ID 1954924
 Administrator Yes, allowed to change own authorisation permissions.

Account name	Account number	Daily (until 23:59)	Weekly (until 2020-01-26)	Monthly (until 2020-01-31)
CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN	<input type="text" value="10 000 000,00"/> Remaining: 10 000 000,00 PLN Utilised: 0,00 PLN	<input type="text"/>	<input type="text"/>
ZFŚS	07 1020 5561 0000 3802 0991 5291 PLN	<input type="text" value="10 000 000,00"/> Remaining: 10 000 000,00 PLN Utilised: 0,00 PLN	<input type="text"/>	<input type="text"/>

Back Execute

NOTE! If the field is left blank, it means that there is not limit, therefore no restrictions as to the maximum amount of the authorized transactions. In the case of a user who had a limit, if the value is deleted, the limit is removed.

NOTE! If value 0 is entered, the limit will be imposed which completely prevents the authorization of transactions from a given account.

Details of user limits

It is possible to verify the current status of the limits available for a given user. To do this, use the “Details” function.

<input checked="" type="checkbox"/>	User	Identifier	Administrator	Signature class	Functions
<input checked="" type="checkbox"/>	ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)	

User limits ✕


User ANNA WANNA
 User ID 30153520
 Administrator Yes, allowed to change own authorisation permissions.

Account name	Account number	Daily (until 23:59)	Weekly (until 2020-01-26)	Monthly (until 2020-01-31)
CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN	10 000 000,00 PLN Remaining: 10 000 000,00 PLN Utilised: 0,00 PLN	No limit defined	No limit defined
ZFŚS	07 1020 5561 0000 3802 0991 5291 PLN	10 000 000,00 PLN Remaining: 10 000 000,00 PLN Utilised: 0,00 PLN	No limit defined	No limit defined

Group modification of user limits

On the screen for the group change of limits you can allocate the same sets of limits to select users and accounts. The rules for defining the limit values are the same as for the single change screen (described above). The list shows the accounts to which the users hold rights.

Group modification of limits

 Administrator's guide

List of users

User	Identifier	Administrator	Signature class
ANNA WANNA	1954924	Yes, allowed to change own authorisation permissions.	PREZES (ID 263861)

Accounts selection

<input type="checkbox"/>	Account name	Account number
<input type="checkbox"/>	CURRENT ACCOUNT	92 1020 5561 0000 3302 0991 5267 PLN
<input type="checkbox"/>	ZFŚS	07 1020 5561 0000 3802 0991 5291 PLN
<input type="checkbox"/>	VAT ACCOUNT	97 1020 5561 0000 3102 0991 5275 PLN

Defining of limit

Daily (until 23:59)	Weekly (until 2020-01-26)	Monthly (until 2020-01-31)
<input type="text"/>	<input type="text"/>	<input type="text"/>

[Back](#)

Use of all of the available limit

If the user has used all of the limit available for a given period, whenever the user attempts to authorize the transaction, a relevant alert will be displayed and the authorisation will fail.

Access channels and tokens

At this point the information about the following is presented: the type and status of the existing authorisation tool (token), (iPKO biznes Integra) certificate, Internet channel status (logon password) and phone channel status (contact with the Bank's Helpline at 800 302 302) for all website users.

Administration / Access channels and tokens / List of access channels and tokens Collapse ▲

Context parameters
Accounts
Users
Services
Access restrictions
New ▼

Whitelists
Transactional limits
File formats
Access channels and tokens

Access channels and tokens

Group functions ▼

<input type="checkbox"/>	▲ User User ID	Type Status of current tool	Status of certificate Certificate expiry date	Status of internet channel	Status of phone channel	Functions
<input type="checkbox"/>	HALINA TESTOWA 1952233	Mobile token Active	None	Access enabled	No access	
<input type="checkbox"/>	JAN TESTOWY 1952200	Token Active	None	Access enabled	No access	

If access to the Internet channel is blocked, the status will change and a new icon will appear that will allow to unblock the access.

