

Onlinebank HALYK System Service Accession Agreement

This Onlinebank HALYK System Service Accession Agreement (hereinafter the “Agreement”) shall regulate the relationship between the Customer and Halyk Bank JSC, hereinafter collectively referred to as the “Parties”, and individually the “Party”. The terms and conditions hereof are defined in a standard form.

The Customer shall accede to the Agreement by affixing its signature in the Application in the form of Annex 1 hereto, or the approved form of the Application-Questionnaire. In this case, the Application in the form of Annex 1 hereto and the Agreement shall be considered only as a single document. The Customer may accede to the Agreement when registering in Onlinebank HALYK system (hereinafter the “Onlinebank System”) using a one-time password.

Signing by the Customer, representative(s) thereof, of the Application/Application-Questionnaire shall mean that the Customer has read the terms and conditions of the Agreement offered thereto by the Bank, including the annexes to the Agreement, and accepts them only by acceding to the Agreement posted at www.halykbank.kz as a whole. The Agreement shall be deemed to have been concluded and come into force upon acceptance by the Bank of the Application of the Customer signed by thereby/representative(s) thereof.

This Agreement determines the rights, obligations, responsibilities of the Parties and other legal relations between the Bank and the Customer, determines the terms and procedure for provision by the Bank of services when connecting the Customer to Onlinebank System, rendering electronic banking services to the Customer, making transactions on the bank account through Onlinebank System by the Customer, and provision by the Bank of other services through the Onlinebank System, as stipulated hereby.

Clause 1. Subject matter

1.1. The subject of the Agreement is the provision by the Bank of electronic banking and other services stipulated hereby through the Onlinebank System, if the Customer pays for those services on the terms of the Bank.

When the Bank renders the above services to the Customer, the Bank shall provide services to the Customer in accordance with the terms of this Agreement and the terms of the corresponding banking service agreement.

1.2. The Parties acknowledge that electronic documents (hereinafter the “Electronic Documents”) used in transactions in the Onlinebank System and/or via the Mobile Application, signed by electronic digital signature (hereinafter the “EDS”) and/or a Dynamic Authentication Method are equivalent to documents on paper and give rise to similar rights and obligations of the Parties hereunder.

1.3. The Parties acknowledge that each Party may electronically transfer to another Party or receive from the other Party documents, communications (instructions) specified herein.

1.4. The Customer acknowledges that the exchange of Electronic Documents is possible only if the sender has a registration certificate that has been verified at the Certifying Center, and/or the Dynamic Authentication Method.

1.5. The Parties recognize the information protection system used thereby hereunder to protect them from unauthorized access, as well as to confirm the authorship and authenticity of the Electronic Documents sent by the Customer using the EDS and/or the Dynamic Authentication Method, subject to provision by the Customer of all security recommendations.

1.6. The Customer acknowledges being agreed with the Agreement by signing the Application for connection to the Onlinebank System/Application-Questionnaire.

Clause 2. Terms and Abbreviations Used

2.1. The terms and abbreviations used herein with a capital letter shall have the interpretation given to them herein, unless otherwise expressly interpreted in the text.

API key	A registration certificate in the form of an Electronic document issued to the Customer's authorized person without recording it on a Key carrier after the Authorized User signs the API key Creation Application in accordance with Annex 10 hereto, and used to accept and transfer the Customer's Electronic Documents when integrating the Customer's accounting/bookkeeping system or other system with the Onlinebank System.
----------------	--

