

INSTRUCTION ON THE PROCEDURE FOR THE PARTIES' INTERACTION IN ELECTRONIC DOCUMENT EXCHANGE

1. Electronic Document Exchange

1.1. For System operation the System User shall use hardware and software that meet the requirements specified in the List of Hardware and Software Required for "Client" Subsystem Performance (hereinafter referred to as the List).

1.2. During the performance, the User will carry out the following actions:

- Registration in the System - generation of a special ED "registration", signed by using the Client's electronic signature (hereinafter referred to as CES). The System operation is allowed only after successful verification of the CES by the System server.
- Working with ED sent by the Client provides for generation of new ED based on the ED existing in the System and specified in the Application. For each type of ED there is an appropriate screen form in the System. For "Payment order" documents, it is possible to import to the System of the Files with a format determined by the Bank. The import file structure description is in the Bank server.
- One or several CES for each ED. Number of CESs for each type of ED is specified in the Application. Having been signed using CES in accordance with the Application, the ED is sent automatically to the Bank for execution.
- Review, stamping, saving in a file format of EDs received from the Bank.
- Logoff.

1.3. The procedure for ED processing by the System server is the following:

- After ED has been generated, the System Users put the CES in the number specified in the Application and send the ED to the Bank.
- The Bank Server receives the ED and verifies all CES they contain.
- The Bank accepts the ED sent by the Client through the System on the basis of the right number and correctness of all CESs, as specified in the Application. In case of a positive result of the checking procedure, the Bank server makes a stamp in the document on the time the ED was received and puts the Bank ES (hereinafter referred to as BES), confirming that the Bank has received the ED, and stores the ED in the System. In case of a negative result, the CES and the BES is not put on the document and the system sends the Client a message that an error has occurred. The Bank's Electronic Signature Verification Keys and copies of corresponding certificates are placed on the system server <https://www.bankline.ru>. The Bank Electronic Signature Verification Key certificate is signed only by the Bank's authorized representative. The Bank's Key Set is valid for 5 years.

1.4. The procedures described in p.1.3 of this Instruction are an integral and indivisible process of ED receiving by the Bank. They can't be performed in a different sequence nor considered independently from each other.

1.5. A document is considered as transferred to the Bank by the Client if it is saved in the Client's outgoing documents archive on the Bank's server. The Client may save any outgoing document in a file for keeping his own archive. The file shall have the CES, stamp with the time of the document was received by the Bank and the BES. Files from the Bank's server and from the Client's archive can be used in dispute resolution procedures between the Parties.

1.6. At any time the document transferred by the Client to the Bank has a certain status on the Bank's server, with a stamp on the time of its receipt. The status of the ED is changed by the Bank. Information on the status change (including the time of the change) of the ED transmitted to the Bank is continuously available for the Client on the Bank's server. The Bank's server assigns the following statuses to the EDs received from the Client:

- Payment orders in rubles:
 - "received by the Bank";

- "document is sent for execution";
- "in the queue at the teller"/ "document processing is finished successfully...";
- "processed without errors" or "processed with errors" indicating the reason of the document rejection;
- "included to be sent to the cash settlement center";
- Other types of documents:
 - "received by the Bank";
 - "document is sent for execution";
 - "in the queue at the teller"/ "document processing is finished successfully...";
 - "processed without errors" or "processed with errors" indicating the reason of the document rejection.

The Parties agree that the assignment to the document of the status "the document has been sent for execution" by the Bank is considered as the Bank's message to the Client confirming that the document is accepted for execution, and in case of the System Depository module it is a receipt of the document type "Status of order/request processing" stating that the Client's ED processing status is "Accepted for execution".

The Bank informs the Client on execution of each ED by sending a message to the Client through the System.

Note: The list and description of ED statuses assigned by the Bank server in the System Depository module are listed in the System Depository module user's manual.

1.7. When generating ED for the Client the Bank stamps the BES on it. The document is considered as transferred to the Client by the Bank if it is signed using BES and placed on the Bank's server, i.e. it is in the Client's ingoing documents list on the Bank server. The Client can save any outgoing document to a file to keep his own archive. Files from the archive can be used in dispute resolution procedures.

1.8. The Bank records electronic archives of ED with CES and BES received from the Client and ED with BES delivered to the Client and stores them in a manner that provides the Client with access to ED on the Bank's server.

1.9. The Client can check BES and CES of any archive file at any time using the ES verification program CryptoManager.exe installed in his personal computer. The above mentioned ED verification program makes it possible to verify ED types (section 3 of this Instruction) allowed for use in the System.

1.10. The ES verification program CryptoManager.exe can be obtain from the System designer - CJSC "INIST" (Russian Federal Security Service License No 12818H dd 16.04.2013) registered at the following address: Building 3, 40-42, Kosmodamianskaya naberezhnaya, Moscow, 115035.

