Electronic Document Workflow Rules

for the information and technology service when performing funds transfer

Kazan

Revision No. 1 of 25 June 2020

Limited Liability Company "Bank 131" (the "Bank"), on the one hand, and a legal entity that has entered into an agreement with the Bank on information and technology service when performing funds transfers (the "Company"), on the other hand, jointly referred to as the "Parties", have entered into this Agreement as follows:

1. Subject of Agreement

1.1 This Agreement establishes the rules for the organization electronic document workflow using an electronic signature between the Parties within the framework of an information and technology service agreement when performing funds transfers.

1.2. The list and forms of electronic documents, which the Parties may sign and transfer to each other under this Agreement, are determined by the Bank and are available at: https://developer.131.ru.

1.3. The Company shall exercise its right to exchange electronic documents signed by electronic signature only through its duly authorized representatives. Such representatives may be both able-bodied individuals vested with the Company's constituent documents with the right to act alone on behalf of the Company without a power of attorney, and able-bodied individuals acting on behalf of the Company by proxy.

2. Concluding the Agreement

2.1. This Agreement consists of the electronic document workflow rules itself and an application for the recognition and verification of an electronic signature key (hereinafter referred to as "Application", Annex 1). The current version of the Agreement is available at https://developer.131.ru.

2.2. The Agreement is not a public offer. The Bank has the right to refuse to conclude the Agreement with the Company in case the Company has no agreement with the Bank on information and technology service when performing funds transfers.

2.3. The Agreement is concluded by the Parties accepting the terms and conditions of the Electronic Document Workflow Rules and signing the Application in two copies. The Agreement shall be deemed concluded from the date of signing the Application.

3. Information and technology interaction

3.1 Parties shall carry out information and technology interaction in accordance with the Protocol on Information Exchange (hereinafter referred to as "API") and the Information Security Instruction (Annex No. 2), the current editions and descriptions of which are available at https://developer.131.ru/.

3.2. The Bank may unilaterally amend the API. If the amendments may affect the Parties' performance of their obligations under the Agreement, the Bank shall send a notice to the Company at least 5 (five) working days before the date when such amendments come into force.

3.3. The Parties shall independently and at their own expense maintain their own hardware and technical infrastructure necessary for implementation of the Agreement, take possible measures to protect information transmitted under the Agreement from unauthorized access, copying and distribution, including those provided for by applicable law.

3.4. The Company agrees that the Bank can not guarantee to the Company the absence of interruptions due to technical malfunctions, preventive maintenance, as well as full and error-free operation of API and communication channels. The Parties undertake to inform (by e-mail and/or phone) each other in a timely manner about all cases of technical failures or other circumstances that prevent the proper performance of this Agreement.

4. Electronic signature

4.1. The Agreement provides for the use of an enhanced, unqualified electronic signature (hereinafter referred to as the "Signature"), which enables confirmation of authorship, authenticity and integrity of signed electronic documents.

5. Electronic Signature

5.1. Electronic signature shall be used for the creation and verification of the Signature, the creation of the Signature key and the signature verification key:

5.1.1. make it possible to determine whether the signed electronic document has been altered after its signature;

5.1.2. make it practically impossible to calculate the key to the Signature from the electronic signature or from the key to verification of the Signature.

5.2. The Company shall independently and at its own expense select the electronic signature means and create a key to the Signature and a key to verify the Signature.

6. The rules of electronic document workflow

6.1. Prior to the beginning of interaction on electronic document workflow, the Bank and the Company shall exchange the keys for verification of the Signature. The Bank's Signature verification key may be published in the public domain at https://developer.131.ru.

6.2 Electronic document workflow includes the following stages: creation, transfer, authentication, accounting and storage of electronic documents.

6.3. Creation of an electronic document includes direct formation of the electronic document and its signing by the Signature using the Signature key.

6.4. The transfer of a signed electronic document is carried out exclusively using the API.

6.5. Authentication of the electronic document includes verification of the electronic document's compliance with the requirements to its format and completion, as well as verification of the authenticity of the Signature using the Signature verification key.

For verification of the Signature, the Parties shall use the electronic signature tool:

1. generates a hash from the original electronic document according to the algorithm defined in the Application;

2. transforms the received Signature using the key of verification of the Signature;

3. compares the value obtained at step 1 with the value obtained at step 2.