Cash by code	The Bank's service for issuing cash to the Customer from the current account through an ATM using a generated code.
Halyk Business ID	An identifier provided by the Bank that is used to authenticate and authorize the Customer in the mobile application and/or website of Partners through the Onlinebank HALYK single sign-on service.
Onlinebank Business	The Onlinebank System version, which allows the Customer to remotely manage its bank accounts opened with the Bank by exchanging Electronic Documents, messages (instructions) between the Customer and the Bank via the Internet without the limitation of the Customer in the number and/or amount of Electronic Documents sent to the Bank for execution.
Onlinebank Start	The Onlinebank System version that allows the Customer to remotely manage its bank accounts opened with the Bank by exchanging Electronic Documents, messages (instructions) between the Customer and the Bank via the Internet with the Bank's limitation (limit) on the number and/or amount specified in the Electronic Documents sent to the Bank for execution. The information on the limits is available at www.halykbank.kz
Onlinebank authenticator	A mobile application installed on a mobile device that allows the Customer to generate a unique sequence of electronic digital symbols (hereinafter the "Code") for single use upon entering the Onlinebank System or the Mobile application, and/or authorizing electronic payments, upon request. At each entry of the Customer into Onlinebank System and/or authorization of payments, it is required to create and use a new one-time code.
OnlineDuken Halyk Platform	A platform designed to optimize and simplify the sales process between distributors and the Bank's customers (small/medium grocery stores and cafes/restaurants). This platform is integrated with Onlinebank, where the full sales cycle, electronic payments, lending, as well as the digital marketing and promotion channel are presented
OTP (One Time Password)	A unique sequence of electronic digital symbols sent by the Bank to the Applicant's trusted number and intended for one-time use when providing the Customer with access to Electronic Banking Services – Authentication. The OTP is intended for Authentication of the Customer to establish the authenticity thereof in order to unambiguously confirm the Customer's rights to receive Electronic Banking Services, and is equivalent to Customer's signature.
PIN Code	The secret code, known only to the owner of the certificate (to the authorized person of the Customer, in whose name the Registration Certificate is issued). PIN Code provides the ability to use the Key Carrier in the Onlinebank System only by a person who knows the PIN Code.
SMS Authentication	Service for receiving an SMS message from the Bank that contains the generated unique sequence of electronic digital symbols (hereinafter the "Code") intended for one-time use when logging in the Onlinebank System or the Mobile app and/or authorizing electronic payments. Every time the Customer enters the System and/or authorizes payments, he is required to create and use a new one-time (one-time) code. For SMS authentication payments, the Bank can set a daily limit. The information on limits is posted at www.halykbank.kz
SMS Informing	The service provided by the Bank for informing the Customer about operations on current accounts by sending SMS messages by the Bank to the Customer's Trusted Number and connected by the Customer independently in the Onlinebank System. The fee size for connection to the Service is determined in accordance with the Tariffs of the Bank at www.halykbank.kz .
Automated Cash Register	A device for operations of accepting/withdrawing cash to/from the current account according to the generated barcode in the Onlinebank System.
Bank	Halyk Bank JSC, including branches thereof.
Mobile Device Verification	The procedure for confirming the Customer's mobile device in order to exercise his rights and fulfill his obligations under the Agreement. When verifying the mobile device, a Cloud EDS is issued and subsequently used, which enables the Customer to sign Electronic Documents sent to the Bank for execution within the established daily limit on the amount of transactions. The information on limits is posted at www.halykbank.kz .

