Internet-Bank for corporate clients

Short user guide

Version 1.6

Table of Contents

Overview

The service "Internet-Bank for corporate clients" provides legal entities (bank's clients) an access to full range of services for remote account control.

Opportunities:

- Sending financial documents to the bank in order to entrust bank to complete particular operations in accordance with the document.

- Receiving different reports for any period:

  — Account statements;

  — Turnover balance sheet;

  — Budget report;

  — Contract performance report;

  — Limits report.

- Service management:

  — Indicator — counterparties searching and checking service;

  — DirectBank+ — service for work with bank directly via "1C:Enterprise" interface;

  — Mobile-Banking — work in "iBank" system on your smartphone or tablet;

  — Standing orders;

  — Electronic Document Management with counterparties.

- Connection of additional services:

  — Currency control;

  — Salary project;

  — Budgeting;

  — Contract settlement control.

- Connection of additional service channels;

- Connection of additional service channels;

- Work with bank guarantees;

- Opening, viewing and editing deposits and minimum permanent balances;

- Work with granted credits, tranche receiving and advanced repayment;

- Work with corporate cards and receiving account statement with use of corporate cards;

- Document sign, confirmation and acceptance;

- Receiving accruals from state agencies and creation payment order for compensation;

- Work with templates of the documents;

- Import and export document for exchange with client's accountant programs;

- Installation system notices;

- Installation system notices;

- Support of system reference books: Banks of Russia, SWIFT, BCC, Trusted recipients, Beneficiaries, Currency rate;

- Online message exchange with the bank's employee with use of widget "Chat".

The service provides support for any number of client's employees.

Data security mechanisms used in the system:

- Signing financial documents with electronic digital signature (ES) in order to provide integrity and authorship proof of the data being transferred;

- Cryptographic algorithms for ciphering information during its transfer between bank and client in order to provide its privacy;

- Parties cryptographic authentication mechanism during protected interaction via the Internet.

Requirements

In order to work with Internet-Bank it is necessary:

- Modern computer with one of the following operating system installed:

    — Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) or higher;

    — Apple Mac OS X: 10.7 (Lion) or higher;

    — Ubuntu or other Debian-based distributions (86/x64 latest versions).

- Display resolution 1280x1024 or higher;

- To ensure the protection of confidential information, you must have CIPF on client's computer. CIPF is used to implement ES key generation functions encryption and electronic signature generation and verification of electronic signature encryption, data encryption and prevention of false data entry;

- Web-browser with support of the plugin BIFIT Signer for using ES:

    — Microsoft Edge;

    — Google Chrome;

    — Yandex Browser;

    — Firefox;

    — Opera;

    — Atom;

    — Safari (provided that the browser is shared with MAC OS).

    It is recommended to use the latest web-browser version.

- Cryptographic service provider as a USB-device with opportunity to use electronic signature (ES) or removable USB storage if you are using file ES keys.

    The correspondence of the types of devices to the number of ES keys which can be stored in their memory is shown in the table below.

    To provide crypto safety can be used:

    — Hardware devices. The list of supported hardware devices and necessary software see Supported hardware devices section;

    — If you use file keys on your computer must be installed cryptolibraries. Cryptolibraries are used to implement functions of encryption keys forming and electronic signature, generation and checking of electronic signature, data encryption and simulation protection (for more details see Appendix 1). Contact your bank to get the cryptolibraries files;

    — The use of third-party ES verification keys may be allowed on the bank side. To use a third-party ES key, the computer must have a CIPF installed, with which was used to generate a third-party key ES. For more details about third-party ES keys see Advanced electronic signature section.

- It is recommended that the client's computer has a USB port for connecting hardware devices;

- Access to the Internet. The recommended connection speed is 33.6 Kbps and higher. When Internet access via dial-up line, you must have a modern modem;

- Printer availability recommended.

Supported hardware devices

Hardware cryptographic service provider is designed for generation ES inside the device and providing its secure and unextractable storage. Formation of ES under a document executing inside the device.

Internet-Bank supports the following devices:

— MAC-token BIFIT;

— Rutoken EDS 2.0;

— MS_KEY K – Angara.

For using listed devices you might need to install on your computer the driver, compatible with your OS:

— driver installation package for MS_KEY K – Angara available at ibank2.ru

— driver installation package for using USB-token Rutoken EDS 2.0 available at rutoken.ru

For using MAC-token BIFIT on MS Windows 7 OS official hotfix must be installed (stored on microsoft.com).

During installation of Rutoken ES 2.0 driver, also installs device control panel for configuring: access PIN-code, management of PIN-code quality policy, formatting the device.

The correspondence of the types of devices to the number of ES keys which can be stored in their memory is shown in the table below.

Device	The number of ES keys
MAC-token BIFIT	83
Rutoken EDS 2.0	29
MS_KEY K – Angara	75

Storing and working with ES keys of responsible employees different legal entities served in different banks with different copies of the iBank system is supported for each device.

For USB-token MS_KEY K – Angara both active and removed ES keys are counted for total number of ES keys. Token memory overflow warning issued when creating the last possible ES key. If token memory got exhausted, you should contact the bank to reinitialize the token. At the same time, all ES keys existing on the token will be deleted.

Advanced electronic signature

Third-party ES check keys — ES keys, that are generated by third-party electronic signatures.

On the bank side, third party ES-keys may be allowed to work with the "iBank" system (generated using the CryptoPro CSP and/or Signal-COM CRPD).

The system can use third-party ES keys that meet the following conditions:

• ES key validation certificate are released by certification authority with which the bank cooperates;

• The ES key validation certificate period has not expired.

Rules of safe work

"iBank" system provides guaranteed level of security, contains data encryption mechanism and electronic signature (ES), supports work with hardware devices.

Users should provide appropriate level of data security on their workplaces. They are responsible for security of the data stealing of which can cause material damage to the organisation: passwords, ES keys and etc.

The following are the fundamental principles of safe operation of the user with the "iBank" system modules.

ADDITIONAL DATA PROTECTION MECHANISMS FOR CORPORATE CLIENTS

• SMS-informing customers about logging in, flow of funds on customer's accounts, new incoming letters;

• Extended multifactor authentication at login the system, using one time passwords;

• Mechanism of additional payment order confirmation with validation code (in addition to the ES).

For confirmation in the "iBank" system are used: "Vestochka" App, MAC-tokens BIFIT, SMS messages, OTP-tokens.

PRECAUTIONS FOR SAFE WORK WITH ES

- To protect ES keys against theft by malware it is recommended to use hardware devices.

- If there are no USB-tokens, save file-key repository on a removable storage (USB-drive). Never keep it in a place where someone else except you has an access to it. Removable storage with ES key repository must be carefully protected from unauthorized access.

- Only you, as the owner, have rights to know ES key access password.

- Avoid continuous and uncontrolled connection of hardware cryptographic service provider with ES keys to the computer.

- Do not give USB-tokens with ES keys to anybody.

- Do not work with Internet-Bank from Internet cafés or places, where you are not sure about PC security.

- At dismissal of responsible employee, who had access to ES key, it is necessary to notify the bank and to lock the ES key.

- If there is any suspicion of ES key or execution environment (presence malware on PC) compromise, it is necessary to notify the bank and to lock the ES key.

PROTECTION MEASURES FOR PC, WHICH USED FOR WORK WITH INTERNET-BANK

- Follow the regulations of limited physical access to the computer. There must be a list of employees, including responsible employees and technical staff, who have access to PCs intended for work with Internet-Bank.

- It is recommended to use a separate computer exclusively for work with Internet-Bank. Any other actions (work with other programs, e-mail, visiting web sites) should not be carried out from this PC.

- Use only licensed software. Do not download and install software received from unreliable sources.

- Try to use modern operating systems (OS). In comparison with older ones, frequently outdated, new versions are safer. Timely install OS updates and patches. Turn on autoupdate, it will install the latest patches, thereby eliminating the vulnerability of the OS.

- Use system and application software from trusted sources, which guarantee the absence of malware. It is necessary to ensure the integrity of updates received on media or downloaded from the Internet.

- Use and timely update special data protection software – antivirus software, personal network firewall, protection against unauthorized access and others.

- Do not connect to the PC removable storage, unchecked for presence of malware.

- Regularly, at least once a week, scan your computer for viruses.

PRECAUTIONS FOR WORK IN THE INTERNET

- Do not click pop-up windows with advertisements. It is recommended to turn on locking of pop-up windows in the browser settings.

- Do not visit unchecked and insecure sites. You can involuntarily download viruses and spy software on your PC.

- Do not read suspicious e-mails from unknown senders, they can contain viruses. Carefully read messages themes. If you are not sure, that the e-mail came from a reliable source, do not open it. Do not trust friendly tone or urgency of requests contained in such messages. Do not follow the links contained in suspicious e-mail. Do not open attached files, especially if the sender insists on urgency of request and asks you to open attached file with the ".exe" extension.

- Reduce as much as possible the using of Internet-messengers (such as ICQ).

- Pay more attention to strange or unclear browser error messages. In case of any suspicions, scan your computer for viruses or spy software.

Start of work in service

To start work in the service you need to have plugin BIFIT Signer installed on your computer.

OS Windows users can install the software, required by the bank for working with the service (drivers for hardware devices, plugin BIFIT Signer and etc.) by using special program (installator). If your bank provides this opportunity, at first visit to the service entrance page you will see a message, containing the link for downloading plugin BIFIT Signer (see Figure 1).

Figure 1. The first entrance to the service

Note:

Close all working applications before launching the installator. This will let the installator to update system files without restarting the computer.

Setup the BIFIT Signer installator and follow it's directions (see Figure 2).

Figure 2. Installation

Login to Internet-Bank

To login to Internet-Bank do the following:

1. Connect to the Internet, launch the browser and open entrance page to the system "iBank" for clients of your bank (see Figure 3).

2. In authorization block choose the ES key, that is registered in "iBank" system for company, which documents you plan to work with (see Work with ES keys section).

3. Click button **Login**. Enter the password for the ES key in dialogue box **BIFIT Signer**.

4. If necessary enter the password of hardware device with stored ES key in dialogue box **BIFIT Signer**.

To enhance security on the side of the bank, an additional confirmation request mechanism can be used. For more details see multifactor authentication.

Figure 3. Clients login page

Registration Page

To go to **Registration Page** (see Figure 4) click button **Registration and ES generation** on Clients login page.
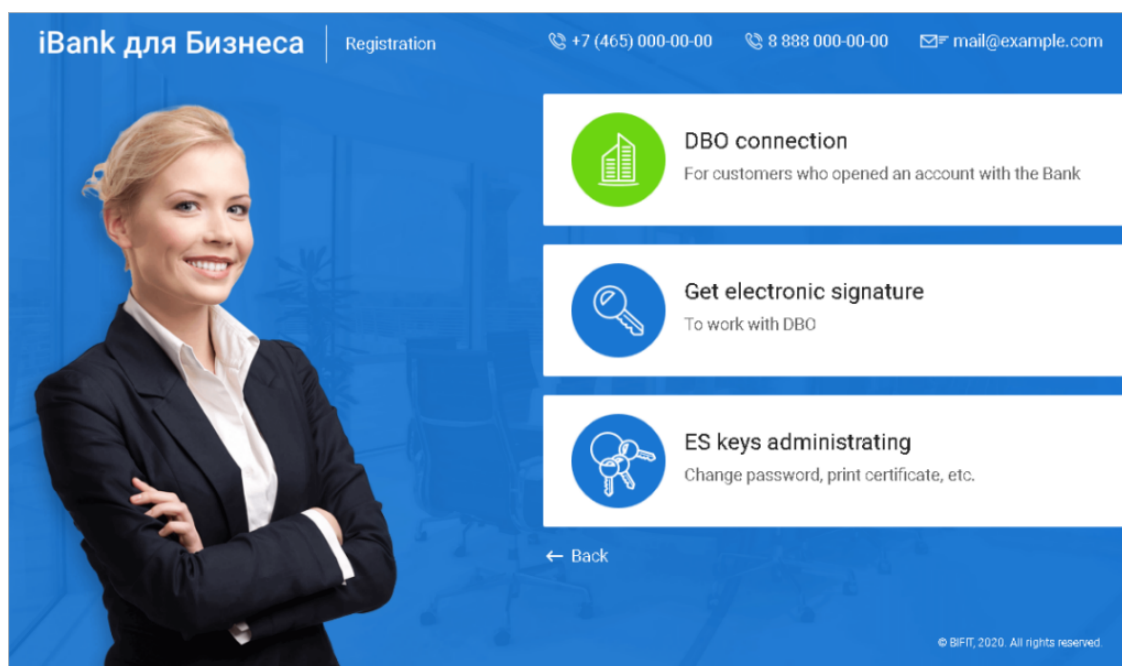
Figure 4. Registration Page

ES Key choice

Information about the ES keys used for authentication is stored on the computer from which the system was logged on. Therefore, the key selection scenarios at the first and second authentications vary.

First entrance

If you are logging in the system "iBank" from a computer that was not previously used to work with "iBank", or after reinstalling the "BIFIT Signer" plugin authorization block has the following appearance (see Figure 5).
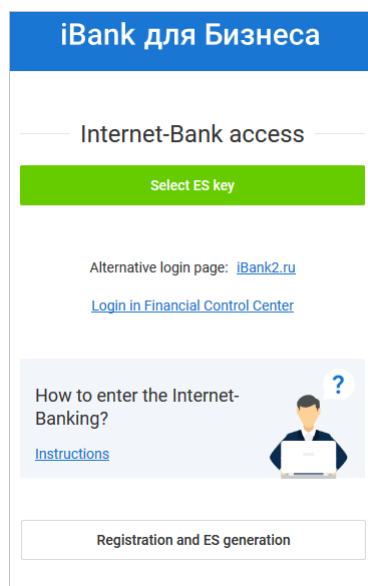
Figure 5. Authorization block. First entrance

Click button **Select ES key** and choose the ES key from the list.

Reentrancy

If you are making the reentrancy in "iBank" system with the ES key is selected by default with which the last entrance was made the authorization block has the following appearance (see Figure 6).
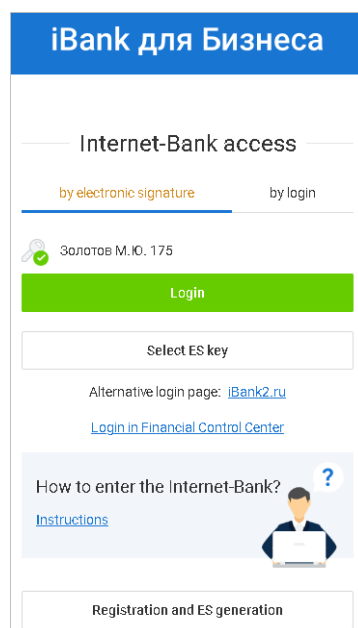
Figure 6. Authorization block. Reentrancy

Click button **Login** to enter with the specified ES key or button **Select ES key** to choose another ES key.