Access channels and tokens

Group functions ▼

<input type="checkbox"/>	▲ User User ID	Type Status of current tool	Status of certificate Certificate expiry date	Status of internet channel	Status of phone channel	Functions
<input type="checkbox"/>	HALINA TESTOWA 1952233	Mobile token Active	None	Access enabled	No access	
<input type="checkbox"/>	JAN TESTOWY 1952200	Token Active	None	Access enabled	No access	

In the table with the list of users, in the “Functions” column you can select the following:

- Details** – the following sections are displayed in the layer:

Access channels and User tokens

User data: HALINA TESTOWA
User ID: 1952233
Phone number for initial password dispatch: +48 777222777

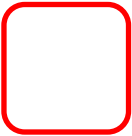

Access channels

Service	Status	Maximum number of failed login attempts	Last successful login	Last failed login	Security image	Functions
Website	Access enabled	3	2017-11-20 17:05:20	2017-04-13 10:26:20		
Call-in service	No access	3				

Authorisation tool

Type	Current tool	Telephone number	Tool number	Status Certificate expiry date	Status change date	Functions
Mobile token	<input checked="" type="checkbox"/>	+48 55555555	6000000000002817	Active	2019-03-11	

If access to the Internet channel is blocked, the following screen is displayed:

	<p>User data AREK JASTRZĘBSKI</p> <p>User ID 1951965</p> <p>Phone number for initial password dispatch +48 666333666 </p> <p>Access channels</p>
---	---

Access channels – the Administrator can activate the Internet and phone channel if they are blocked (logon password and the option to contact the Bank Helpline at 800 302 302)

Authorisation tools – you can block and unblock any authorisation tool (tokens and certificates)

- 🔒 **Lock** – you can block the token/certificate. The function does not require authorisation with the token code.
- ✅ **Unlock** – you can unblock the token/certificate. The function requires authorisation with the token code.
- 🔒 **Activate the Internet channel*** – you can activate the Internet channel (password) if it is blocked. The function required authorisation with the token code.
- 🔒 **Activate the phone channel*** – you can activate the Internet channel (password) if it is blocked. The function required authorisation with the token code.

NOTE! The Group functions of “locking” and “unlocking” apply only to the existing authorization tool (token).

* After the Internet channel is activated by the Administrator, the user will activation of the Internet channel by the administrator, the user will be able to log into service again. After entering the logon page at www.ipkobiznes.pl and entering your alias number, text message** will be sent to the phone number indicated by the user with the initial password which should be entered in the password field. Then the user should change this password by replacing it with their own password, as in the case of the first logon.

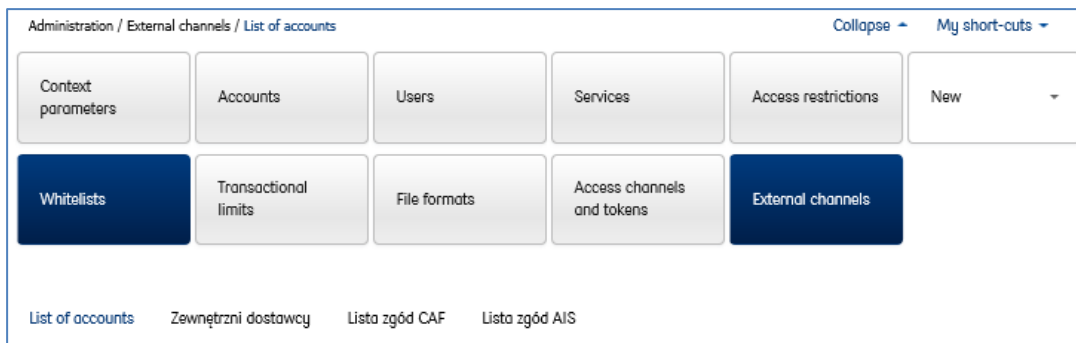
** example of the text message:

iPKO biznes initial password: 550h15nD, active for 10 minutes

External Channels

The “External Channels” module allows to manage access to data exchange between the Bank and Third Party Providers. With the consent of the User, the Third Party Providers will be able to obtain access to information about accounts with the use of three services:

- AIS (Account Information Service) – access to Bank account information
- PIS (Payment Initiation Service) – initiation of payments
- CAF (Confirmation of the Availability of Funds) – confirmation of the availability of funds on the account



The access to the context by internal entities is activated by modification of the context parameters.