Registration Certificate Owner	An individual who is an authorized representative of a legal entity on the basis of an Application for connecting a user to the Onlinebank System, in whose name the Certifying Center issued the certificate, and who lawfully owns the private key corresponding to the public key specified in the certificate with respect whereto the key and/or the Cloud EDS certificate in protected area of the HSM hardware security module are issued.
Statement	A duly executed document (on paper or in electronic form) on the status of the Customer's Account for a certain period. The Onlinebank System provides two types of account statements: preliminary for the current operating day and final for the closed operating day.
Applicable law	Legislation of the Republic of Kazakhstan, consisting of regulatory legal acts adopted in accordance with the established procedure.
Trusted Number	The mobile (cellular) phone number provided by the Customer to the Bank, in ways determined by the Bank independently and used by the Customer to receive electronic banking services using the Customer Dynamic Authentication.
Agreement	Onlinebank HALYK System Service Agreement.
EDS Private Key	The sequence of electronic digital symbols created on a key carrier or in the Cloud Storage registered in the certifying center and known only to the owner of the registration certificate is designated to create an EDS using cryptographic information protection facilities. In case of loss or compromise of the EDS Private Key, the Customer shall promptly submit to the Bank an application for the withdrawal of the EDS Key and the registration certificate to it. The private key is accessed by the owner through at least two authentication factors, one of which being biometric authentication.
Card Reader	Electronic mechanical device that ensures the interaction of the equipment used by the Customer's authorized person (Certificate Owner) with a chip (smart card) in the Key carrier in order to create Electronic Documents using its digital signature on the equipment used by the Customer.
Customer	Legal entity or separate subdivision of a legal entity (branch, representative office), sole proprietor, peasant farm, private notary, private bailiff, lawyer, professional mediator, foreign diplomatic and consular representation, which has entered into this Agreement.
Key carrier	A secure electronic device designed to generate, store private and public EDS keys and perform cryptographic operations using cryptographic information protection facilities.
Callback	A call or notification from the Bank to the Customer about the need to confirm the transaction. To confirm the transaction, the Customer may receive a call 24 hours a day, including weekends and holidays. To confirm the transaction, the Customer shall call the "code word" and details of the transaction, or confirm the transaction in the Mobile application. To confirm a transaction in the Onlinebank for Business Mobile application, the Customer's mobile device shall be verified. Confirmation of the Customer's transactions is available to the user with the right of first or second signature in Onlinebank HALYK System.
International Economic Sanctions (IES)	Coercive measures of a political, diplomatic, or economic nature imposed by an international organization, a foreign government, or an authorized governmental body of a foreign state and providing for a partial or total ban on trade, financial, and other transactions/payments/transfers of individuals or legal entities, the state/territory and/or its residents who are subject to sanctions.
Mobile Application	Application installed on the Customer's Mobile Device for use in Onlinebank System. When operating this application, restrictions and limits on the amount of transactions in Onlinebank System are applied. Information on limits is available on the website at www.halykbank.kz
Mobile Device	A tablet computer, smartphone or phablet with iOS or Android operating systems installed, on which the Mobile Application is installed
Cloud EDS	EDS of an individual (authorized representative of the Customer) generated in the Cloud Data Storage of the Certex Cloud System after registration through the Bank's Certifying Center, and confirming the authenticity of the electronic document signed therewith, its ownership and invariability of the content.
Operating day	The period of time during which the Bank accepts and processes instructions, orders to suspend the execution of instructions, or revoke such instructions.

Operation	Operations, services, and features performed and used by the Customer in the Onlinebank System
EDS Public Key	The sequence of electronic digital symbols that is accessible to any person and intended to confirm the authenticity of the digital signature in an Electronic Document.
Partner	A company with which the Bank has entered into a cooperation (partnership) agreement/contract. As part of the technological cooperation between the Bank and the Partner, the Customer can create an account or log in to the Partner's mobile application and/or web service via Halyk Business ID.
Halyk FX Platform	Additional section of the Onlinebank System that provides the Customer with an individual exchange rate for currency conversion transactions on terms determined by the Bank.
Security Procedure	A set of organizational measures and software and hardware to protect information intended for the Customer identification and authorization when compiling, transmitting and receiving electronic documents, messages (instructions) in order to establish its right to receive electronic banking services, and to ensure confidentiality and detection of errors and/or changes in the content of transmitted and received electronic documents, messages (instructions).
Workstation	Equipment to which the Card Reader, smart card or Java Token is connected and/or the Customer logs on, and is authorized in, the Onlinebank System.
Business Days	Days when banks in the Republic of Kazakhstan and/or country of origin of the relevant foreign currency are open for transactions.
Registration Certificate	An electronic document issued by the Certifying Center to confirm the compliance of the EDS with the requirements established by the Law of the Republic of Kazakhstan "On electronic document and electronic digital signature".
Onlinebank System	The Bank's service system, which provides the Customer with the opportunity to remotely manage its bank accounts opened with the Bank by exchanging Electronic Documents, messages (instructions) between the Customer and the Bank via the Internet.
Internet Banking Support Service	Subdivision of the Bank servicing telephone calls, electronic and written requests and supporting existing and potential Customers of the Onlinebank System by phone.
Dynamic Authentication Method	The method chosen by the Customer for obtaining a one-time code, by which the Customer confirms the entry into the system and/or the dispatch of the Electronic Document to the Bank. The dynamic authentication methods include Onlinebank Authentication, SMS Authentication, and eToken PASS Authentication.
Cryptographic Information Protection Facilities (CIPF)	A set of software and hardware that implement algorithms for cryptographic transformations, generation, formation, distribution or management of keys, and ensure the use of EDS and encryption in information systems. CIPF can be used both in the form of independent software modules and in the form of tools embedded in the application software.
Account	The Customer's bank account with the Bank in any currency opened based on the Bank Account Agreement, Accession Agreement for Opening a Current Account in a Card Base and Servicing a Corporate Payment Card, Bank Deposit Agreement. Here, we also take into account the cases where one or more accounts are opened under a single Bank Account Agreement.
Tariffs	Amounts of the Bank's fees for services rendered to the Customer available at the Bank's website www.halykbank.kz .
Certifying Center	A subdivision of the Bank that issues and maintains an EDS, certifies the compliance between EDS Public Key and EDS Private Key, and confirms the authenticity and activity of the registration certificate.
OnlineDuken Authorized Cashier (OnlineDuken Cashier)	An authorized representative to whom, in accordance with the application in the form of Annex 8 to the Agreement, the Customer grants the right to sign using EDS and the necessary powers to perform transactions, actions, sign documents, including documents for transactions between the Customer and the Bank, using electronic digital signature within the OnlineDuken Halyk platform