Service will display the list of all ES keys, that were previously used to log in system from this computer (see Figure 7). If the required ES key is not listed, click button [Q Find ES key] Service will switch to the selection of ES keys from all available storages at the current time (for more details see Work with ES keys).
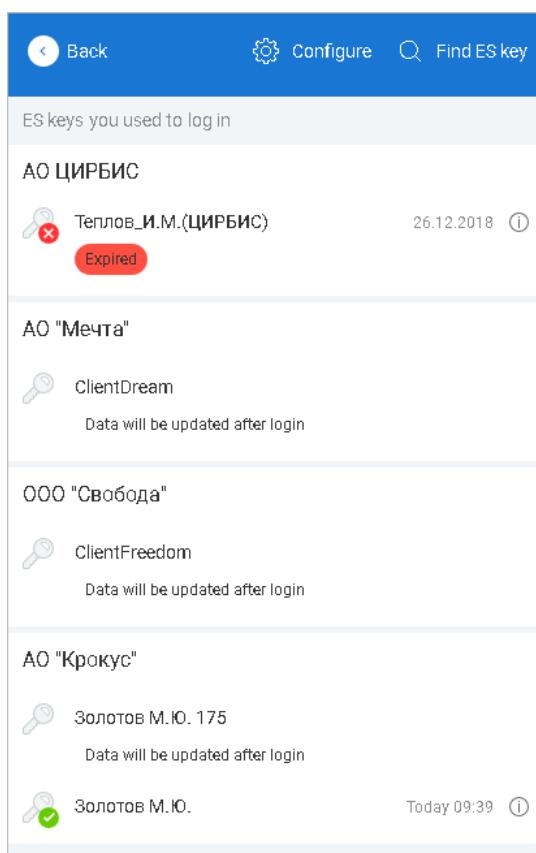
Figure 7. List of ES keys

To configure the list of ES keys click button [⚙ Configure] Service will display ES keys list setting mode (see Figure 8).
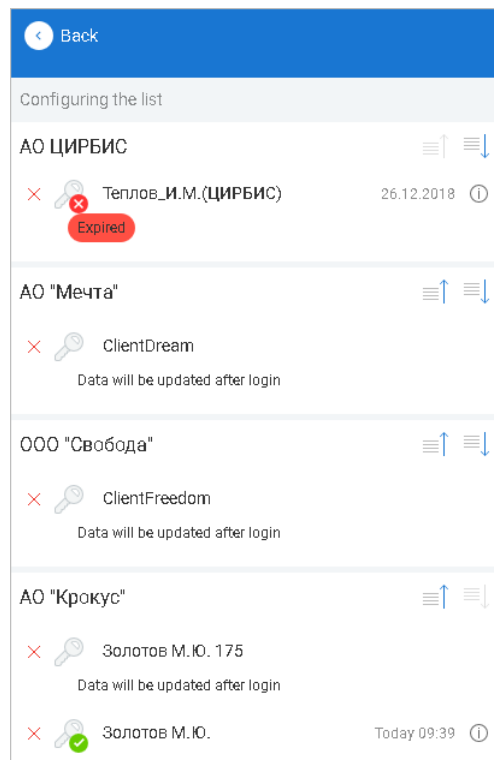
Figure 8. List of ES keys. Setting mode

Reference ES keys setting mode contains the following buttons:

≡↑ / ≡↓   — up/down cursor ES keys;

✕   — hide ES key in the list;

[< Back]   — exit the ES keys list setting mode.

Work with ES keys

In the general list are displayed all those currently available ES keys storages, that contains ES keys (see Figure 9).

To specify the path to the file keystore, click [🔍 Choose a file]

To view a list of available ES after connecting hardware devices or installing certificates click [↻ Refresh]

To display the list off all ES keys, which are contained in the selected ES keys storage, click ⌄

If necessary, to access the ES key list on the hardware device, enter the PIN code to the device.

The following information may be displayed for ES key or certificate:

• Type of ES key storage or cryptographic service provider:

📁 — ES key in file storage;

✎ — ES key in USB token (token's picture may differ and depends on type of connected token). The name of the token type and its serial number are displayed above the list of ES keys it contains;

▦ —ES key at MAC-token BIFIT. The name of the device type and its serial number are displayed above the list of ES keys it contains;

🔲 — third-party ES certificate for using a cryptographic provider CryptoPro CSP;

⊡ — third-party ES certificate for using a cryptographic provider Signal-COM CSP;

⊡ — third-party ES certificate for using a cryptographic provider Message-Pro CSP.

- ES key name (in case the ES key has never been used to login with current computer);

- Name of the organization whose employee this ES key belongs to[1];

- ES key owner full name[1];

- ES status[1];

- ES expiration date[1];

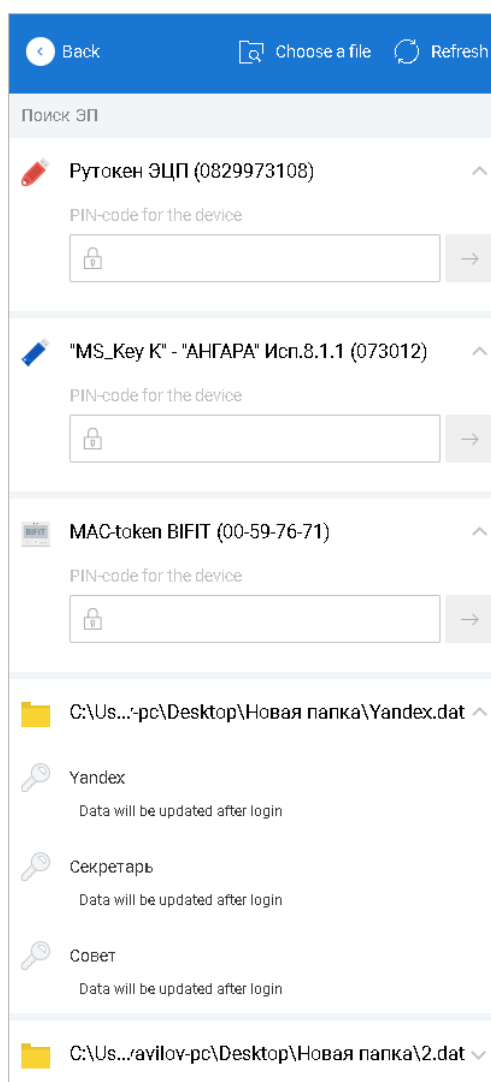- Date and time of the last login to the system by this ES key from the current computer[1].

Figure 9. Common list of ES keys

"iBank" versions choice

If the bank granted you the rights to Internet-Bank and Internet-Bank Lite, then after passing the authentication you will be redirected to web-page to choose the version of "iBank" system (see Figure 10).

---

[1]Information is shown for those keys, that were used at least once for login from current computer.
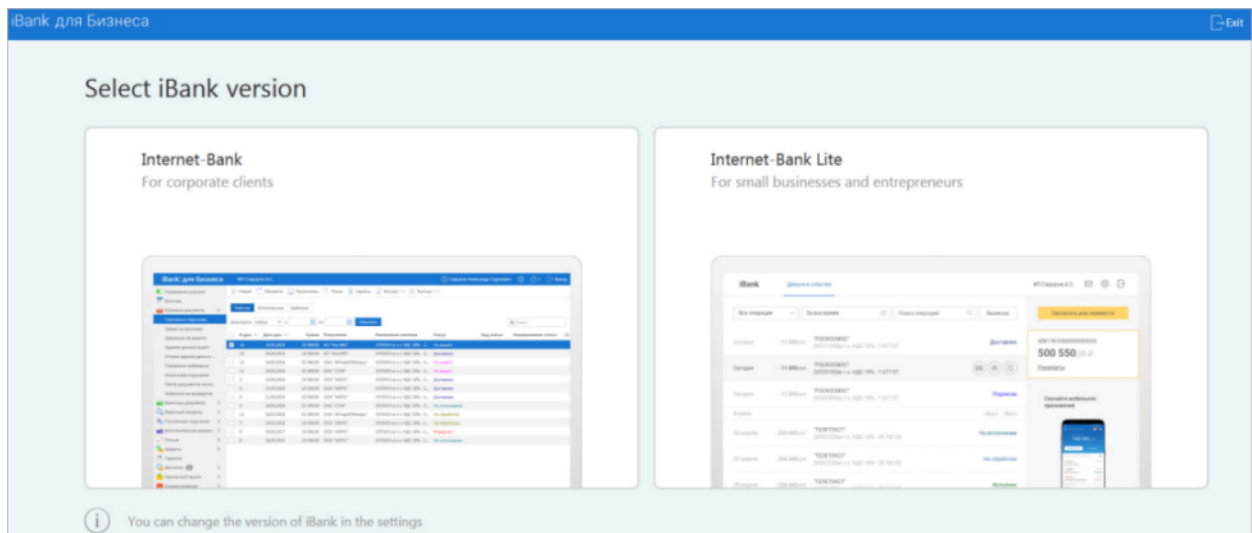
Figure 10. Internet-Bank versions choice

Otherwise, the corresponding "iBank" version will be displayed.

You are able to switch between versions in Settings section.

Working sessions

After authentication the page with the last work sessions will open (see Figure 11).

Figure 11. Working sessions

On the page the following information is displayed:

- Information about today's payment orders – the number of documents in statuses **Delivered**, **Executed**, **Rejected**, **New** (for more details see Document kinds and statuses section);

- Information about incoming documents – the number of new payment requests and collection orders, unread important letters and documents, waiting for acceptance. work in the system will be blocked until the client reads them. When trying to select any section or when accessing to the menu without reading the letter with note **Important** , the following warning message is displayed see Figure 12;
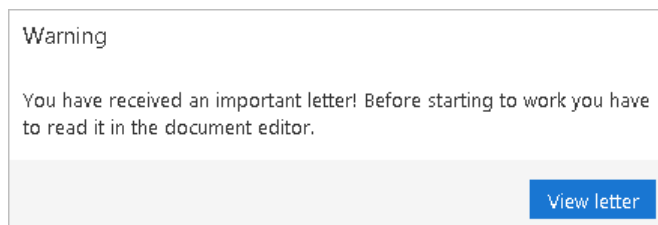
Figure 12. Warning about new important letter

- Advertising banner of the mobile application "Vestochka";

- Information about company's accounts – number, BIC, type, current balance, debit and credit amounts for today. To view the details and account information, click on the line with the required account. Account information page will open (see Figure 13).

Figure 13. Account information

To send requisites to the specified e-mail address, click **Send by e-mail**. In the opened dialog (see Figure 14) specify the e-mail address of the counterparty and click **Send**.

Figure 14. Sending of account info by email

To specify several e-mail addresses click ✚ Add To delete recipient's e-mail address click 🗑

Attention!

This operation is available only if you have rights to the message delivery channel by e-mail.

You can make saving account details in PDF format and printing it by clicking the corresponding buttons.

If the selected account is blocked, information on suspensions/arrests is displayed (see Figure 15). To get complete list of details of the arrests available and account suspensions click ⌄

Figure 15. Information about blocked account

- Information about last work sessions of company's employees in Internet-Bank – name of the ES key owner, which was used for authorization in the service, information about IP-address and region, from which the connection was set.

Get to the page "Work sessions" you can by clicking the logo iBank for Business

If you have not performed any actions in the service for a long time, it will happen session disconnect. Inactivity timeout is set on the side of the bank.

Switching between clients during working session

If you have several ES keys for working with different clients, you can quickly switch between them without logging off the system:

1. Click the button with the name of the current client on the menu bar.

2.
    Choose necessary client from the listbox (see Figure 16). You can use search field ⌕ Search for fast searching of the client (full or a part of name is supported for search). The list contains ES keys stored in the same storage as the ES key used for logging in the system.
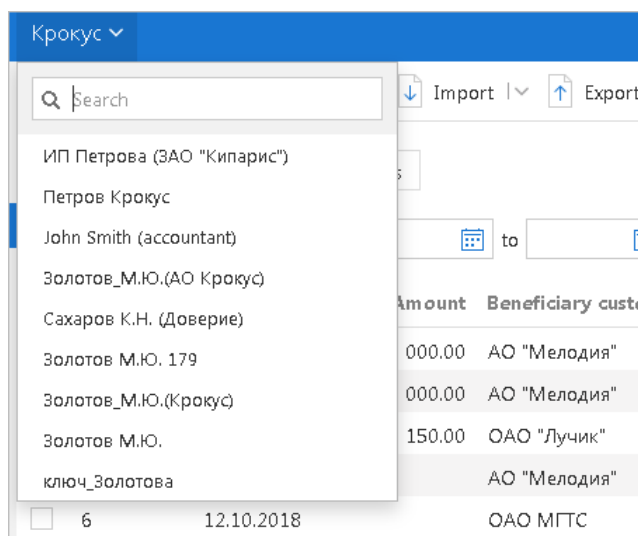