Modification of context parameters

Administrator's guide

Context name:

Context parameters

<p>Awaiting funds availability *</p> <p><input checked="" type="radio"/> Inactive</p> <p><input type="radio"/> Active (indefinitely)</p> <p><input type="radio"/> Active for Days <input type="text"/></p>	<p>Session duration *</p> <p><input type="radio"/> 5 minutes</p> <p><input type="radio"/> 10 minutes (default)</p> <p><input type="radio"/> 15 minutes</p> <p><input checked="" type="radio"/> 20 minutes</p>
<p>Execution of Split Payment despite insufficient funds in VAT account *</p> <p><input checked="" type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>Language version *</p> <p><input type="text" value="PL - Polish version (default)"/></p>
<p>Duplicate verification *</p> <p><input checked="" type="radio"/> Inactive</p> <p><input type="radio"/> Active <input type="text" value="Select"/></p>	<p>Accounts sort order *</p> <p><input checked="" type="radio"/> Default (currency, type, account number)</p> <p><input type="radio"/> By account name (alphabetically)</p>
<p>Lock on modification of operation from file *</p> <p><input checked="" type="radio"/> Inactive</p> <p><input type="radio"/> Active</p>	<p>Access to context for external entities *</p> <p><input type="radio"/> Non-active</p> <p><input checked="" type="radio"/> Active</p>
<p>Checksum verification *</p> <p>Transactions <input checked="" type="radio"/> Inactive</p> <p><input type="radio"/> Active <input type="text" value="Select"/></p> <p>File exchange <input checked="" type="radio"/> Inactive</p> <p><input type="radio"/> Active <input type="text" value="Select"/></p>	

* Mandatory field


Back Execute

List of accounts

In the "List of accounts" section a table is displayed with the list of services activated on the accounts. The settings can be modified one by one for every account or by using the group functions.

List of accounts Zewnętrzni dostawcy Lista zgód CAF Lista zgód AIS


List of accounts

 Administrator's guide

Group functions ▾

<input type="checkbox"/> (0)	Account name Account number	Account Information Service (AIS)	Transaction initiation service (PIS)	Available funds verification service (CAF)	Functions
<input type="checkbox"/>	CURRENT ACCOUNT 92 1020 5561 0000 3302 0991 5267 PLN	Inactive	Inactive	Inactive	
<input type="checkbox"/>	ZPŚS 07 1020 5561 0000 3802 0991 5291 PLN	Inactive	Inactive	Inactive	
<input type="checkbox"/>	VAT ACCOUNT 97 1020 5561 0000 3102 0991 5275 PLN	Inactive	Inactive	Inactive	

Changing access to services

 Administrator's guide

Account name CURRENT ACCOUNT
Account number 92 1020 5561 0000 3302 0991 5267 PLN

Access to services

Account Information Service (AIS)

Inactive
 Active

Transaction initiation service (PIS)

Inactive
 Active

Available funds verification service (CAF)

Inactive
 Active

[Back](#) [Execute](#)

Changes should be confirmed with the token code.

Third Party Providers


The “Third Party Providers” section allow to provide the selected Third Party Providers with access to the services activated earlier. To do so, select the Add/Delete Providers option and select the Third Party Provider approved by PFSA from the list.

Administration / External channels / External suppliers Collapse ▾ My short-cuts ▾

Context parameters	Accounts	Users	Services	Access restrictions	New ▾
Whitelists	Transactional limits	File formats	Access channels and tokens	External channels	

List of accounts External suppliers CAF consent list AIS consent list

External suppliers

 Administrator's guide Add / Delete Suppliers

Changes should be confirmed with the token code.