Authorized Person/Authorized Representative	An individual – an authorized representative of the Customer, in whose name the Certifying Center issued a Registration Certificate, who legally owns the EDS Private Key corresponding to the EDS Public Key specified in the Registration Certificate.
Competent Authority	National Bank of Kazakhstan or other state competent authority.
Authentication Devices	When using this term, it means all the devices issued to the Customer to confirm the user when connecting to the Onlinebank System, specified by the Customer in the Application for connection of the user to the System
eToken PASS Device	A stand-alone device that allows the Customer to generate a unique sequence of electronic digital characters (hereinafter the “Code”) for single use upon authorizing electronic payments upon request. Each time the Customer enters the Onlinebank System, he is required to create and use a new one-time code.
File Certificate	Registration certificate in the form of an Electronic Document issued to the Customer’s authorized person without recording it on the Key carrier after signing the Agreement for the issuance of a file certificate in the form of Annex 7 to the Agreement and used to transfer the Customer’s Electronic Documents when integrating the Customer’s accounting system with the Onlinebank System.
Financial Number	Mobile (cell) phone number provided by the Customer to the Bank in ways determined by the Bank independently, and recorded in the Bank’s systems and used to transfer money to the Customer’s bank account. One phone number is possible to connect to the service of money transfer by Financial number only to one current account of the Customer or a corporate card (card) of the authorized representative of the Customer (cardholder).
Electronic Digital Signature (EDS)	A set of electronic digital symbols created by means of an electronic digital signature and confirming the authenticity of an Electronic Document, its ownership and the invariability of its content. It is allowed to affix one or more electronic signatures under Electronic Documents that belong to the Customer and have been verified at the Certifying Center.
Electronic Document	A document in which the information is presented in electronic digital form and certified by means of EDS and/or confirmed by the Dynamic Authentication Method.

Clause 3. Onlinebank System Connection

3.1. The Customer for connection to the Onlinebank System shall complete the Application in the form of Annex 1 hereto or Application Form as approved by the Bank (hereinafter the “Application Form”), and provide all duly executed documents in accordance with the requirements of the Bank.

3.2. The Bank informs in proper and accessible ways about the existence of versions of the Onlinebank System, such as “Onlinebank Business” and “Onlinebank Start”.

3.3. By signing the Applications in the forms set forth in Annexes 1, 2 hereto or the Application Form, the Customer confirms that the Bank has informed on the necessary Key Carrier devices and/or Dynamic Authentication method when connecting the versions of the Onlinebank System.

3.4. The Customer cannot be connected simultaneously to two available versions of the Onlinebank System.

3.5. The Customer cannot be connected to the Mobile Application without connecting to the Onlinebank System.

3.6. The Mobile Application can be connected to the Customer only when the Customer indicates a Trusted Number.

3.7. Connection to any version of the Onlinebank System is impossible if the Customer does not indicate the Trusted Number.

3.8. The Trusted Number is fixed in the Bank systems and used to send a one-time code as an SMS Message. The use (input) by the Customer of a one-time code confirms the authentication of the Customer and, in conjunction with the second authentication factor, is the basis for providing access to the Customer to electronic banking services and other services under the Agreement.