Figure 16. Clients ES keys list

3. Enter the password for the ES key in **BIFIT Signer** dialog box and click **OK** (see Figure 17). If the multifactor authentication is settled for the client, complete the necessary procedures.
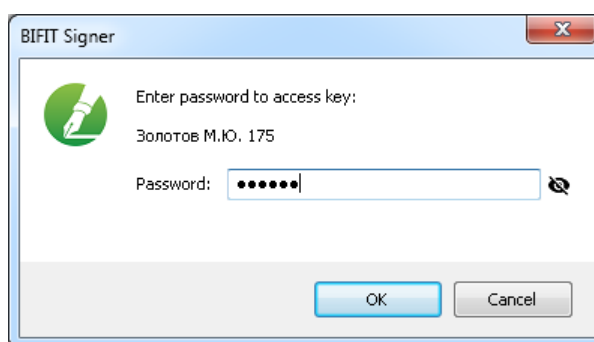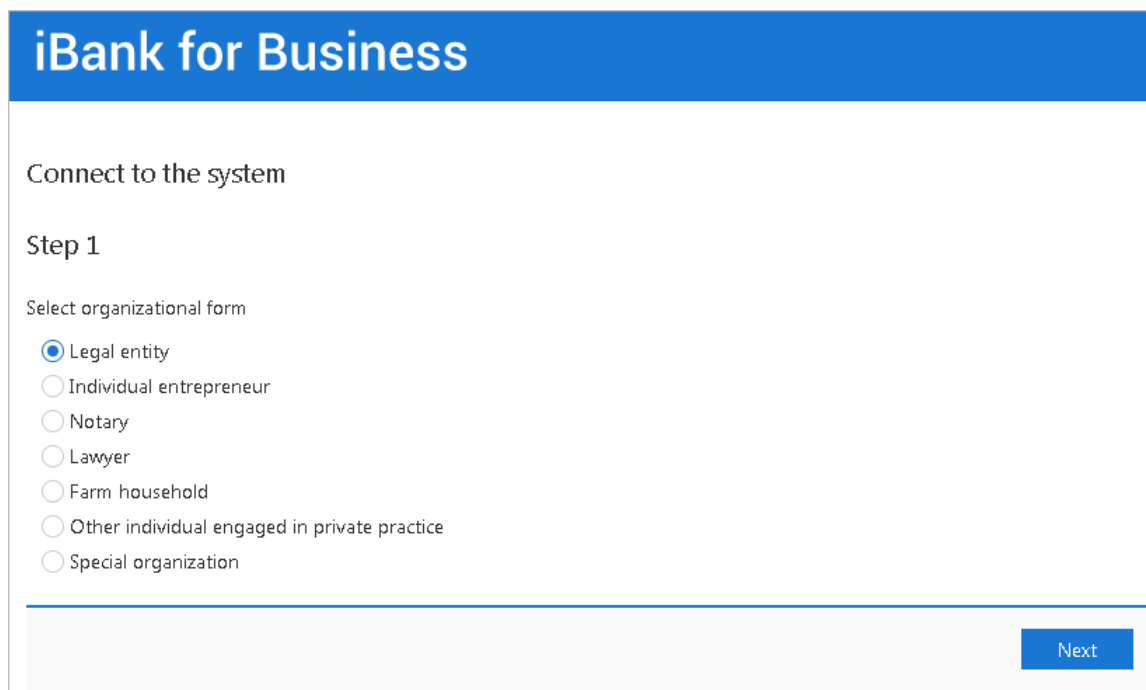

Figure 17. Entering ES Key password

Client registration

To work with Internet-Bank you need to register. At first carry out initial registration via "Internet-Bank for corporate clients", then visit your bank to complete the procedure.

To start the initial registration click the link **Registration** on the login page (see Figure 6) and choose **DBO Connection**. Then complete the steps on the pages **Registration of the new client** (see Figure 18).

Figure 18. Client registration

At registration user specifies organization form of the new client, its details, information about contact person and ES key owner, organisation accounts numbers, opened in the chosen bank. Then he generates ES key and client's ES check key. The ES key is saved on the client-side with the specified name. The access to it is protected by password. ES check key must be initially registered in the bank.

To complete the initial registration user prints out 3 copies of ES check key certificate. One copy is left unfilled to be used as a sample. The rest copies must be filled and certified. They are used as an appendix to the Internet-Bank service contract.

Retention period for information about new registered client is specified by the bank (30 days by default).

To complete the registration client must visit the bank in person with his identity paper and two printed, filled and certified with a stamp and signature copies of the ES check key certificate. Employee of the bank verifies the accuracy of the certificate filling and then activates the ES key. After that the client is able to work with Internet-Bank.

Interface

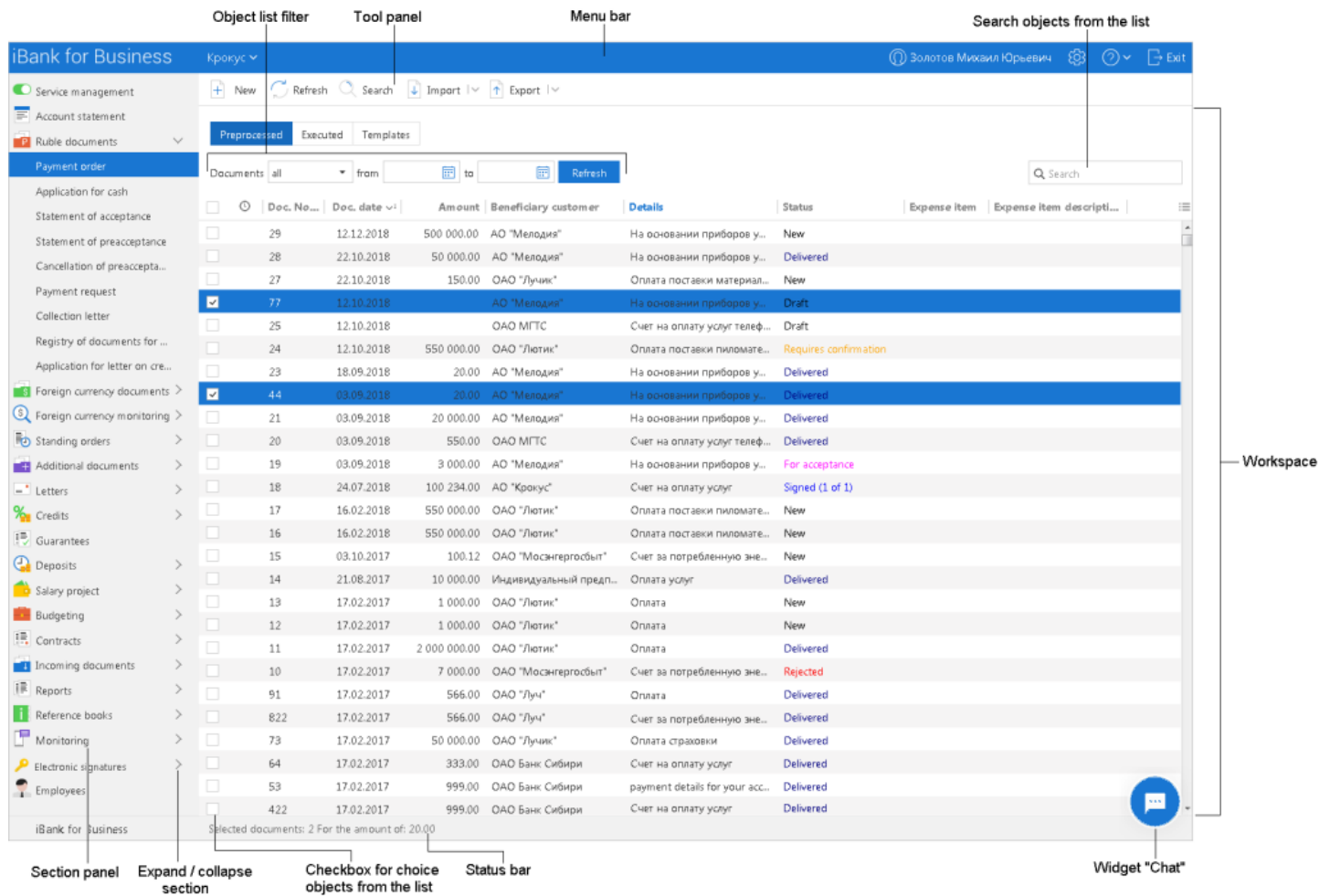Internet-Bank interface consists of tool panel, section panel and workspace (see Figure 19).

Figure 19. Internet-Bank for corporate clients

Menu bar

Menu bar contains the following buttons:

Крокус ∨ — button with the name of the organization, whose accounts are being worked on in current session. Used for quick user change. The button can display the internal name of the organization (for more details see Settings section);

— information about user;

— go to Settings page;

— reference information. Reference information contains a brief user guide, program information and information about bank;

Exit — logout.

Tool panel

Tool panel contains the following buttons:

New — create a new document;

Save — save a new document / save changes in document;

Edit — edit document;

⊗ Cancel — cancel changes in document;

Sign — sign a document;

Confirm — confirm a document;

Reply — create a reply to incoming letter;

Copy — create new document on an existing;

Search — search a document by specified features;

Accept — accept payment request;

Decline — decline payment request;

Import — import a document to Internet-Bank from file created with accounting software;

Export — export a document from Internet-Bank;

Print — print a document;

Delete — delete a document;

Create template — create a template;

Refresh — update shown information.

Section panel

On the section panel are displayed sections for work with documents and services of which you have rights according to your service contract. For example: if you don't have rights to use e-mail, item **Letters** will be absent on the section panel (but if you do not have rights for **Foreign currency documents**, this item will be present on the section panel, but its containing will be disabled for viewing). Use the buttons ❯ / ⌄ next to section's name to expand/collapse it.

Workspace

Workspace includes list of objects and control elements.

Control elements:

> **Object list filter.** Period beginning and end dates are specified in the fields **from** and **to** respectively,

in DD.MM.YYYY format of via 🗓 button. Via drop down list you can filter documents by categories (status groups). Filtering of such kind is only valid within a specific folder. To set uniform filter for all kinds of documents use Internet-Bank settings (see the description in the Settings section).

> **Search the object from the list.** To find a particular object in the list enter the value of one of its details to

the field Q Search It is possible use a part of the value for search. As you type in your search criteria, the objects on the page will begin to filter accordingly.

To find an object by its several details specify them in the search string, press **Enter** key after entering each detail (see Figure 20). It is not necessary to enter a complete value of a detail or follow the order of the columns. Use ✖ to delete a detail.

Figure 20. Search the object in the list

To find a document using a set of criteria click Search

Sort the items in the list. To sort the records in the list by value of one of its columns click on column's header. The action is available for all shown columns. The order of sorting is indicated by mark on columns header: ascending ⌃, descending ⌄ By default objects are sorted by date and number.

To sort records by values of several columns holding **Shift** key pressed click on column's headers. In each header will appear a number, indicating sorting order.

Show/hide columns. To show/hide columns click on the button and put/remove a tick next to the name of an appropriate column.

Broaden a column. To change the width of the column click and drag column's border.

Change columns sequence. To move the column click on its header and drag it to the necessary position. The last columns sequence defined by a user will be retained.

Change the width of the section panel. To change the width of the section panel click and drag panel's border. Last customized width is preserved.

Group operations. To perform a group operation choose several documents in the list and click the button for necessary action.

For more information see section Operations for group of documents.

Widget "Chat"

Depending on the settings on the bank side in Internet-Bank, online chat with bank employees may be available. Messaging is carried out in the special widget "Chat", which displayed over the Internet-Bank page (see Figure 21).

Widget's elements:

, **Enter** — send message to the bank employee;

 — attach files to the message. Maximum file size and formats allowed to be sent are set by the bank;

Shift+Enter — hard line break;

 — close widget menu.
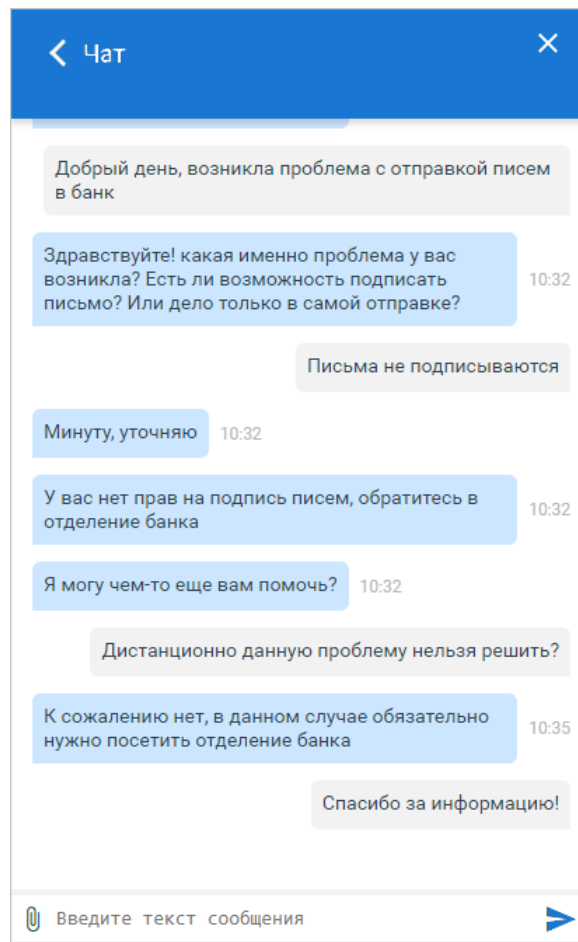
Figure 21. Widget "Chat"

Document form

The main user work with documents (viewing, editing, saving, etc.) performed on page **Document Form** shown at Figure 22.

Figure 22. Document form

Document form page consists of the following elements:

- Tool panel — contains buttons for work with documents. Button assignment is described in Interface section.

- Document sheet — contains form of the document. It has a different appearance depending on document's type.

- Notification settings – available, if the bank has configured notification system. Set the flag **Notify on the document status change** and choose channel type: sms or/and e-mail. Specify the necessary contact information. Use buttons ✚ Add / ✎ to add/edit notification channels.

- Status — index of document processing stage. Click on the relevant link to view document changing history. More details about statuses read in the Document kinds and statuses section.

- Signatures — information about ES under electronic document. Click on the relevant link to view information about signing time and ES key owner. If the document has not been signed the link will be inactive.

- Bank's comments — additional information about the document from the bank. Click on the relevant link opens a dialog box containing additional information about the document added by bank employee . All documents can have bank's comments except documents in statuses **New** and **Signed**.

- Customer's comments — additional information about the document added by the client. Entering comments is available only for documents in statuses **New** and **Signed**, for documents in other statuses only its viewing is possible.

Fields which names are underlined are links. Click on them to call up dialogs associated with them. For example, click **Account** to see the **Select account** dialog.

Hide list / **Show list** — the button for controlling displaying of document list from the current section. Click on document in the list to open its form.

Back to list — use this button to return from document form page to the section main page. Navigation buttons of browser toolbar can not be used to switch between service pages.