2. Procedure for keys obtaining, replacement and storage

2.1 For electronic Key Sets generated for use on a personal computer:

2.1.1. A Corporate Segment Client may generate the Sets of Keys of his/her System Users pursuant to an Application with the help of the software provided by the Bank on USB-tokens with use of its own technical facilities.

2.1.2. A Business Segment Client may generate the Sets of Keys of his/her System Users pursuant to an Application with the help of the software provided by the Bank on USB-tokens or other information media (hard discs, removable media (optical discs, flash memory, external hard drive, etc.)) with use of its own technical facilities.

2.1.3. Each System User's Electronic Signature Verification Key is registered by the Bank based on the Key Certificate signed by the Parties.

2.1.4. The Key Set validity is stated in the Key Certificate. The period of validity of the Key Set may not exceed the term of validity of the System User's authority in accordance with the documents confirming his authority. In the event that, based on the documents submitted by the Client, it is not possible to establish the term of validity of the System User's authority, the period of validity of the Key Set may not exceed three years. The Client shall initiate the Key Set replacement procedure prior to the expiration of the established period. Upon the Client's application sent to the Bank through the System before the Key Set expires, the Key Set validity can be extended for a period not exceeding 3 months. At the discretion of the Client, the Key Set can be replaced at any time during its validity period. Each new Key Certificate signed by the Parties revokes automatically the validity of the System User's Key Certificate issued earlier.

2.1.5. The Key Certificates issued for the Client by the Bank are delivered by hand to the Client's representative, Client's courier or sent to the Client by mail. Key Certificates shall be kept by each Party for no less than five years after they have expired.

2.2. For the Key Set generated on the Mobile application:

2.2.1 The user has the right to generate the Key Set for the Mobile application by using the software provided by the Bank, in case there is an active Key Set that has been generated for use on a personal computer.

2.2.2 The Key Set validity is stated in the Key Certificate. The validity of the Key Set generated by the Mobile application can not exceed the expiration date of the User Key Set generated for use on a personal computer. The Client shall initiate the Key Set replacement procedure prior to the expiration of the established period. Each new Key Certificate signed by the Parties revokes automatically the validity of the System User's Key Certificate issued earlier.

2.2.3 The status of the System ED User generated through the Key Set for the Mobile application, corresponds to the status of the System ED User indicated in the Application when generating Key Sets on USB-tokens.

2.3. It is obligatory to replace Key Sets in the following cases:

- the Key Set has expired;
- the Key has been compromised.

2.4. In case the Client withdraws the System User's right to sign ED using ES, the corresponding Key Sets are canceled upon the receipt of the Client's written application or a free form ED sent through the System.

3. Document exchange safety and ED exchange safety

3.1. ED exchange safety is ensured by using the following tools:

3.1.1. For the personal computer:

- Cryptographic information protection facilities based on the software package *Bicrypt 5.0*. (software version 2) developed by *InforCrypt* (Certificate of Conformity issued by the Federal Security Service of the Russian Federation No.SF/114-3021 on December 30, 2016). A Business Segment Client shall be entitled to use for storage of ES Keys other media instead of USB-tokens (hard discs, removable media, (optical discs, flash memory external hard drives, etc.). The Bank shall notify the Client that use of other information media instead of USB-tokens significantly reduces the level of security upon exchange of electronic documents, and the Client shall be fully aware of the arising risks. The Bank recommends not to make use of any information media except for USB-tokens;
- Data cryptographic protection facilities *Cryptotoken* and *Cryptoken 2* that comprise USB tokens *JaCarta GOST* (eToken GOST) developed by *JSC Alladin R.D.* (Certificates of Conformity No.SF/111-2750 issued by the Federal Security Service of the Russian Federation on December 1, 2015, and No.SF/124-2963 issued on September 9, 2016. The digital signature key shall always be kept in the internal protected USB token memory. ES Key shall be generated and stored and documents shall be signed in the internal memory of a USB-token. Access to an ES Key shall only be provided with use of a password;
- Data encryption in telecommunication channels, using the data cryptographic protection facilities *CryptoPro CSP* Version 4.0 and higher. To protect the data from unauthorized access, Transport Layer Security (TLS v. 1.0, RFC 2246 and higher) protocol shall be used in telecommunications channels;
- Certificate of Appurtenance of the server of PJSC ROSBANK's System with use of the certificate issued to PJSC ROSBANK by the accredited Certification Authority *CRYPTO-PRO* LLC.