If the mobile number of the Customer’s Authorized Person, being registered in the Onlinebank System as a Trusted Number is changed, or the Customer’s Authorized Person is changed, the Customer submits to the Bank an Application for changing the means of authentication in accordance with Annex 5 hereto. In case of loss/theft of the mobile (cell) phone of the Customer’s Authorized Person, upon an activated Cloud EDS available, the Customer is obliged to block access to Onlinebank System to the Authorized Person as soon as possible by contacting the Internet Banking Support Service or the Bank’s servicing subdivision. After the temporary blocking of the Authorized Person,

the certificate can be revoked or, at the request of the Customer, the Authorized Person can be unblocked. The revoked certificate is subject to replacement.

3.9. The Customer confirms that upon signing the Application/Application-Questionnaire, the Bank notified the Customer of the existence of various security levels in the Bank when connecting the Onlinebank System.

3.10. When selecting high security level the Customer selects the Key Carrier device (smart card or Java Token device) offered thereto, and one of the Dynamic Authentication Methods (Onlinebank authentication or eToken PASS device authentication) offered in Annexes 1, 2 hereto, and assigns the right to sign Electronic Documents to two authorized signatories (first and second signatures), where the signature of two Authorized Persons will be required for sending for execution to the Bank.

The Customer undertakes to connect the available Dynamic Authentication Method at the first login to the Onlinebank System and use this Dynamic Authentication Method when sending Electronic Documents to the Bank. If the Customer did not use the method chosen in Annexes 1 and 2 hereto, it will be considered that the Customer has connected the System with the medium security level, accepting all risks and has no claims to the Bank in the event of unauthorized access to the System.

3.11. When the Customer selects the Key Carrier device offered thereto (smart card or Java Token device), and one of the Dynamic Authentication Methods (Onlinebank authentication or authentication with eToken PASS Device) offered in Annexes 1, 2 hereto, and if the Customer specifies one user authorized to sign all documents in Onlinebank System and solely make decisions on sending the Electronic Documents to the Bank for execution, the Customer agrees to having chosen an average level of security, and being aware of the existing risk of such transaction signing scheme.

3.12. When the Customer selects only the Dynamic Authentication Method (Onlinebank-authentication or SMS authentication), without the Key Carrier, the System with a low security level is connected.

3.13. The Customer confirms that the Bank, by any means chosen by it, has informed the Customer about the risks incurred when connecting the Onlinebank System and selecting medium or low level of security.

3.14. When Customer selects medium and low security level, it will be fully responsible for the possibility of unauthorized access to the Workstation, potential risks when sending Electronic Documents for execution to the Bank, and in the event of damage, including actual damage and/or lost profits, and has no claims to the Bank.

When using a mobile device to access Onlinebank System, the threat of fraudulent attacks increases due to numerous vulnerabilities of mobile platforms, and simplified scenarios of users' work with mobile apps. The Customer undertakes to comply with the requirements to ensure the confidentiality of information stored on the mobile device connected to Onlinebank System.

3.15. The Bank transfers to the Customer the devices selected by the Customer upon connection to the Onlinebank System, in accordance with Annexes 1 and 2 hereto, which the Customer is entitled to use solely to receive electronic banking services and other services under the Agreement.

In the event that the Customer, upon connection of the Onlinebank System, selects the Key Carrier – smart card, the Bank also delivers to the Customer a card reader.

3.16. The warranty period of the Authentication Devices issued by the Bank is 1 year from the date when the Bank employee issued devices. In the event of failure of this device during the warranty period due to manufacturing defect, the Bank shall replace it at no charge, upon any visible damages (through the Customer's fault) – as per the Bank tariffs. In the event of a breakdown of the device after the warranty period expires, replacement is made on a fee basis according to the tariffs of the Bank.

If the Customer disconnects from the Onlinebank System, the Authentication Device breaks and/or Customer's registration certificate expires, all Authentication Devices remain with the Customer, or, if desired, can be transferred to the Bank. When accepting Authentication Devices from the Customer, the Bank carries out mandatory clearing of Key Carriers.

If the Customer loses the Authentication Devices, the Bank shall, upon the Customer's initiative, reissue the device to the Customer on a fee basis according to the tariffs of the Bank. Key Carriers will be cleared.

3.17. The Parties agree that Authentication Devices will be deemed transferred by the Bank to the Customer from the moment the Parties sign the Acceptance and Transfer Certificate (Annex 6 hereto).