Settings

To open settings page click button on the action panel. The page includes the following tabs:
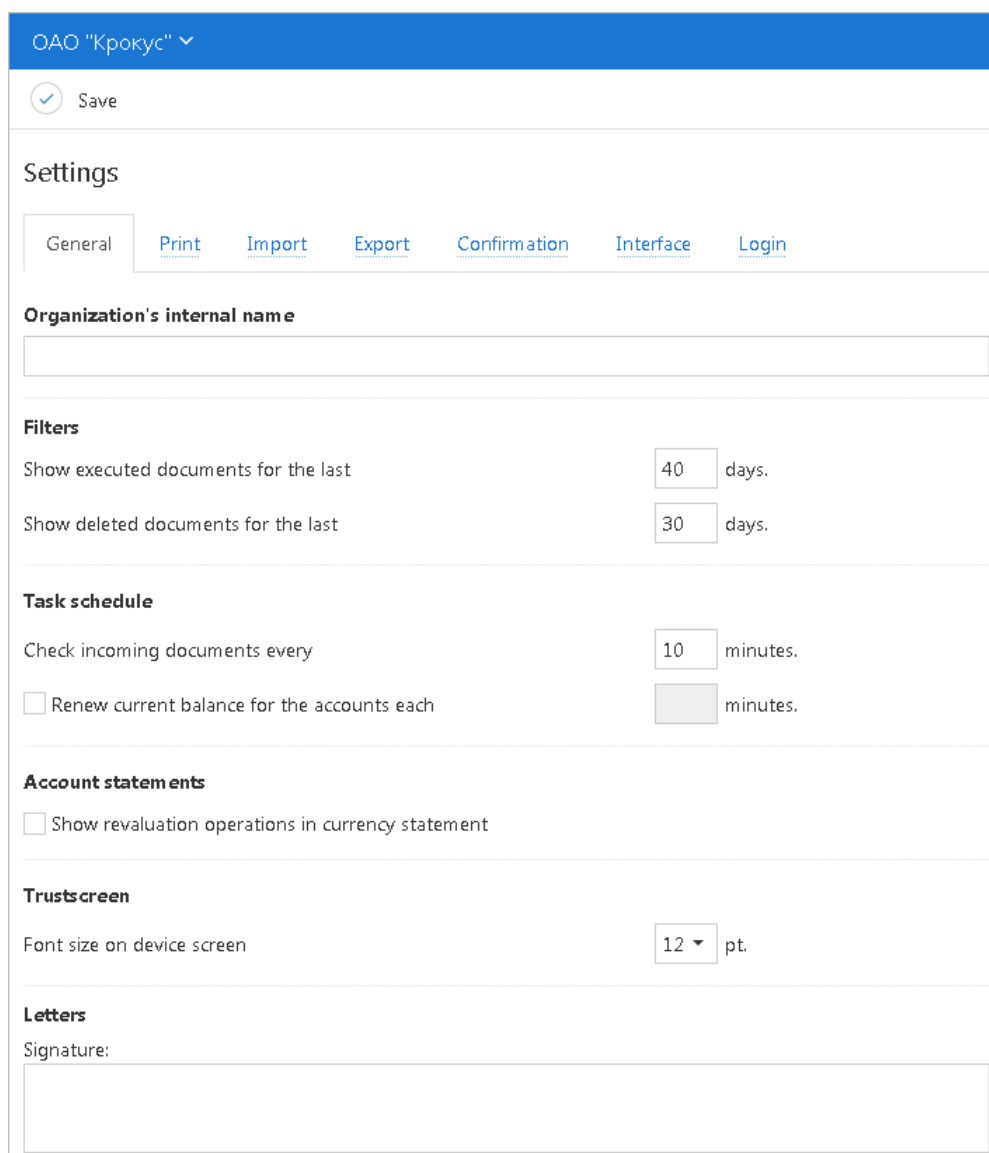
- **General** — documents filter settings; tasks launch schedule settings; signature for letters.
- **Print** — setting the display of additional information when printing documents, setting the print format of ruble and currency statements.
- **Import** — settings of exchange formats of files for downloading to Internet-Bank.
- **Export** — settings of exchange formats of files for uploading from Internet-Bank.
- **Confirmation** — specifying cases and methods of confirmation.
- **Interface** — selection of the appearance of the system "iBank";
- **Login** — settings of "iBank" entrance by login.

Note:

If you work in Internet-Bank from the same PC with several corporate clients, import, export, print and confirmation settings are retained individually for each corporate client. To use individual settings you need to configure and save them once.

Settings description

Tab **General** is shown on the Figure 23.

Figure 23. Tab "General"

The tab contains the following blocks:

Organization's internal name — name assigned to the organization by controlling company at Financial Control Center.

Filters — setting uniform display documents in lists filter. Specify the number of days for which executed and deleted documents will be shown. By default all executed and deleted documents are shown. The filter influences all types of documents.

Task schedule — setting of schedule for launching tasks of automatic check for incoming messages from the bank and accounts balances update. By default the checking is launched every ten minutes.

Account statements — setting display of revaluation operations in currency statement. If the checkbox is selected, statement displays operations for adjusting the exchange rate difference of the balance.

Letters — the text, added in your outcoming messages as a signature at creating a new message or reply to the incoming message. Only one caption text can be set. By default caption text is not set. To the letters created by copying the signature is not added.

Tab **Print** is shown on the Figure 24.

Figure 24. Tab "Print"

The tab contains the following blocks:

Printing of the documents — additional information display for printing documents settings. Choosing page orientation for printing ruble and foreign currency account statements (see Figure 25).

- **Stamp of the bank.** Displaying the following information: bank details and document processing stage (ИСПОЛНЕНО — for executed documents, ПРИНЯТО — for documents in statuses **Delivered**, **Processing**, **At execution**). For documents in statuses **New** and **Signed** the stamp is not printed **[2]**.

  — Bank details and document processing stage (ИСПОЛНЕНО — for executed documents, ПРИНЯТО — for documents in statuses **Delivered**, **Processing**, **At execution**). For documents in statuses **New** and **Signed** the stamp is not printed **[2]**.

  — Bank details for discharge. Bank stamp is not printed statement or for external accounts and with type **Cashbox**.

- **Official information.** Displaying of document ID numbers, ES check key, date and time, when the document obtained status **Delivered**. For documents in statuses **New** and **Signed** official information is not printed **[4]**.

- **Information about ES key owner.** Displaying of surname, name and patronymic name of ES key owner who has signed the document. For documents in status **New** this information is not printed **[1]**.

  In foreign currency documents next to the name of the signer is shown his position, according to the information about ES key owner.

- **Client comments.** Displaying of client's comments to the document **[3]**.

- **Bank's comments.** Displaying of bank's comments to the document **[6]**. Printed only in the next documents:

— Payment Order;

— Transfer Order;

— Interbank Transfer;

— Order for Currency Purchase;

— Order for foreign Currency Sale;

— Order for Currency Conversion;

— Order for Transfer from the Transit Account;

— Order for Compulsory Sale of Foreign Currency;

— Currency operation information;

— Letter;

— Bargain confirmation.

- **Information about the acceptance.** Displaying on the payment order form the stamp confirming the acceptance of the document by FCC. After each acceptance the stamp is supplemented with the name of FCC employee, date and time of acceptance **[5]**.

- **Signers list.** If a document has more than two signatures, the information about two first (in time order) signers is printed on the main document page and full list of signers is printed on a separate page. The full list contains ES keys IDs, ES keys owners names and positions.

  For payment order, letter of credit, payment request and collection order the number of signers on the main page can be increased to three by the relevant setting.

  On printed forms of documents which are not provided with signatures block (only with stamp) signers names and positions are not printed.

Figure 25. Displaying of additional information at payment order print form

Save each document as a separate file — if the flag is set, then simultaneous export of several documents to PDF / RTF files all documents will be saved to different files. If the flag is cleared, then while exporting several documents to PDF / RTF files, all documents will be saved in one file.

Default statement print format — defines print format for foreign currency and ruble statements. It can take the following values:

- **Standard** — print form contains general information about the account, operations list and information about turnovers for the requested period;

For ruble accounts standard statement is printed in portrait orientation, for foreign currency accounts — in landscape orientation.

- **Extended** — print form contains general information about the account, operations list and information about turnovers for the whole requested period and for each day from it;

  Operation list is split on days. Each day starts from a new page. Under operations list there is a table with turnovers for this day.

  On the last page there is a table with turnovers for the whole period.

  Extended statements for ruble and foreign currency accounts are printed in landscape orientation.

- **Brief** — print form contains general information about the account and operations list;

  For ruble accounts standard statement is printed in portrait orientation, for foreign currency accounts — in landscape orientation.

IMPORT — data import settings (see Figure 26). The following formats are available: 1C, iBank2, CSV, DBF and UFEBS. If allowed to save documents in status **Draft**, then at import, all documents containing erroneously filled or blank required fields, imported in status **Draft**.

Figure 26. Tab "Import"

For the import of document "Payroll" may be used an additional format, setted by the bank. Contact your bank to get all the details about this opportunity.

EXPORT — data export settings (see Figure 27). Specifying of exchange files formats, which will be uploaded from the system and the path to the exchange folder. The following formats are available: 1C, iBank2, CSV, UFEBS and Excel.

Figure 27. Tab "Export"

Flag **Export to the single file** allows you to save the received statement for all customer accounts in one file, otherwise — in the export folder will be saved the number of files equal to the number of client accounts with the appropriate name.

Flag **Do not export statement with empty overturns** allows you to upload statements only for those client accounts for which operations were performed for the specified period. Customization carried out for 1C and iBank2 formats.

CONFIRMATION — Specifying cases and methods of confirmation, which will be used to confirmation of the payment orders, trusted beneficiaries confirmation or group payment confirmation (MAC-token BIFIT, MAC-token, SMS, "Vestochka" App, OTP-token). On the tab (see Figure 28) are available the methods assigned to the client.

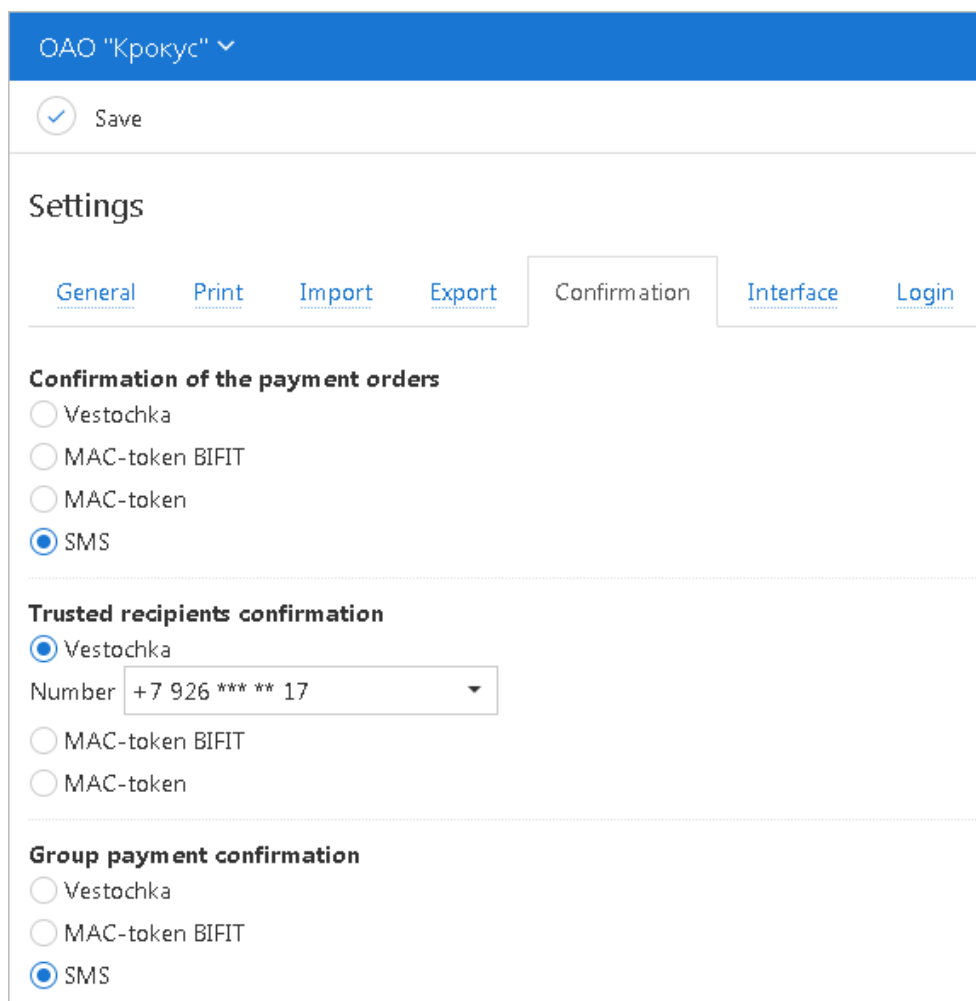**Figure 28. Tab "Confirmation"**

To apply new settings click ⊘ Save button.

INTERFACE — choice of service "iBank" interface.

Attention!

Availability of the tab **Interface** depends on the presence of rights for "Internet-Bank Lite", that is set in consultation and coordination with your bank.
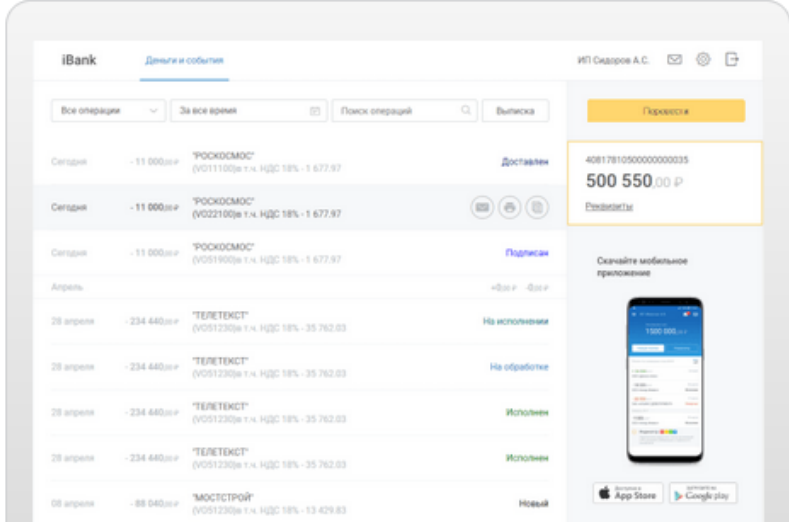
To log on the Internet-Bank Lite click button **Go to** (see Figure 29).

Figure 29. Tab "Interface"

Work with documents

General principles for work with documents in service

In general, the scenario of work with the document is as follows: client creates a document by filling the relevant form, saves it, signs the document with required number of signatures, thereby charging the bank to execute the created document.

For a document can be assigned certain combination of signatures of client's employees, which is necessary for sending the document to the bank.

Signature combination influences document signing scenario and depends on document type:

- **Payment document** — a document, in which as the main account is used the account opened in the bank-the owner of the system. For example, payment order, transfer order and etc.