3.1.2. For the Mobile application:

- In order to protect data from unauthorized access in telecommunication channels, the following means of cryptographic protection of information with the use of RSA protocol are used: Transport Layer Security Protocol (TLS v. 1.2, RFC 2246), RSA (3072 bit) international cryptograph algorithms, Diffie-Hellman key exchange, hashing algorithm according to SHA512.
- Symmetric encryption of AES with a key length of 256 bit., generation and storage of Electronic Signature Key, as well as ED signing is performed on the internal secure memory of the Mobile device. The Client has been informed by the Bank that the use of other data storage devices instead of USB-tokens will significantly reduce the security level when exchanging electronic documents and is fully aware of the risks involved. The Bank does not recommend to use any data storage devices designed for generating and storing ES keys, except for USB-tokens.

3.2. The Client is recommended to take the following organizational and technical measures aimed at fulfilling the following safety requirements:

3.2.1. For working on a personal computer:

- To arrange a separate *Client Subsystem* computer intended only for operations with the Bank;
 - The Key Information shall be generated and stored and the documents shall be signed with use of USB-tokens *JaCarta GOST/JaCarta-2 GOST*;
 - If ES Keys are generated by a Business Segment Client for his/her users on the media different from USB-tokens, workstations shall be operated and their security ensured by organizational and technical measures in accordance with the requirements specified in the operating documentation for CIPF *Bicrypt 5.0* for class KS1: *Cryptographic Information Protection Facility Bicrypt 5.0. Directions for Use* (INFK.11485466.4012.027.31). The Document is posted at the official web-site of the Bank at <http://www.rosbank.ru>.
 - A restriction shall be introduced with regard to network interconnection of the Client Subsystem computer with the necessary trusted list of IP-addresses;
 - A protected TLS-connection shall be checked with the official resource of the server <https://www.bankline.ru>. The *Client Subsystem* computer network communication shall be restricted to the necessary trusted IP-addresses;
 - In order to ensure the Bank's control, the *Client Subsystem* computers IP address/IP-addresses shall be assigned to the System Users through the *Client Subsystem*;
 - To ensure use on the assigned computer of facilities for protection from malware, their operability and regular updating;
 - To preclude on the assigned computer opening of letters with attachments received from unknown or unreliable sources;
 - Licensed software and operating systems shall only be used;
 - The software and operating system security package shall be updated on a regular basis;
 - Use of remote administration tools shall be excluded;
 - Provisions shall be made for using a licensed firewall (it shall be allowed to use a personal firewall);
 - To take organizational measures to ensure information security (setting of operation system security parameters, restricting of rights of access to the information system, ensuring password protection, preparing incident response procedures, etc.);
 - To monitor compliance with security requirements.
- 3.2.2. For working on a mobile application:
- Only licensed software and operating systems shall be used;
 - The software and operating system security package shall be updated on a regular basis;
 - The use of remote administration tools shall be excluded;
 - Take organizational measures to ensure information security (setting operation system security parameters, restricting information system access rights, ensuring password protection);
 - Monitor compliance with security requirements.
- 3.3. The Client shall:
- By using licensed software products for protection against malicious codes and updating them on a regular basis, protect the *Client Subsystem* computer or the Mobile application from viruses and other malware which may destroy or modify the subsystem software or compromise the keys of the System User;
 - Exclude the possibility of making changes in the Client's hardware and software identified in the List that have not been authorized by the Bank;
 - Exclude the possibility of compromising the keys during their transportation, using and storage.
- 3.4. The Parties shall:
- protect the confidentiality of Electronic signature keys, in particular, not allow that their own Electronic signature keys be used without their consent;
 - inform the other Party about the breach of the Electronic signature keys confidentiality (Key compromise) within no more than one business day from the date information on such breach is received;
 - not to use the Electronic signature key in case there are reasons to believe that confidentiality of this key has been breached.
- 3.5. The Bank has the right to unilaterally block the System User Key in case of reasonable

suspicious of viruses and other destructive software programs in the System User's computer and/or the System User's Mobile device. The Bank will unblock the System User electronic signature Key after it has received the Client's confirmation that all viruses or other destructive software have been removed from his personal computer and/or System User Mobile application.

3.6. In case Confidentiality of the keys has been endangered, the following sequence of actions is established for the Parties.

In case any System User Key has been compromised, the System User shall:

- In case of access to the Key Set (suspected unauthorized copying), send the ED "Key lock" to the Bank immediately. In this case the System will automatically lock the possibility for using the System User Key Set;
- In case of inaccessibility (loss, theft and so on) of the Key Set, inform the System Administrator about this fact by telephone (the System Administrator's telephone number and e-mail address can be found at www.bankline.ru), as well as in the Application, by using the passphrase stated in the key Certificate for authorization;
- In case the System User has lost the passphrase, the System Administrator may take additional measures for the System User authorization (callback at the telephone number indicated in the Application, request for additional information: the Client's account manager in the Bank/ Bank's authorized employee last name, number of users, and so on). In case the provided information is not correct, the Administrator shall inform the Client's account manager in the Bank/Bank's authorized employee about this and upon agreement with him decide weather to continue or to block the Client's work in the System;
- Within the period of no more than three business days from the date of the telephone communication on the Key compromise, send a written explanation of the incident on the Client's form, duly certified by the signatures of the Client's authorized persons and the Client's seal (if available) to the Bank. The letter shall instruct the Bank to discontinue ED processing until the causes of the incident have been eliminated or the Key Set is replaced;
- In case the decision is made to replace the Key Set generated for the Personal computer, the Client shall generate a new Key Set himself and send his representative to the Bank to register it. In case the decision is made to replace the Key Set generated by means of the Mobile application, the Client shall generate a new Key Set himself in accordance with the Instruction.