List of CAF consents

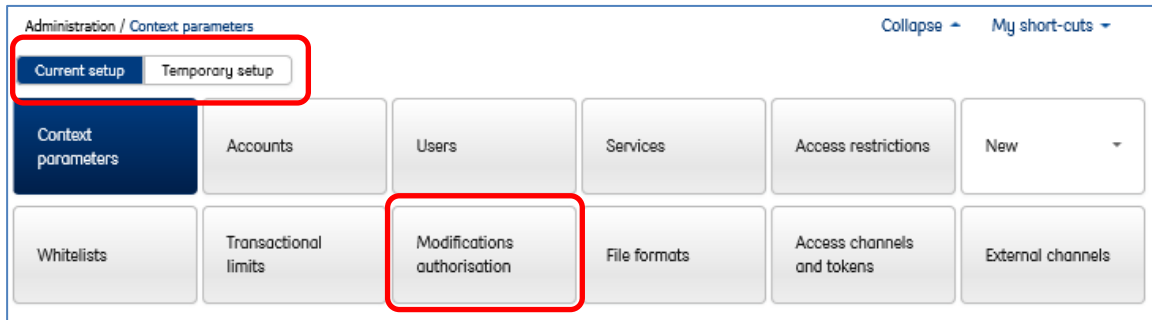
The list of CAF approvals shows all questions about the availability of a specific amount on the account asked by a defined Third Party Provider.

List of AIS consents

The list of AIS consents shows the consents provided in the authentication service (the process initiated by a defined Third Party Provider) for the Bank Information Service,

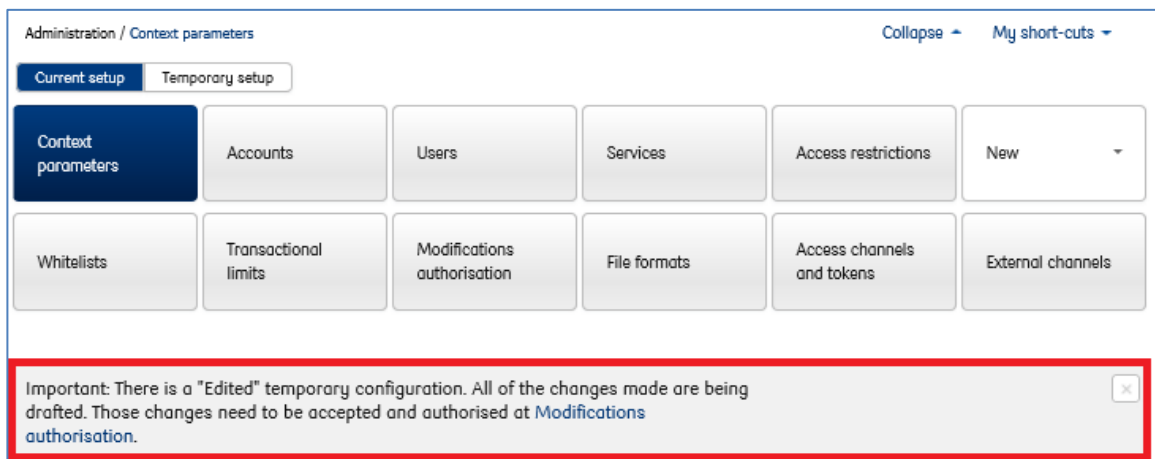
Authorisation of changes

The iPKO biznes website allows to use additional security measures in the form of additional authorisation of changes made by the next user with the administrator's rights (up to five users). This option is set by the Bank's employee on the basis of an individual request of the Client. If these parameters are set, the "Modification authorisation" tile appears and the option is enabled to switch between the current authorisation and the configuration pending authorisation (Temporary setup).



Temporary setup

When the authorisation pending configuration changes are made, a message is displayed in the Administrator module informing that additional authorisation is required.



After selecting the "Modification authorisation" tile, it is possible to view the changes made by clicking details and triggering a pop-up window from which you can download a detailed list of configurations with shaded fields of changes pending additional authorisation.