- **Non-payment document** — a document in which account is not specified or specified the account opened in another bank. For example, letter, deal passport, currency transactions inquiry.

- **Mixed** — a document, in which it is not obligatory to specify the account opened in the bank-the owner of the system. For example, order for foreign currency purchase, currency conversion order.

Signing scenarios for payment and non-payment documents are different:

- Signature combinations for **payment** documents are specified for the account used in the document. The number of signatures in combination can be from 1 to 15.

  The same employee can enter in some signature combinations including related to the same account.

- Signature combinations for **non-payment** documents are specified by the number of signatures set for the document and list of employees eligible to sign this kind of documents. The number of signatures in combination can be from 1 to 8.

The sequence of signing does not matter.

Document kinds and statuses

In Internet-Bank are used the following types of documents:

Outgoing documents — financial documents created by client as his request to the bank to execute certain actions according to the document.

Incoming documents — documents which client receives from the bank. Receiving of incoming payment requirements and collection order is supported.

Statements — account statements formed by client's inquiry.

Letters — messages between the bank and the client. Incoming letters — messages from the bank to client. outgoing — messages from client to the bank.

Reference books — contains information about bank and client details, currency codes and other data necessary for filling in documents. They are intended to ease document creation.

Documents processing stage is characterized by the term **status**. Outgoing documents can have the following statuses:

Draft assigns when creating and saving a new document or importing a document, not passed the check for correct filling fields. After correcting all errors in the document with this status and the subsequent saving the status of the document is changing to **New**. Document with status **Draft** is not processed on the bank side.

New assigns to the documents which have been created and saved, edited or imported. Document with status **New** is not accounted and processed by the bank.

Signed assigned to the documents which have less signatures then required. After editing such document is transferred to the status **New**.

Requires confirmation assigned to payment orders signed by all required signatures if the bank applies additional document protection measures.

To deliver documents to the bank which uses the mechanism of payment orders confirmation client needs to use MAC-token BIFIT or specify confirmation code. The confirmation code can be generated via MAC-token, OTP-token or received via SMS on number registered in the bank.

Delivered assigned to documents signed by all required signatures. The status **Delivered** is designation to the bank to start document processing (to execute or to reject it).

Processing assigned to documents uploaded to the automated banking system (ABS) after passing all checks.

At execution assigned at accepting document to execution.

On acc. 90902 assigned to payment order if there are not enough funds at the account. As soon as funds arrive in the account, they will be written off in accordance to the priority set in the payment order. At carrying out such writings off payslip is formed. If the payment has been partial status **On acc. 90902** will be shown as a link. Click it to view information about all payments connected with the payment order.

Executed assigned to the document at his execution by the bank and creation of accountant entry.

Rejected assigned to the document not accepted to execution. Client can edit and save the document (it will be transferred to the status **New**) or delete the document (it will be transferred to the status **Deleted**).

Deleted assigned to the document deleted by client. Only documents in statuses **Draft**, **New**, **Signed**, **Rejected** can be deleted. Documents in statuses **Draft**, **New** and **Signed** are deleted irrevocably. Documents deleted after rejection can be viewed using filter on information panel. Documents in the status **Deleted** displayed in Internet-Bank according to its settings (see Settings).

Basic operations on documents

To perform any operation on a document you need to choose document category, type and folder. Any operation can be performed by one of the following ways:

- Via tool panel: highlight the document and click on tool panel the button relevant to the required operation.

- Via context menu: highlight the document, call up the context menu and choose the item relevant to the required operation.

- At the document form page (see Figure 30). Use tool panel buttons.

Figure 30. Payment order document form page

Basic operations on document are the following:

Document creation

To create a new document fill in the form and save it. At saving the document is checked on Application Server: whether all necessary fields are filled correctly. If errors occurred while saving the document (not filled required field, incorrect field value), an error message displayed on the screen with the indication causes of error will appear (see Figure 31). Such a document can be edited or saved as a draft.

Figure 31. Error message

Any client's employee has an access to all documents on which the client has rights. The access does not depends on signature combination in which the employee is included or rights on documents assigned to him. Any employee can create, save and view previously created documents.

In addition to the methods listed above new document can be created by copying of previously created document.

To do this open the necessary document and click [ ] Copy : the system will create new document with fields filled with values from the original.

Document editing

Only documents in statuses **Draft**, **New** and **Signed** can be edited.

Document in status **New** can be edited or deleted by any client's employee if the client is eligible for work with this type of documents. Partly signed document can be edited by any employee whose signature belongs to the same combination as signatures of previous document signers. After such editing all the signatures under the document will be deleted. If an employee who has signed the document is deprived of the right to sign documents of this type or his signature is excluded from the combination of signatures, and the document has not yet received the status of **Delivered**, the document becomes unavailable for signing, but it can be edited by any client employee in case he possesses the rights to work with this type of documents.

Document signing

Attention!

During the signing of document the hardware device containing ES keys (Rutoken EDS 2.0, MS_KEY K – Angara) must be connected to the computer.

The number of signatures necessary for document acceptance to consideration by the bank is defined by settings specified on the bank server.

Corporate client employees with the right to sign documents are separated on signature combinations. More details see at signature combinations [35].

According to the document type, employee's rights to sign it can be defined by:

- for **payment** documents rights are specified for the account, used in the document;
- for **non-payment** documents rights are specified by the number of signatures set for the document and list of employees eligible to sign this kind of documents.

As soon as the document which requires more than one signature is signed, it gets status **Signed**. After all required signatures are collected, the document gets status **Delivered** or **Requires confirmation**.

Note:

On the bank side, limits can be set to limit the amount of one-time payment and general day and month payments. If the signature of the payment order reveals an excess of one of the established limits, the error message will appear. Such a document it will be possible to send to the bank only after the expiration of the period in which the limit is exceeded, or you can reduce the amount and make a partial payment.
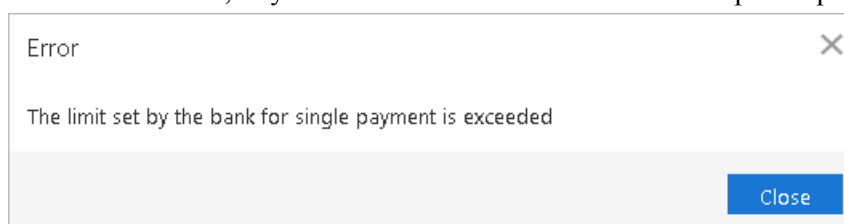
When calculating limits, the amounts of documents per day / month in status **Delivered** or higher.

You can find out the limits set for your organization by contacting your bank.

Payment order confirmation

Action is intended for additional protection of client's electronic orders and can be used in addition to ES.

If the amount of the order exceeds set limit, client needs to use an additional confirmation code. Status changing will be as following:

New → Signed → Requires confirmation → Delivered → ...

Confirmation can be performed via MAC-token BIFIT or by confirmation code. The code can be generated via "Vestochka" App, MAC-tokens, OTP-tokens or received in SMS message on number registered in the bank.

Document confirmation is available only for payment orders.

Document confirmation is done after the document is signed by the required number of signatures. Confirmation can be performed right after signing or later.

Payments in favour of trusted beneficiaries, which do not exceed set limits, do not require additional confirmation (see Work with trusted beneficiaries).

If payment amount exceeds the limit and the correspondent does not belong to the list of trusted beneficiaries, the warning will appear (see Figure 32).

Figure 32. Overlimit

Set the switch to the upper position to add the beneficiary to the list of trusted beneficiaries or to the down position to confirm only current payment order (see Figure 33).

Figure 33. Payment order confirmation

Payment order confirmation

1. The method of receiving is specified according to the settings (see Settings).

2. Receive confirmation code with one of the methods.

MAC-token

MAC-token can generate confirmation code in two modes: medium and standard. Depending on the mode chosen, the device produces different data. Generation mode is specified by the bank.

Generation in *medium mode* requires beneficiary's bank BIC, beneficiary's account number and document amount.

Generation in *standard mode* requires session ID, document number and last six digits of beneficiary's account.

Medium mode	Standard mode
1. To turn on MAC-token press key ⏻ on its keyboard	
2. On the display appears the message "ВВЕДИТЕ ПИН". Enter PIN code	
3. After entering correct PIN-code on the display will appear the message "ВЫБРАТЬ"	
4. Press on the keyboard button **"2"**	4. Press on the keyboard button **"3"**
5. On the display appears the message "БИК БАНКА". Enter beneficiary's bank BIC and press ⏻	5. On the display appears the message "ИД СЕССИИ". Enter session ID from confirmation form and press ⏻
6. On the display appears the message "Счет 1...10". Enter first ten digits of beneficiary's account and press ⏻	6. On the display appears the message "СУММА". Enter the whole amount (without copecks) and press ⏻
7. On the display appears the message "Счет 11...20". Enter the rest ten digits of beneficiary's account and press ⏻	7. On the display appears the message "ПАРАМЕТР 1". Enter last six digits of beneficiary's account and press ⏻
8. On the display appears the message "СУММА". Enter the whole amount (without copecks) and press ⏻	8. On the display appears the message "ПАРАМЕТР 2". This parameter is not used in standard mode. Press ⏻
9. On the display appears confirmation code, which is necessary to enter to the relevant field on the document form	

SMS Click **Receive code on SMS**. On the mobile phone number registered in the bank will be sent message with confirmation code. Make sure that details in SMS message match with details of the confirmed document.

OTP-token Press the button on the OTP-token. On the display appears a numeric sequence (the confirmation code).

3. Enter the code to the relevant field at the confirmation dialog and click **OK** to transfer the document to the bank for execution or **Cancel** to turn down the confirmation.

Confirmation of payment order by mobile application "Vestochka":

1. On the screen of smartphone in mobile application "Vestochka" will appear the message is as follows:

```
Подтвердите платежное поручение:
Запрос № 41
П/п № 54
Сумма 800 руб.
БИК 044525311
```

Счет 40702810300180001774

Carefully check that the details on the smartphone screen match the details of the confirmed document.

2. Click the button **Confirm** to confirm the operation or **Cancel** to turn down the confirmation.

If confirmation period is expired, press the button **Send a new request** or choose another confirmation type by pressing matching link (see Figure 34).

Figure 34. Confirmation of payment order by "Vestochka" App

Confirmation of payment order by MAC-token BIFIT:

1. Click the button **Confirm**.

2. On the screen of the MAC-token BIFIT appear key details of the confirmed document: type, date, number, amount and recipient's details. Make sure that details on the MAC-token BIFIT match with details of the document being confirmed (see Figure 35).

Figure 35. Key details on the screen of the MAC-token BIFIT

3. To confirm the operation press the button ✔ on the MAC-token BIFIT case, to cancel — ✖

If the button ✔ is not available (there is no relevant button on the device screen), scroll down the document using ▲ / ▼ buttons on the device case.

It is possible to confirm a group of documents by one confirmation code received on SMS or generated by OTP-token (opportunity of such confirmation is defined by the bank).

Document group confirmation:

Select from the list documents for confirmation and click the button **Confirm**.

> **SMS**

In the dialog **Confirmation of the payment orders** is shown the number of confirmed documents and their total amount (см. Figure 36).

Figure 36. Payment orders confirmation via SMS

SMS message with a confirmation code contains details with the number of confirmed documents and their total amount.

> **"Vestochka" Application**

1. If some of the document are not able to be confirmed dialog with list of all documents will appear (see Figure 37).

Figure 37. Document group confirmation

To confirm the documents, that have passed the check click button **Continue**.

2. On the screen of smartphone in mobile application "Vestochka" will appear the message is as follows:

   Подтвердите платежные поручения:
   Запрос No 65
   Количество п/п 2
   Общая сумма 11862 руб.

   Carefully check that the details on the smartphone screen match the details of the confirmed document.

3. Click the button **Confirm** to confirm the operation or **Cancel** to turn down the confirmation.

   MAC-token BIFIT

1. In the dialog **Confirmation of the payment orders** click the button **Confirm**.

2. On the screen of the MAC-token BIFIT appear parameters of the group of documents being confirmed: the number of documents and their total amount. Make sure that parameters on the MAC-token BIFIT match with parameters of the documents being confirmed (see Figure 38).
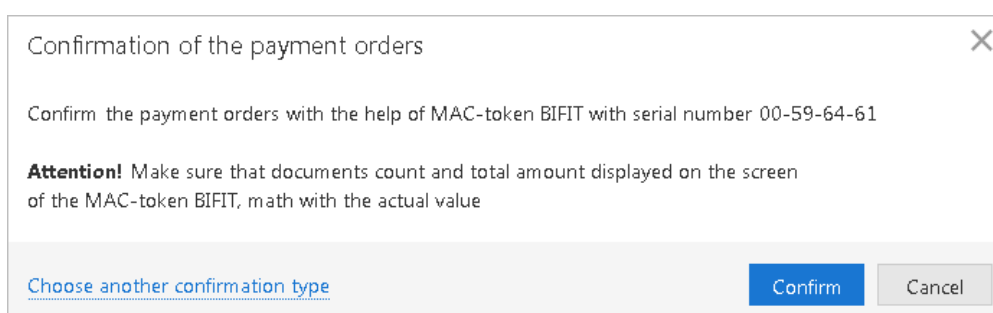
Figure 38. Confirmation of the payment orders

3. To confirm the operation press the button ✔ on the MAC-token BIFIT case, to cancel — ✖

If the bank does not allow **group confirmation**, use **sequential confirmation**:

1. Select from the list documents for confirmation and click the button **Confirm**.

2. In the dialog **Confirmation of the payment orders** click the button **Confirm**.

3. The dialog **Confirm documents** appears (see Figure 39). Confirm the documents sequentially, comparing document's details in the dialo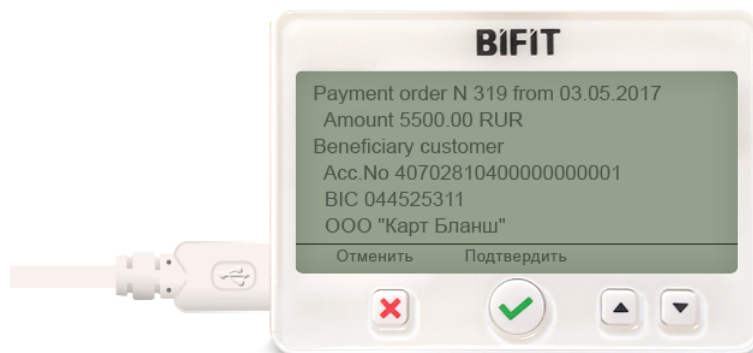g and on the screen of the MAC-token BIFIT. To confirm the operation press the button ✔ on the MAC-token BIFIT case, to cancel — ✖
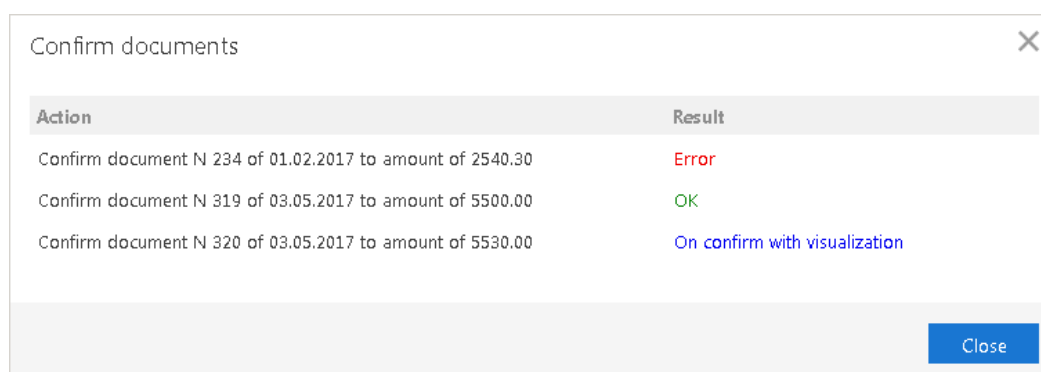
Figure 39. Confirm documents

Sending payment orders by e-mail

Attention!