If the values match, the Signature shall be considered authenticated. If it does not match, the Signature shall be deemed not to have been authenticated, and the verifying Party shall immediately inform the other Party thereof.

6.6 Electronic documents are recorded by electronic registers of incoming and outgoing electronic documents signed with the Signature. The electronic registers shall be maintained by the Bank's hardware and software tools. The moment of receipt of an electronic document is the moment it is reflected in the register.

6.7. Electronic documents received by or outgoing from the Bank shall be stored in the Bank's archive for the period of time established for documents of the respective type, but not less than five years after receipt of the electronic document. In case of any disputes regarding the content of electronic documents, electronic documents kept in the Bank's archive shall take precedence.

7. Recognition of electronic documents

7.1 The Parties acknowledge that electronic documents signed with the Signature are equivalent in legal force to paper documents signed by hand and sealed (if any).

7.2 Legal effects provided for an electronic document will only occur if a positive result of verification of the Signature of this electronic document is obtained, provided that the requirements to the format and procedure of filling in of the electronic document established by this Agreement and the legislation of the Russian Federation are met.

8. Liability of Parties

8.1 The Parties assume all risks related to the performance of their equipment and communication channels, safety and confidentiality of Signature keys.

8.2 In the event of non-fulfillment or improper fulfillment of its obligations by one of the Parties, the other Party shall have the right to demand that such Party fulfill its obligations and compensate for the damage caused to it.

8.3. The Company shall be responsible for the confidentiality of the Signature key, as well as for the actions of its employees when using the Signature. The Bank shall not be liable for losses incurred by the Company in connection with unauthorized use of the Signature by unauthorized persons.

9. Privacy .

9.1. The Parties undertake to ensure confidentiality of the keys of the Signature, in particular, to prevent the use of the keys of the Signature belonging to them without the consent of the Parties. Not to use the key to the Signature if there are grounds to believe that the confidentiality of this key to the Signature has been violated.

9.2. The party which has allowed the compromised key of the Signature shall be liable for the electronic documents signed using the compromised key of the Signature. A Party's signature key shall be deemed valid until the date on which the other Party receives notification of the cancellation (revocation) of the relevant Signature key.

9.3. The Parties shall undertake to inform each other within no more than one calendar day of any violation of confidentiality of keys to the Signature (including loss, theft, unauthorized access to a key of the Signature). In this case, the Agreement shall be suspended until the signature keys are changed. The change of keys to the Signature shall be carried out by signing a new Statement by the Parties.

10. Force Majeure .

10.1 The Parties shall be exempt from liability for partial or full non-fulfillment of their obligations under the Agreement in the event of force majeure, such as: natural and man-made disasters, military operations, civil unrest, epidemics, pandemics, the collapse of the world economic and financial system, the adoption of regulations of a restrictive nature. Force majeure also includes: failure or failure of hardware and software, failure or disconnection of communication systems, power supply, interference of third parties (DDoS-attack), etc.

10.2 In the event of force majeure, the Party affected by such circumstances shall, within 3 (three) calendar days, notify the other Party thereof. The Party that missed the notice period shall be deprived of the right to refer to the said circumstances as a ground exempting from liability.

11. Dispute resolution

11.1 This Agreement shall be governed by and construed in accordance with the laws of the Russian Federation (applicable law).

11.2 In the event of any disagreement on the issues of the implementation of the Agreement, the Parties shall take all measures to resolve them through negotiations.

11.3 Any disputes between the Parties, the subject of which is a dispute over the content of an electronic document, shall be referred for resolution to a specially established expert commission. The composition of the expert commission shall be formed in equal proportions from representatives of the Parties. The Commission shall establish the authorship, authenticity and integrity of the Signature of the challenged electronic document. Results of work of the expert commission shall be executed by the act, which shall be signed by the Parties. From the moment of signing the act the Parties recognize the indisputability of the information specified in this act. The procedure for dealing with conflict is specified in Annex No. 3.

11.4. In case of impossibility to settle differences through negotiations, the disputes shall be settled in the Arbitration Court of the Republic of Tatarstan with the application of the substantive and procedural law of the Russian Federation.

11.5. A written pre-trial claim procedure for settling disputes is mandatory. The term of reply to the claim is 15 (fifteen) calendar days from the moment of its receipt.