Administration / Modifications authorisation Collapse ▾ My short-cuts ▾

Current setup **Temporary setup**

Context parameters

Accounts

Users

Services

Access restrictions

New ▾

Whitelists

Transactional limits

Modifications authorisation

File formats

Access channels and tokens

External channels

Modifications authorisation

Configuration number	Configuration type	Configuration history		Status	Functions
71735	Context configuration	Creation: ANNA WANNA (1954924)	2020-04-02 18:14:33	Edited	

Configuration details ✕

Context name: Corpo SA
 Configuration number: 71735
 File name: 71735-20200402_1817.zip
 Status: Edited

Attention: see details regarding system configuration at Configuration report. Modifications made has been marked grey in the Report


History

2020-04-02 18:14:33 Creation: ANNA WANNA (1954924)

When the verification is completed, you can use the “End editing” function which saves the configuration. The configuration sign-off requires the entry of the token code.

Configuration signing


Context name: Corpo SA
 Configuration number: 71736
 File name: 71736-20200402_1830.zip
 Status: To sign

 Attention: see details regarding system configuration at [Configuration report](#). Modifications made has been marked grey in the Report

History


2020-04-02 18:29:14 Creation: ANNA WANNA (1954924)
 2020-04-02 18:29:58 End of editing: ANNA WANNA (1954924)

I accept configuration Report number 71736.

Security image:  Type code from token:

* Mandatory field


[Back](#) [Authorise](#)

Or “Delete”  function which rejects the settings made.

Note: the removal of the configuration will delete all the settings made in the working mode. Last modification: ANNA WANNA, 2020-04-02 18:32:13.

Configuration removal

Context name: Corpo SA
 Configuration number: 71736
 File name: 71736-20200402_1832.zip
 Status: Edited

 Attention: see details regarding system configuration at [Configuration report](#). Modifications made has been marked grey in the Report

History


2020-04-02 18:29:14 Creation: ANNA WANNA (1954924)
 2020-04-02 18:29:58 End of editing: ANNA WANNA (1954924)
 2020-04-02 18:32:13 Restore to editing: ANNA WANNA (1954924)

[Back](#) [Execute](#)

When the operation is complete an outcome table will be displayed with the configuration history and the status description.

The configuration has been deleted.

Modifications authorisation

Configuration number	Configuration type	Configuration history	Status	Functions	
71736	Context configuration	Creation: ANNA WANNA (1954924) End of editing: ANNA WANNA (1954924) Restore to editing: ANNA WANNA (1954924) Removal: ANNA WANNA (1954924)	2020-04-02 18:29:14 2020-04-02 18:29:58 2020-04-02 18:32:13 2020-04-02 18:33:28	Removed	

iPKO biznes parameters setting by the Bank

At the request of the Client the Bank may assume the function of managing the rights of the Users and setting parameters of the iPKO biznes system, including the first setting of the system parameters.

Security

Internet Browser and Passwords

When making operations in the iPKO biznes system it is recommended to use the latest versions of browsers: Firefox. In addition, it is recommended to disable the function of form storing in the Internet browser.

Never share the Client's password and number to any third parties and never provide them on unencrypted pages. If a wrong password is entered three times, the website is blocked.

All operations made after logging into www.ipkobiznes.pl are secured by default with the TLS (Transport Layer Security) protocol, version 1.2. TLS 1.0. is also acceptable