Sending payment orders by e-mail can be unavailable according to the system settings set by the bank.

Print forms of the payment orders can be sent by e-mail directly from AWP "Internet-Bank". For example, you can send necessary documents to your counterparty to confirm the fact of the payment.

1. In the section **Ruble documents → Payment order** select the documents for sending and choose the item **Send by e-mail** in the context menu.

   One message can contain up to 50 documents.

2. • In the dialog **Sending documents by e-mail** specify recipients' e-mail addresses. Use buttons ✚ Add / 🗑 to add/delete recipients (see Figure 40).
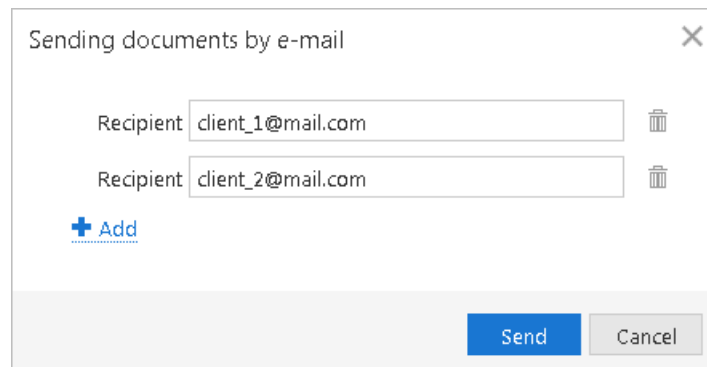
Figure 40. Sending documents by e-mail

3. Click **Send** button.

Export

In the current version of the service is available uploading of the following documents:

- 1C, CSV, iBank, UFEBS and Excel formats:

  — Statement.

- 1C and CSV formats:

  — **Salary project**. List of employees.

- CSV format:

  — **Budgeting**. Budget report, Budget item operations;

  — **Monitoring**. General report, Detailed report on client.

- iBank2 format:

  — Account statement addendum;

  — Incoming letters;

  — Reference book **Correspondents**;

  — Reference book **Beneficiaries**;

  — **Budgeting**. Payment calendar accomplishment.

- Excel format:

  — Register of payment orders.

To export a document go to the section relevant to its type and click the button ⬆ Export |ˇ on the tool panel. Before export make sure that export settings is specified a folder for document uploading (see section Settings). If the folder is not specified, service display a message error with a suggestion to set up a folder for sharing.

Import

In the current version of the service is available downloading of the following documents:

- 1C format: Payment order, Payment request, Payroll, Application for card issue, External account statement.

- UFEBS format: Payment order.

- iBank2 format:

— All ruble documents except:

Register of documents for collection.

— All foreign currency documents except:

Currency conversion on on-line courses;

Order for foreign currency reverse sale.

— All foreign currency monitoring documents except:

Currency receipt information.

— All **Salary project** documents except:

List of employees.

— All **Budgeting** documents except:

Payment calendar accomplishment.

— **Contract** documents:

Contract terms;

Payment order with contract.

— Outgoing letters;

— Information on beneficiary;

— Reference book **Correspondents**;

— Reference book **Beneficiaries**;

— External account statement.

- In CSV and DBF formats is available downloading of the same documents as in iBank2 format except:

— Statement for DP renewal;

— Statement for DP closing;

— Currency transactions inquiry;

— Confirming documents information;

— Information on beneficiary (legal entity);

— Budget transaction basis;

— Budget order;

— Creating/adjustment/distribution of budget transactions;

— Application for payment;

— Payroll.

Downloading with some restrictions in format DBF is available for the following documents: Contract deal passport, Loan deal passport, Transfer order. Restrictions apply to the fields with lists which are not obligatory.

- Special format set by the bank: Payroll (presence and name of this import option is set by the bank).

To import a document go to the section relevant to its type and click the button ⬇ Import |⌄ on the tool panel. Before import check that exchange folder contains files of the same format, that specified in import settings (see section Settings). If the folder is not specified during the import operation, a standard dialog opens to select folders.

Document print form preview

To view document print form before printing choose the item **Preview** in the context menu or in the menu available by the button 🖨 Print |⌄

Saving document in RTF format

To save document print form in RTF format choose the item **Save as RTF** in the context menu or in the menu available by the button 🖨 Print |⌄

Document deleting

To delete a document use the button 🗑 Delete or relevant item in the context menu. You can delete documents with statuses **Draft**, **New**, **Signed** and **Rejected**. This action can be performed using the context menu (item **Delete**) or using button at the tool panel.

Operations for group of documents

Some operations are available for group of documents. Highlight documents using the appropriate method:

- To highlight successive documents in the list click on the first document, and holding **Shift** key click on the last document.
- To highlight separate documents in the different parts of the list click on them holding **Ctrl** key.

For group of documents the following operations are available:

- **Export** to RTF format. For each highlighted document file with print form will be created.
- **Document sign** Signing process is displayed in separate dialog. Document signing can result into error if document has inappropriate status or contains mistakes (for example, document date is less than current date). To view error details occurred at document signing double click on relevant line at the **Signing of document** dialog.
- **Preview** of document printing form.
- **Printing** of documents.
- **Deleting** of documents.

Templates

For some types of documents can be created templates for further using. Template is a partly pre-filled document form which can be used for creation of unlimited number of documents. Its usage eases the procedure of new document creation.

Clients can create, edit, delete templates and use them to create new documents.

To create a template do the following:

1. Go to the tab **Templates** at the relevant document page and click ⊞ New or context menu item **Create template**. Or open document form page and click the button ☆ Create template on the tool panel.

2. In the dialog **Template name** enter template name and click **OK** (see Figure 41).
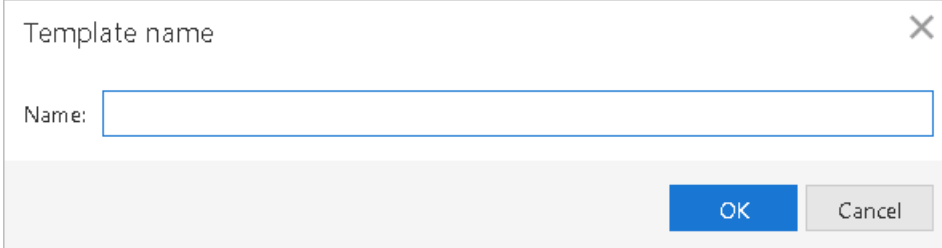
Figure 41. Template name

3. Fill in the fields which will be constant in documents based on the template and click the button ⊘ Save

During saving a template (as opposed to other documents), there are no checks for mandatory field fillings, however, checks for field lengths (maximum or fixed) are kept and their contents (any characters or only numbers). Fields **Date** and **Document number** is automatically cleared.

To create a document based on a template do the following:

1. Open template form for editing using one of the following methods:

   - On the template page click the button ▢ Create document

   - Highlight the necessary template in the list and choose in the context menu item **Create document**.

2. Fill in or edit necessary fields.

3. Save the document and sign it if necessary.

Revocations

You can revoke documents in statuses **Delivered**, **Processing**, **At execution**. To revoke document do the following (see Figure 42):

1. Highlight document in the list and click item **Revoke**.

2. If necessary, edit the number and date of withdrawal. Fields of the reclaimed Document Form are not available for editing.

3. Specify the reason for the revocation in the appropriate field.

4. Save and, if necessary, sign the document.

Figure 42. Document revocation

Almost all fields will be completed automatically and will not be available for editing. You can change document's number and date. Specify the reason of revocation in the relevant field.

Account statement

In the section **Account statement** you can receive and view account statements for your bank accounts.

Figure 43. Account statement section

To receive statement account do the following:

1. On the information panel specify bank, account and statement's period.

   If the field **from** is empty, a statement will be formed from the account opening date. If the field **to** is empty, a statement will be formed up to the current date. If both fields **from** and **to** are empty, a statement will be formed for all account existence time.

Figure 44. Select account

2. Click **Get**.

Use filter to get statement for operations suiting to given conditions. Click the **Filter** button, set filter criteria and click **Get** (see Figure 43).

If statement end date is greater than the date of the last closed operation day, the **Preliminary statement** will be get.

If necessary, you can perform authentication of bank employee's ES key under uploaded statement or entry. For more details see **ES check utility** user guide, which is included to the utility installation package.

If the statement is got for foreign currency account and there is account statement addendum, you can view it by clicking the link Primary documents in the **Information on transaction** page.

Statement printing

To print a statement click 🖨 Print on the tool panel, or press **Ctrl+P** or click **Print → <Print format>** in context menu. Print formats are equal to ones described in the section Settings.

Statement export

To export statement use button ⬆ Export |˅ or relevant items in the context menu.

There are five modes for statement export:

- Export in the format, specified as common in the Settings with a choice of fields for uploading. Performed by clicking ⬆ Export or first item **Export** in the context menu.

- Export to the folder different from one specified in the Settings with choice of format (1C, iBank2, CSV). Performed by the item **Export as** in the context menu.

- Export to the folder specified in the Settings with choice of format (1C, iBank2, CSV, UFEBS, Excel). Performed by clicking |˅ part of ⬆ Export |˅ button or third item **Export in** in the context menu.

- Export account statement with bank employee's ES:

  1. In context menu click **Export statement with ES**.

  2. The system will offer to specify the way to the exchange folder, ES check key ID will be saved to the same catalog. By default statement is exported in iBank2 format. File with ES check key ID gets a name `<key_id>.xml`, where `<key_id>` — is ES check key ID.

  3. If entries and statement have different ES, the number of files with ES check key ID in exchange folder will match the number of ES key used for signing.

- Export account statement for selected accounts:

  1. In context menu click **Export for selected accounts...**

  2. In dialog **Select account** choose accounts and click the **Export** button (See Figure 45).
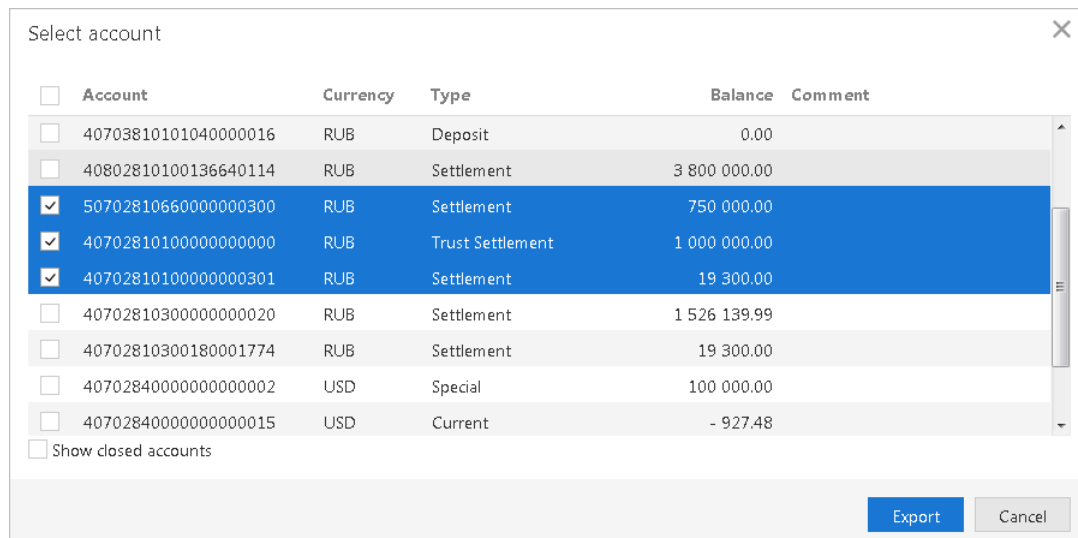
Figure 45. Select account

Viewing information on transaction

To view information on transaction from statement double click on needed operation (see Figure 46).

On the page **Information on transaction** for ruble settlement account you can create payment order by clicking **Create document**.

Entry signed with bank employee's ES can be exported:

1. Open for viewing necessary entry and click **Export** (see Figure 46). If the button is inactive contact your bank for instructions.

2. Information about entry and ES check key ID is saved to the folder specified in the AWP settings (tab **Export**, block **Common**), otherwise the system requires to specify the folder for saving. By default entry is exported in iBank2 format. File with ES check key ID gets a name `<key_id>.xml`.

To print separate payment documents from statement perform any of following actions:

- highlight required documents in the list and click **Print → Documents** in the context menu;

- in the page **Information on transaction** click the button **Print** or press **Crtl+P**;

- highlight required documents in the list and click **Preview → Documents** in the context menu. Then click **Print** to print them out.

Figure 46. Page "Information on transaction" for ruble account statement

Letters

The system provides the possibility of letter exchange between client and bank. Clients can use this channel to send to the bank inquiries and claims regarding their bank operations. Whereas the bank can reply to client's letters, inform clients about new products and services and etc.

On the section panel letters are grouped in the following folders (see Figure 47):

Incoming — letters received from the bank.