3.18. If the Customer opens new accounts with the Bank, they are automatically uploaded to the Onlinebank System. The rights of the Authorized Persons will automatically apply to newly opened accounts. To make changes in setting the rights of Authorized Persons to newly opened accounts, the Customer will need to contact the Bank.

3.19. Individuals, who will be entitled to sign the Customer's Electronic Documents as the Customer's authorized persons, will be determined based on the applications submitted by the Customer to the Bank in the form of Annexes 1 and 2 hereto or Application Forms, where for connection to the Onlinebank System, the trusted number of the Authorized Person is indicated, or upon the application for linking the user in accordance with Annex 3 hereto. The application for linking the user (Annex 3 hereto) is to be completed by the Customer if the Authorized Person who the Customer grants the right to sign its Electronic Documents to already has the EDS of the Certifying Center, and a new certificate is not required to be issued. Each application submitted by the Customer will form an integral part of the Agreement. If an Authorized Representative of another Customer is connected to view and manage the Customer's accounts, the Customer granting the right to view or manage its accounts shall fill in the User Linking

Application (Annex 3 hereto). The Bank may grant the Authorized Representative of another Customer access to viewing and managing the Customer's accounts subject to the Customer's written consent or an agreement between the Customer and another Customer.

The Customer can use Onlinebank Halyk web-version and Onlinebank for Business mobile application to connect a user - holder of the Fuel Corporate Card with viewing rights within the Fuel section and the possibility to make a payment using the Fuel Corporate Card by means of QR.

If the Customer resigns or changes the Authorized Representative, the Customer shall submit to the Bank a user disconnection application (Annex 4 hereto), in case of loss/damage of the Key Carrier, forgetting the password or compromising the keys, the Customer shall submit to the Bank a new certificate issue application in the form of Annex 2 hereto, as prescribed by the Bank, marked "certificate reissue".

The Customer may activate OnlineDuken cashier - a user with the right to independently sign documents generated by OnlineDuken Halyk platform through Onlinebank for Business Mobile Application based on the application in the form of Annex 8 hereto. OnlineDuken cashier shall also be deactivated in Onlinebank for Business Mobile Application based on the application in the form of Annex 9 hereto.

Remote reissue of EDS keys is available only to the Customer's user connected to Business version via the Onlinebank Halyk web-version not earlier than 30 days before the expiration date of the certificate.

3.20. The Customer agrees that the Authorized Person, who, in accordance with the application, has been granted the right to put signature using EDS and/or one of the Dynamic Authentication Methods, can perform operations, actions, sign documents, including for transactions, using the registration certificate of an individual – Cloud EDS. Electronic documents used when performing transactions in the Onlinebank System and/or through the Mobile Application, signed by the Cloud EDS, are equivalent to paper documents and give rise to similar rights and obligations of the Parties.

The Customer agrees that the Authorized Person, who has been granted the right of first signature with the use of EDS and/or one of the methods of dynamic authentication in accordance with the application, may submit applications for connection of other users to Onlinebank HALYK System with the granting of the right of signature with the use of EDS and/or one of the methods of dynamic authentication. The Customer and the authorized person with the right of first signature are responsible for the actions of the authorized persons as their own.

3.21. The Customer assures the Bank that the Authorized Person specified in Annexes 1, 2 or 3 hereto will perform operations, actions, sign documents, including documents for transactions, not only in accordance with the power of attorney issued thereto by the Customer, but also if the Customer has:

- a preliminary resolution of the relevant body/official of the Customer, if such a resolution is necessary for the Customer to perform operations, actions, sign documents in accordance with its internal procedures, requirements of third parties, legal requirements, any other requirements that the Customer is obliged to fulfill, comply with, and/or
- resolution, permission, consent, approval, notification of the relevant state body and/or a person authorized by the state, the availability whereof may represent a necessary condition for the Customer to perform operations, actions, sign documents between the Customer and the Bank, including the conclusion of a transaction between them, as well as the Customer's execution of its obligations thereunder.

3.22. The Customer confirms that when the Bank expands the list of operations that can be performed through the Onlinebank System using Electronic Documents, the Customer will issue a power of attorney to the said Authorized Person with the authority to perform new operations using an EDS and/or one of the Dynamic Authentication Methods. The above Customer's assurances also apply to new operations. The Customer assures having a proper system of control over the use by persons authorized to sign using EDS and/or one of the Dynamic Authentication Methods, of the authority to use EDS and/or one of the Dynamic Authentication Methods.