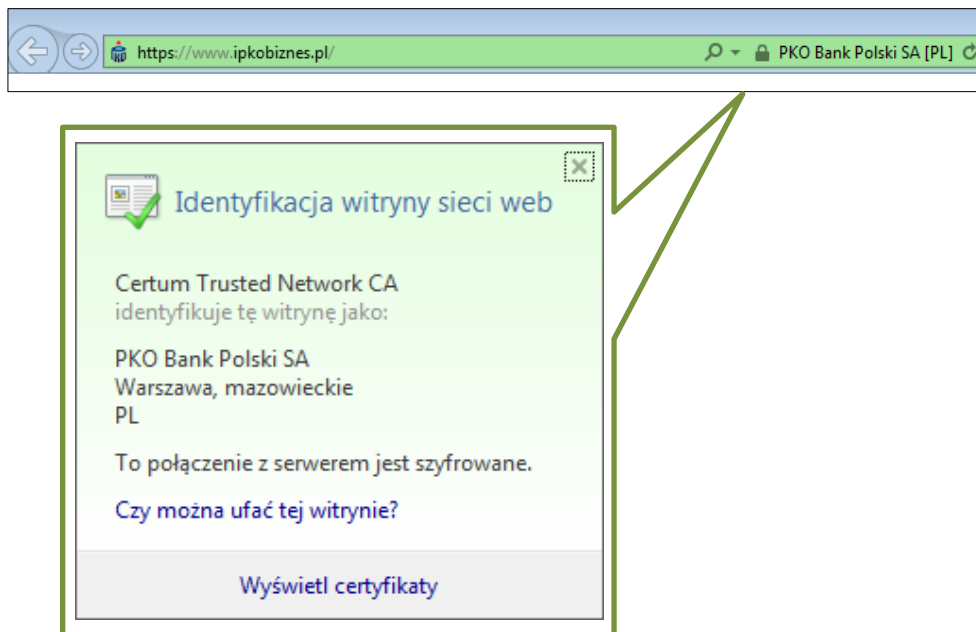
Secure logging (page address and certificate)

Before logging into the iPKO biznes website, made sure that the connection used by the User is encrypted.

The website address of the website shall be as follows: <https://www.ipkobiznes.pl>

The logon page secured with the Extended Validation certificate. This way the address bar can be marked in green. The name of the website operator (PKO Bank Polski SA) is also displayed. Next to the Internet address there should be an encrypted connection icon – usually displayed in the form of a padlock (in older versions of the browsers this icon may be displaced at the bottom of the screen). To verify that the certificate is correct, click the icon and verify the following data:

- Website is operated by: PKO Bank Polski SA, Warsaw, Mazowieckie, PL.



Next verify the content of the “Thumbprint” field. To do that:

- In Internet Explorer browser, after clicking the encrypted connection icon, select the “Show certificates” option, select the “Details” tab and then find the “Thumbprint” field in the drop-down list.
- In Firefox browser, after clicking the encrypted connection icon, select the “Learn more” icon, select the “Security” tab and then select the “Show certificate” option. In the “Thumbprint” section find the “SHA1 thumbprint” field.

The correct value of the SHA 1 thumbprint for www.ipkobiznes.pl is (small and capital letters are supported):

99 96 58 a4 41 9c e3 4a 41 b1 af 5f 1b 21 b2 15 cf a2 47 cb

Antivirus Software and E-mail Security

The use of the Internet involves the risk of installation of viruses, Trojan horses or spyware software on the computer. To avoid such a risk and to make the use of electronic banking services safer, it is worth knowing the best way to protect yourself.

Antivirus software – there are many tools to fight viruses which ensure safe use of the Internet resources. PKO Bank Polski recommends to all its Clients install and use anti-virus software.

Firewall

Firewall – a network wall is another very effective tool protecting against computer viruses. It is hardware with software, or software only that blocks unauthorized access to the secure computer network, computer or server.

E-mail Security

It should be remembered that, by opening e-mails from unknown senders the User is exposed to computer infection with viruses. In order the computer against it, it is necessary to use the antivirus scanner that scans every incoming mail for viruses or Trojan horses. All files and client pages opened are also scanned. In this way, it is possible to prevent phishing that involves the displaying of the “fabricated” false website instead of the original website, and in consequence to block the outflow of confidential information such as logins, passwords, PIN codes.

Prevention

To make the use of the network as safe as possible, it is worth respecting several important rules:

- New viruses appear in the network every day and therefore the antivirus software should be updated frequently.
- The antivirus software should be never disabled when you work online.
- Every file downloaded by the User to the drive of their computer should be scanned for viruses before opening.
- The software of operating systems and Internet browsers should be updated frequently. Current patches are published on websites of software producers and they are very effective security measures.

Support for iPKO biznes System Users



iPKO biznes Helpline for Corporate Clients and Public and Local governments

- 801 36 36 36 * option 3

*national calls

- +48 (61) 855 94 94 *

international and mobile phone calls

*charged according to the operator's tariff, the Helpline is available from Monday to Friday, from 8:00 a.m. to 6:00 p.m.