Outgoing — letters sent to the bank. The folder includes three tabs:

- **Preprocessed** — client letters drafts and letters rejected by bank operator. Relevant statuses — **New** and **Rejected**.

- **Sent** — letters sent to the bank. Relevant statuses — **Delivered**, **Processed**, **At execution**, **Executed**.

- **Deleted** — letters rejected by the bank and deleted from the folder **Preprocessed**. Can be in **Deleted** status only.

Figure 47. List of incoming letters

The list of incoming letters located in the workspace is presented as a table with following fields:

- ★ — sign marking letters by the client. To affix a mark (for example, for further coordination with management) click sign ☆ near the chosen letter;

- **Important letter** — a sign of the type of letter. If the incoming letter has the form **Important** sign ❶ will be displayed in the appropriate column;

- **Attach** — sign of the presence of files attached to the letter. If the incoming letter has attach sign 📎 will be displayed in the appropriate column;

- **Date** — date of dispatch of the letter;
- **Subject**.

To view a letter choose it from the list (see Figure 48).
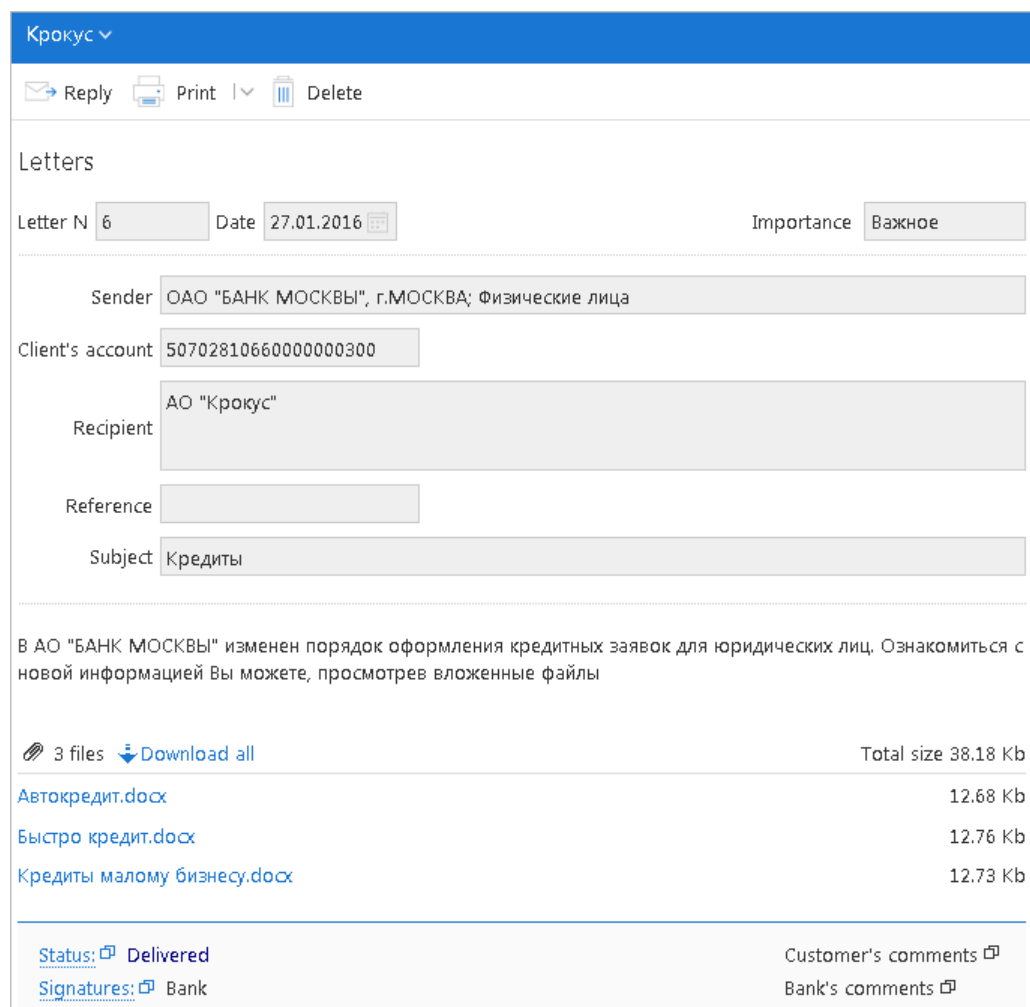
Figure 48. Letter viewing

To view the list of attached files click the relevant link **Files**.

To save file attached to the letter, select it and click the **Receive** button. To save all letter attachments click **Receive all**.

To reply incoming letter click At answer creation a signature text can be added automatically. See more at Settings.

Outgoing letters are created on the **Preprocessed** tab.

To attach files use the link Files. In the dialog **Files** click **Attach**. The maximum attachment size is specified by your bank.

At outgoing letter signing its attachments are signed too, i.e. letter and its attachments are compose a single entity. Signed outgoing letters get status **Delivered** and are transported to the folder **Sent**.

To delete the letter click

Reference books

Reference books contain information about banks and correspondents details, currency codes and other data, which is frequently required at document filling up.

System reference books

System reference books are reference books which are controlled and updated by the bank:

- Banks of Russia;
- SWIFT banks;
- BCC;
- Currency rate:
    - — Bank currency rates;
    - — CB and MICEX rates.
- Country reference;
- Currency reference;
- Currency operations codes reference;
- Currency purchase base reference.

System reference books are used to ease the process of document filling up (for example, after bank BIC is specified the rest bank details will be automatically filled according to the ruble details reference book). Reference books not shown on the section panel such as **Currency reference** or **Country reference** are available at filling relevant fields in a document (for example, fields **Currency**, **Country** and etc.).

User reference books

User reference books are created by user for his own needs. To this category are related:

- **Correspondents** — correspondent ruble details;
- **Beneficiaries** — correspondent foreign currency details.

User adds records to his reference books by himself. Work with reference books records (adding, editing, deleting) is equal to work with outgoing documents.

Work with trusted beneficiaries

Functionality **Trusted beneficiaries** allows user to create the list of contractors in the benefit of which payments are made regularly. Client can set individual payment limit for each beneficiary. Payments which do not exceed individual limit are made without additional confirmation and at once get status **Delivered**.

Attention!

To work with **Trusted beneficiaries** you need to have special rights.

Choose on the section panel **Trusted beneficiaries** reference and its content will be displayed at the information panel (see Figure 49).
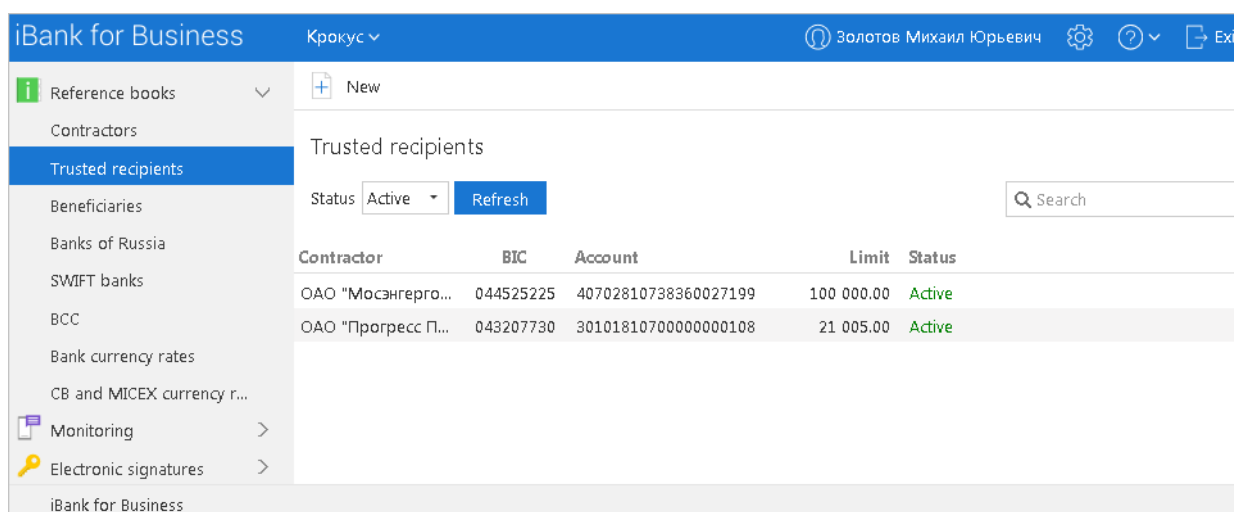
Figure 49. "Trusted beneficiaries" reference book

The list contains the following information about beneficiary:

- **Correspondent** — payment recipient name;

- **BIC** — payment recipient bank BIC;

- **Account** — payment recipient account number;

- **Limit** — payment limit set for this beneficiary;

- **Status** — payment recipient number.

On the upper part of information panel there is a filter for the **Status** field. It can take the following values:

- **All** — displays beneficiaries in all statuses;

- **Active** — displays list of beneficiaries in status **Active**. Used by default;

- **Deleted** — displays the list of beneficiaries in status **Deleted**.

To add new beneficiary to the list of trusted click ⊞ New or item **Create** in the context menu.

Depending on the number of confirmation methods set in the AWP settings, new trusted beneficiary creation will consist of one or two steps.

Enter new beneficiary details in the dialog **Add trusted beneficiary** (see Figure 50).

Figure 50. Trusted beneficiary adding

- In the field **Beneficiary** specify payment order recipient or choose it from **Correspondents** reference available at link Beneficiary. Fields **BIC** and **Account** will be filled automatically with data presented in information about correspondent. Otherwise specify account and BIC manually.

  Beneficiary's name in the **Trusted beneficiary** reference book may differ from its name in payment order. The main trusted beneficiary's details are its BIC and account.

- To set limit for beneficiary tick the relevant flag and specify the amount. If the payment order amount does not exceed the limit, the transaction will not require additional confirmation. Otherwise you need to confirm the payment order or change the limit for its beneficiary.

- Click the button **Next**.

- Confirm the operation. Confirmation procedure is similar to confirmation of payment order (see section Payment order confirmation).

- Click **OK** to save new trusted beneficiary or **Cancel** to abort the procedure.

To edit a record in the reference book double click on it. You can change only the limit amount set for this trusted beneficiary. Fields **Beneficiary**, **BIC** and **Account** are uneditable.

To change trusted beneficiary's status click the relevant item in the context menu:

- **Activate** — to reactivate the beneficiary in the status **Deleted**.

- **Delete** — to delete trusted beneficiary in the status **Active**.

Status **Deleted** means that beneficiary is not trusted any more and its individual limit does not considered. Such records are not deleted from the reference. You can activate them in future.

To view statuses history click item **History** in the context menu (see Figure 51).

Figure 51. History

On the page **History** the following data is displayed:

- **Time** — revision time and date;

- **Status** — trusted beneficiary's status;

- **ES check key ID** — ES check key ID owned by employee who has made the changes;

- **ES check key owner** — name, surname and patronymic of employee who has made the changes;

- **Description** — at limit change in the column **Description** are specified old and new amounts.

Trusted beneficiary can be also added from the reference book **Correspondents**. To do this highlight the record in **Correspondents** reference and click item **Add to trusted** in the context menu. The dialog **Add trusted beneficiary** will appear. Check the details and set limit if necessary.

Electronic signatures

Section **Electronic signatures** (see Figure 52) offers the following opportunities:

- View list of organisation's employees ES keys;

- Creation of new ES keys;

- Administration of requests and ES keys:

    — Confirming requests to use or receive keys;

    — Change of password for access to the ES key;

    — Change ES key name;

    — Removal ES key.

- Print ES keys verification certificates for employee ES keys;

- Change PIN-code of hardware devices with ES keys.
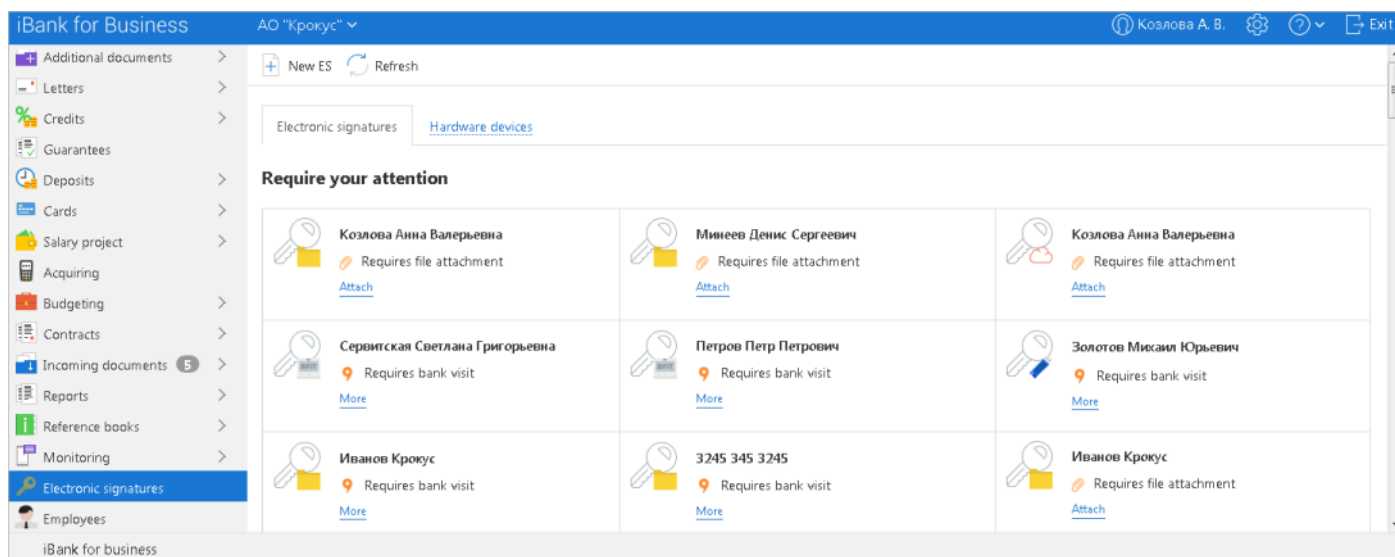
Figure 52. Employees ES keys information

View ES keys information

Information about ES keys and hardware devices is situated on following tabs:

- **Electronic signatures**;
- **Hardware devices**.

On the tab **Electronic signatures** is displayed the following data:

- **Owner** — ES key owner full name;
- **Status** — current ES key status;
- **Link** — link for details ES key page.

On the tab **Hardware devices** is displayed the following data:

- **Device name** — name of connected ES keys store;
- **Device ID** — hardware device ID;
- **Link** — link for details hardware device page.