In case the Bank Key has been compromised, the Bank shall:

- Inform the Client about the Bank's Key Set compromise, continuation/discontinuation of the System operation and on the Bank's Key Set replacement through the System indicating the date and exact time of the mentioned Key Set replacement;
- Shall replace the Key Set out-of-schedule, publish a new Electronic Signature Verification Key and the Bank's Key Certificate copy with a new Electronic Signature Verification Key of the Bank to the System server.

3.7. Upon receipt of a message on the threat to the Key confidentiality by telephone from the Client authorized by the passphrase, the Bank shall immediately suspend the use of the System by this Client. Since this moment, all operations shall be performed based on documents issued in written form.

- Further use of the System by the Client is only possible after the threat to the Client's key's confidentiality has been removed.
-

4. Procedure for ED and ES verification in case of disputes

4.1. In order to resolve disputes regarding the ED authenticity, at the request of the Party concerned that believes that its rights have been breached, the Parties shall appoint a Conciliatory committee within two weeks from the application of the interested Party; all activities related to the preparation and resolution of the dispute shall be carried out in the presence of this Conciliatory committee. The Conciliatory committee will consist of two Bank's representatives and two Clients' representatives, as well as of independent experts, if applicable (as agreed by the Parties). The Bank's representatives and the Client's representatives can be appointed from among employees of these organizations, as well as other competent persons authorized by a corresponding power of attorney.

4.2. An ED is considered to be disputable if one Party makes a claim for its authenticity to the other Party.

4.3. The ED verification procedure shall be carried out in the Bank's premises and using the Bank's equipment.

4.4. In the presence of the Conciliatory committee, the Bank shall install the operating system Windows 7 or higher and the ES verification software program specified in p.1.10 of this Instruction provided by the software developer "INIST" JSC, on a computer free from software

4.4.1. The Party arguing for the disputable ED authenticity shall provide the disputable ED, Key Certificates valid at the moment the disputable ED was generated by the Party that signed the disputable ED; the Bank shall provide the Electronic Signature Verification Keys recorded in a removable information device in the form of a file in the format supported by the System (in case the Client does not provide the disputable ED, it shall be provided by the Bank).

4.4.2. The parties shall provide all available Key Certificates, information on planned and unplanned replacement of the Parties' Key Sets and documents confirming the Key Sets replacement. The Parties shall also provide official System EDs where the fact of receiving EDs through communications channels and the results of their processing (verification) are indicated.

4.5. The Conciliatory committee members shall perform the following actions:

4.5.1. Carry out the ED verification using the ED verification software program indicated in p.1.10 of this Instruction and each Electronic Signature Verification Key used to sign the disputable ED;

4.5.2. Create the ED Authentication Protocol - a paper document created by the System as a result of the verification of the ES of the disputable ED (hereinafter referred to as the Protocol). The protocol shall contain the Electronic Signature Verification Keys printed on paper, used for the ED authentication, and a conclusion on the results of verification of the ES of the disputable ED. The protocol shall be signed in person by all members of the Conciliatory committee;

4.5.3. Compare the Electronic Signature Verification Keys contained in the Key Certificates with the corresponding Electronic Signature Verification Keys registered in the disputable ED Authentication Protocol and evaluate whether they are identical; make records about it in the Protocol (this record shall be signed by the members of the Conciliatory committee);

4.5.4. Determine if the Electronic signature keys were valid by the time the disputable ED was generated and make records about it in the Protocol (this record shall be signed by the members of the Conciliatory committee). The Electronic Signature Verification Key is considered valid by the moment the disputable ED was generated if the disputable ED generation date falls within the validity period of the Electronic Signature Verification Key. Otherwise, the Electronic Signature Verification Key will be considered as invalid by the moment of the ED generation.

4.6. The Conciliatory committee shall recognize the Electronic document as genuine provided that the following conditions are simultaneously met:

- The Electronic Signature Verification Keys contained in the Key Certificates and in the Protocol are identical,
- All results of the ED verification stated in the Protocol are positive,
- The Conciliatory committee has recognized all Electronic Signature Verification Keys stated in the Protocol as valid by the moment the ED was generated.
- Otherwise, the Conciliatory committee shall recognize the ED as invalid.