12. Notifications .

12.1. Unless otherwise provided in the Agreement and in the Agreement on Information and technology services for transferring funds transfer, any letters, notifications and documents transmitted by the Parties to each other under the Agreement by e-mail shall be deemed duly sent and received if sent from/to the e-mail addresses specified by the Parties in the Application.

12.2. A change in the e-mail address of the Parties (para. 12.1) shall be made by sending an e-mail message from the previously specified e-mail addresses containing a clear indication of the new e-mail address for communication.

13. Amendment of the Agreement

13.1. The Bank may unilaterally and extrajudicially make any amendments and/or additions to the Agreement by posting a new version of the Agreement at https://developer.131.ru.

13.2 The new version of the Agreement comes into force and is subject to application to legal relations of the Parties after 10 (ten) calendar days from the date of its placement at https://developer.131.ru.

13.3 The Company shall independently and timely familiarize itself with the new version of the Agreement. In case the Bank has not received a written notice to the Company on termination of the Agreement prior to the entry into force of the new version of the Agreement, the new version of the Agreement shall be deemed to be unconditionally accepted by the Company, and conclusion of an additional agreement to the Agreement is not required.

14. Term of validity and termination

14.1 The term of validity of the Agreement is limited by the term of validity of the agreement concluded between the Parties on information and technology service for performing funds transfers.

14.2. The Bank may unilaterally withdraw from the Agreement by giving at least 30 (thirty) calendar days' written notice to the Company.

14.3. The obligations of the Parties arising before the termination of the Agreement shall be retained until their full execution.

15. Other conditions

15.1 This Agreement has been drawn up in the Russian and English languages. In the event of any discrepancies, the Russian language version shall prevail.

15.2 All annexes are integral parts of the Agreement, namely:

15.2.1. Annex No. 1 - "Application";

15.2.2. Annex No. 2 - "Instructions on ensuring information security";

15.2.3. Annex No. 3 - "Dealing with conflict".

15.3. The Parties may not transfer their rights and obligations under the Agreement to third parties without prior written consent of the other Party.

15.4 If any provision of this Agreement is found invalid or unenforceable under the applicable law, such provision shall be brought by the Parties in accordance with the applicable law, and the validity and applicability of any other provision of the Agreement shall not be affected.

16. Bank's details

Limited Liability Company "BANK 131"

License of the Bank of Russia №3538 dated 12.04.2019

ORN 1191690025746

INN/KPP 1655415696 / 165501001

Address: 420012, Russian Federation, Republic of Tatarstan, Kazan, 38 Nekrasova Street

Correspondent account: 30101810822029205131

at the Office of the National Bank of the Republic of Tatarstan

BIC: 049205131

Addendum № 2
to the Electronic Document Workflow Rules

Instructions on ensuring information security

To ensure information security when working with the Information Exchange Protocol ("API"), the Company is assigned the following responsibilities:

1. The electronic signature key (hereinafter referred to as "signature key") should only be kept out of reach of unauthorized persons.
2. Not allowed:
   - make unauthorized copies;
   - hand over the Signature key to unauthorized persons.
3. Do not use as a password:
   - character sequences consisting of the same digits (including dates, phone numbers, car numbers, etc.);
   - sequences of repetitive letters or numbers;
   - consecutively in the keyboard layout or alphabetical characters;
   - names and surnames;
   - Taxpayer identification number or other details of the Company.
4. The password shall:
   - must be at least 8 characters long;
   - contain numbers, lowercase and uppercase letters;
   - contain at least 1 character, which is not a letter or a number.
5. The computer must have a password protection for entering the device operating system.
6. The user password in the device operating system must be changed by the Company at least once a quarter.
7. The password for access to the Signature key shall be kept separately from the Signature key.
8. It is strictly prohibited to write down passwords on paper or in text files at the workplace, leave them in easily accessible places, or transfer them to unauthorised persons.
9. Use the Signature key only when signing electronic documents.
10. To use the Signature key, only for signing electronic documents within the framework of "API" usage.
11. Use licensed anti-malware tools at the workplace with the possibility of automatic update of malware signature databases.
12. If a laptop is used as a computer for work under the "API", its connection to public networks in places of free access to the Internet (office centers, cafes, etc.) should be excluded.
13. To constantly monitor the messages sent when working under "API".
14. If any signs of compromise of the Signature key or detection of malicious code in the computer used for operation of "API" are detected, the Bank shall be immediately notified by telephone: (843) 598-31-40, (843) 598-31-39 from 9:00 a.m. to 6:00 p.m. (on business days), or come to the Bank in person in order to block compromised keys of the Signature with their subsequent replacement.
15. The events related to the compromised keys of the Signature shall also apply:
   - loss (loss) of the Signature key carrier, including, but not limited to, its subsequent discovery;
   - discovery of the fact or threat of use (copying) of the Signature key and/or the access password to the Signature keys by unauthorized persons (unauthorized sending of electronic documents);
   - detecting errors in the operation of the "API", including those resulting from attempts to breach information security;
   - dismissal of the responsible employee who had access to the Signature key.
16. Upon detection of unauthorized transactions or loss of the "API", notify the Bank immediately.
17. Use the key combinations "Ctrl + Alt + Del" to identify a user in the operating system.