Print ES key validation certificate

For printing ES key validation certificate choose ES key from the list and click ☐ Print

Creation of new ES keys

Employees, who already have ES keys, are able to create new ES keys themselves. For other employees ES keys are created by **Administrator**[2].

Depending on the settings on the bank side, issuing the ES key validation certificate for ES keys, that created in this section may or may not require a visit to the bank of the owner of the ES key. Scenario issuing a ES key validation certificate is determined by:

- Employee status — **Active** or **Blocked**;

- Status in the details system of the employee's identity document (relevant, not relevant);

- ES key standard (GOST34.10-2001, GOST34.10-2012).

ES key creation includes the following steps:

1. Click button ☐ New

2. Perform all steps of the ES keys creation wizard, following the instructions contained in them.

3. According to the results of passing all the steps of the ES key creation wizard, the ES key validation certificate with pre-filled application is automatically created. Complete the design statements:

   - Notice the bank to which the application should be sent;

   - If a visit to the bank is not required, a list of documents that scanned copies of which should be attached to this application as attach;

   - Sign the statement.

After the application is executed and the ES key is activated on the bank side new key is enabled to work in the system "iBank".

---

[2]Responsible employee of the client to whom the bank granted the rights to manage work in the system of other employees.

Multifactor authentication

Multifactor authentication is designed to improve the security level by using one time passwords.

Using multifactor authentication corporate client has to confirm logging to the AWP by specifying one time password or by mobile application "Vestochka" or MAC-token BIFIT.

One time password can be generated by MAC-token, OTP-token or received by SMS, sent on number registered in the bank. Dialog for choice confirm type appears at logging the system after ES key choice and its password entering (see Figure 53).
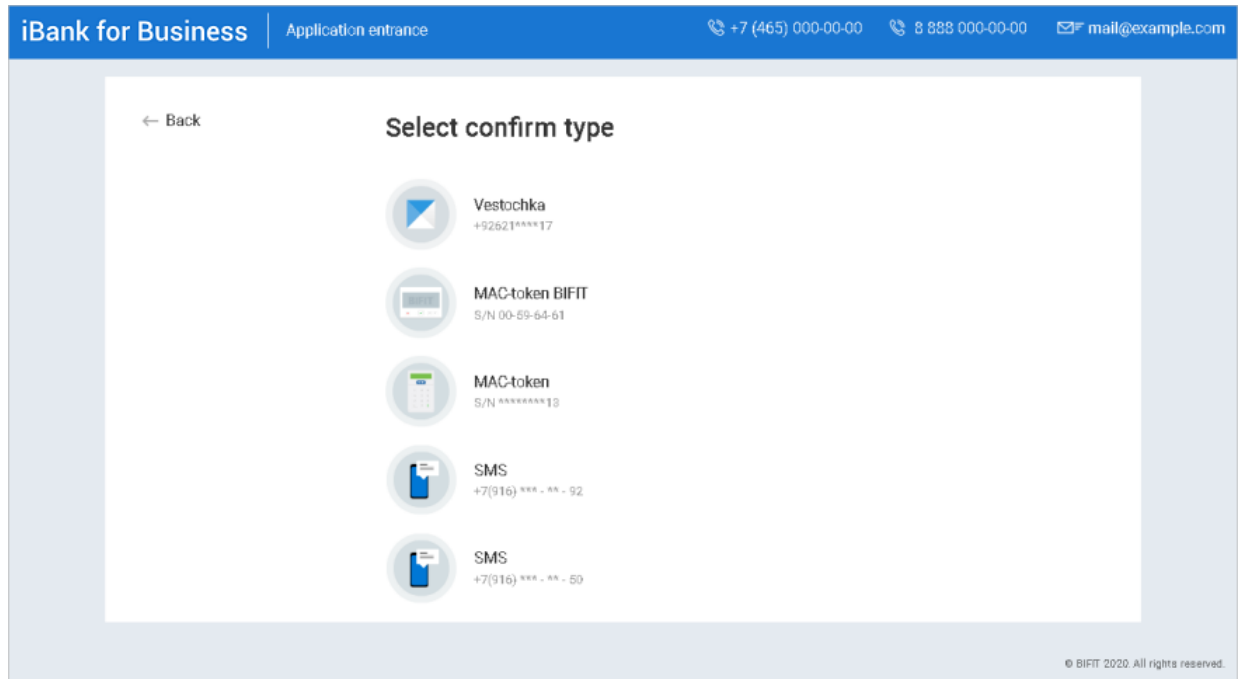

Figure 53. System logging. Multifactor authentication

One time password authentication

1. Choose one of available to you methods to get one time password. Dialog for entering one time password appears (see Figure 54).
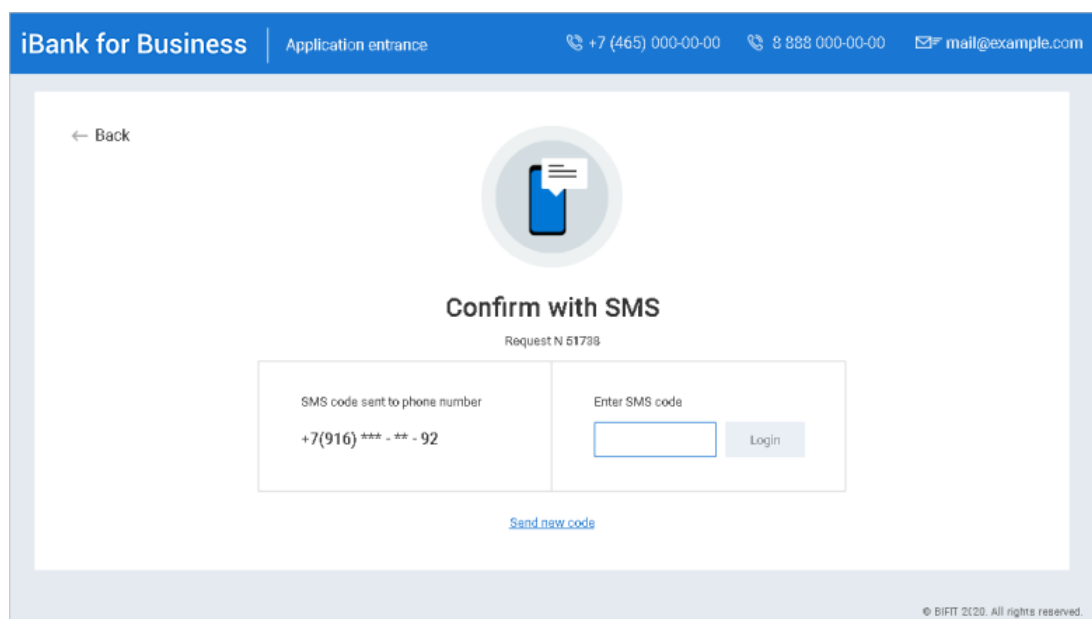

Figure 54. Confirmation by SMS-code

2. Get one time password by chosen method.

> **MAC-token**

a.
Turn on MAC-token by pressing ⏻ on its keyboard. On the display appears the message **"ВВЕДИТЕ ПИН"**. Enter PIN code. After entering the correct PIN code on the display will appear the message **"ВЫБРАТЬ"**. Press key **"1"** on the device keyboard.

b. On the display appears one time password.

> **SMS** To get one time password click **Receive password on SMS**. On the mobile phone number registered in the bank will be sent message with confirmation code. Check that details in SMS message match with details of the document being confirmed. To re-receive one time password click link Send new code.

> On the bank side, sending a notification about the SMS code request can be configured. The notification is sent to the phone number of the employee whose ES key was logged in the service.

> **OTP-token** Press the button on the OTP-token. On the display appears numeric sequence (one time password).

3. Enter generated password to the field **One-time password** in the authentication dialog.

4. Click **Login**.

Authentication with Vestochka

1. Choose Vestochka (see Figure 53).

> *Note:*
>
> For using "Vestochka" Application as confirmation type it must be registered by the using phone number. If it is not registred warning message appears (see Figure 55). To continue confirmation install the "Vestochka" App and click the link "Vestochka" application is installed. If it is necessary use the manual instruction at the link Learn more.
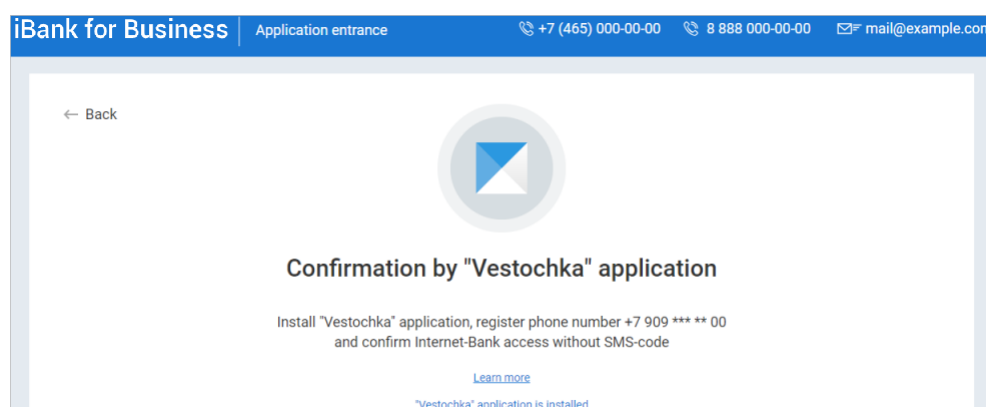

Figure 55. Confirmation by "Vestochka" App. Application is not installed

2. On the screen of smartphone in mobile application "Vestochka" will appear the message is as follows:

```
Подтвердите вход в iBank:
Запрос No 1056
Организация АО -"Крокус"
IP-адрес 192.168.5.175
```

Carefully check that the details on the smartphone screen are correct.

3. Click the button **Confirm** to confirm the entrance or **Cancel** to cancel.

   If confirmation period is expired, press the button **Send a new request** or choose another confirmation type by pressing matching button (see Figure 56).
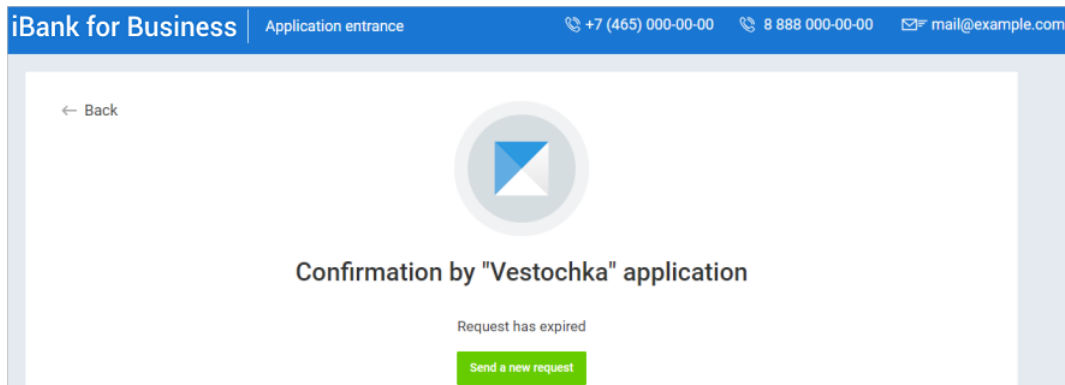
Figure 56. Confirmation by "Vestochka" App. Request has expired

Authentication with MAC-token BIFIT

1. Connect the device with the computer.

2. Enter device PIN-code.

3. On the screen of the MAC-token BIFIT will appear the message as follows:

   ```
   Login to -"iBank 2"
   ОАО -"ОТП Банк"
   IP-address 192.168.4.178
   ОАО -"Крокус"
   ```

4. To confirm the operation press the button ✔ on the MAC-token BIFIT, to cancel — ✖

The same MAC-token BIFIT, MAC-token, OTP-token, or cell phone number can be used by several corporate clients. It allows employee who works in several organizations use only one device.

Appendix 1

Using CIPF "Crypto-COM 3.4"

In data protection purposes the system "iBank" has a build-in support of multiplatform certified by Federal Security Service of Russia encryption library. CIPF "Crypto-COM 3.4" of "Signal-COM" company (Code certificates Federal Security Service of Russia № СФ/114-3975 from January 11, 2021, № СФ/124-3976 from January 11, 2021).

Encryption library is intended to provide protection of confidential data which is not supposed to be official secret from confidential and integrity breach threats by means of encryption procedures, build-in application programs.

Encryption library installation on the client-side

Encryption library "Crypto-COM 3.4" is installed by placing its files in the operation system environment. To install the cryptographic information protection system, it is necessary to place the crypto library files in the appropriate directory:

For Windows x86_64:

64-bit	`ccom.dll`, `ccom.dll.sig`	into directory	`C:\Windows\System32`
32-bit	`ccom.dll`, `ccom.dll.sig`	into directory	`C:\Windows\SysWow64`

For Windows x86:

32-bit	`ccom.dll`, `ccom.dll.sig`	into directory	`C:\Windows\System32`

For Linux x86_64:

64-bit	`libccom.so`, `libccom.so.sig`	into directory	`/usr/lib/`

For Linux x86:

32-bit	`libccom.so`, `libccom.so.sig`	into directory	`/usr/lib/`

Contact your bank to get encryption library files.

CIPF user guide

Working with cryptographic information protection facilities (CIPF) follow the rules listed below:

- Encryption library is not included to the installation package of "iBank" client part. CD with encryption library is got against receipt in register in bank security service.

- Workplaces on which CIPF is installed must be checked for absence of backdoors (trojans, keyloggers and etc.) and instrument bugskeyboard hardware keyloggers and etc.).

- Only original licensed software must be used on technical items, intended for using with CIPF.

- CIPF is installed from CD got against receipt in register in the bank security service.

- On the computer with CIPF should not be installed software development and debug tools.

- System unit and slots of the computer with CIPF should be sealed by security service employee. Check seals integrity every time the computer switched on.

- In case of detecting any unregistered programs, software integrity breach or breach of seals on system unit all activity on this workplace must be stopped.

CIPF user is not allowed:

- to launch programs which are not allowed by security administrator;

- to proceed with provided CIPF information which is supposed to be official secret;

- to connect to the computer additional devices, which are not provided of the box;

- to perform unauthorized computer system unit opening;

- to fetch and use in the room, where CIPF is installed, cordless phones and radio transmitting equipment (the requirement is a recommendation);

- to perform unauthorized CIPF copying.