18. Disable the possibility of remote and terminal connection to the computers used to work in the System, block 3389 (RDP Remote desktop).

19. Enable the security log in the operating system.

20. Use only licensed software - operating systems, anti-malware, office packages, etc.

21. Ensure that system and application software can be updated in a timely manner.

22. Allocate a desktop computer for "API" work only.

23. Provide access to the room where the computer with "API" is located only to authorized persons of the Company.

24. The computer from which the electronic documents are prepared and sent to the Bank should be singled out into a separate network segment with its obligatory exclusion from the Company's common local network.

25. To exclude access to computers used for work under 'API' to unauthorized persons and personnel of the organization not authorized to work under 'API' and/or to service computers.

26. When servicing the computer by IT employees to ensure control over their actions.

27. The Bank does not send e-mails requesting to send the Signature keys and/or password used in the "API" and never asks you for this information. When applying on behalf of the Bank by phone, e-mail, SMS-messages of persons with a request to provide confidential information (passwords, code words, etc.) under no circumstances do not provide this information and inform the Bank about it.

28. The Company is independently and solely responsible for ensuring the confidentiality of passwords, Signature Keys, and other data obtained from the Bank or generated by the Company independently for the purpose of their use in "API", as well as for ensuring confidentiality and non-disclosure of data, documents and information obtained and/or sent using "API".

Dealing with conflict

Any disputes between the Parties, the subject of which is the establishment of the authenticity of the Signature in an electronic document, i.e., the integrity of the text and authenticity of the sender of an electronic document, shall be referred for resolution to a specially created expert commission.

The expert commission shall be convened on the basis of a written application (claim) of any of the Parties. In the specified statement the Party specifies details of the challenged signed electronic document and persons authorized to represent interests of this Party in the expert commission.

Not later than 3 (three) working days from the moment of reception by the other Party of the statement (claim), the Parties define date, a place and time of the beginning of work of the Expert commission, define, what Party gives premises and makes a configuration of means of the electronic signature.

Powers of attorney of the Expert Commission members shall be confirmed by powers of attorney issued in a simple written form.

The composition of the Expert Committee shall be formed in equal proportions from representatives of the Parties.

Expert examination of the contested electronic document shall be performed in the presence of all members of the expert commission.

The expert examination shall be carried out in four stages:

1. The Parties jointly establish, configure and test the electronic signature means.

2. The Parties shall provide their Signature keys and signature verification keys used for creating the signature of the contested electronic document.

The expert commission shall compare the keys provided for the verification of the Signature with the keys specified in the Application. 3. The keys of verification of the Signature and the codes that have coincided shall be deemed authentic.

4. If the third stage has been successfully completed, the expert commission shall verify the authenticity of the Signature in the disputed electronic document.

The results of the expert examination shall be executed in the form of a written conclusion - an act of the expert commission signed by all members of the expert commission. The act shall be drawn up immediately after completion of the last stage of the expert examination. The act shall record the results of all stages of the expert examination, as well as all essential details of the disputed electronic document. The act shall be drawn up in two copies - one for each of the Parties. The act of the expert commission shall be final and not subject to revision.

Authentication of the Signature in the act will mean that the disputed electronic document has legal force and causes the Parties' respective rights and obligations.

In case of absence of consent on disputable issues and voluntary execution of the expert commission's decision, all materials on these issues may be submitted to court for consideration in accordance with the terms of the Agreement.