3.23. If the Customer has not installed the components of Onlinebank HALYK System within one year from the date of issue and receipt of the Key Carriers, the Customer shall re-apply for the installation of Onlinebank HALYK System, as the certificate has expired. A new certificate is issued upon reapplication.

Clause 4. Provision of Services in the Onlinebank System

4.1. When providing services in the Onlinebank System, information exchange between the Customer and the Bank is carried out using EDS and/or Authentication method.

4.2. The Customer shall fill in documents, form messages (instructions) in accordance with the applicable legislation and the Bank's instructions, which the Bank shall familiarize the Customer with in advance, and the Customer shall bear all responsibility, including possible damage caused for improper execution of documents, messages (instructions).

4.3. Information on the Key Carrier and/or the generated one-time code, PIN code are confidential. In the event that the Customer discloses this information to third parties, the Bank shall not be liable for the losses, damages incurred by the Customer.

4.4. The Customer has the opportunity to use the Onlinebank System regardless of time and/or date. The Customer can send electronic Documents to the Bank for execution also at any time. At the same time, the processing and execution by the Bank of the received Electronic Documents addressed to counterparties who are not the Bank's Customers are possible only during the Operating Day.

The Bank's Operating Day is set by the Bank and can be changed unilaterally by the Bank. The Bank informs the Customer about the duration of the operating day and/or its changes in any accessible way, including without limitation, in the Bank's operating rooms.

4.5. The Bank suspends the provision of electronic banking services and other services under the Agreement due to a malfunction of the technical means providing the provision of electronic banking services and other services. In case of elimination of the reasons that caused the suspension of the provision of electronic banking services and other services, the Bank resumes provision of electronic banking services and other services under the Agreement.

4.6. To work in the Onlinebank System, the Customer shall ensure the availability of the following software and hardware and settings:

- licensed operating system Microsoft Windows 10 and above with installed up-to-date updates, or Mac OS latest version (with official license, and installed updates to the latest/up-to-date version);
- installed manufacturer's recommended security settings in Microsoft Windows 10 and higher operating system);
- Microsoft Edge, Chrome, Mozilla, Opera of latest versions;
- Internet access at a minimum speed from 2 Mb/s and higher;
- administrator rights on its computer;
- licensed antivirus software with current updated databases (with an official license and installed updates to the latest/up-to-date version);
- availability of a free USB port on the Customer's computer.
- CryptoSocket and TUMAR-CSP.

When Key Carrier on the smart card is selected:

- driver for the card reader;
- control panel KAZTOKEN (Kaztoken);
- if proxy server is used to access <https://halyk.onlinebank.kz>, a port 443 shall be opened to 195.200.74.55 and to access <https://onlinebank.kz>, a port 443 shall be opened to 195.200.74.49.

4.7. The list of transactions that can be made through the Onlinebank System using Electronic Documents:

1) acceptance of electronic payment orders for transfers in national currency, including:

- tax payments;
- transfer of mandatory pension contributions, social charges, compulsory medical insurance contributions;
- payments for goods and/or services;

2) receiving and sending instructions by means of the Financial Number;

3) acceptance of electronic payment orders for making transfers in foreign currency;

4) acceptance of electronic applications for conversion (purchase/sale) of foreign currency by the Customer;

5) acceptance of electronic applications for conversion through the Halyk FX platform;

6) provision to the Customer in electronic form:

- final Account statement;
- preliminary statement;
- savings account statement;
- savings account statement (deposit terms and conditions, opening/closing date, validity period);
- corporate card account statement broken down by corporate cards;

7) providing the Customer with certificates in electronic form (account certificate, account balance certificate, certificate on account turnovers for the period);

8) acceptance from participants of export-import currency control of documents related to currency control (contracts, invoices, agreements, invoices for payment, supplementary agreements, etc.), except for extra sheets to transaction passports, and transaction passports;

9) letters of the Parties (requests, applications, notifications, etc.);

10) applications for opening savings account and making, replenishing a bank deposit;

11) requests for registration certificates issue;

12) application-offers for the conclusion of a (covered, non-covered, blank) guarantee agreement;

13) replenishment of an account using the Automated Cash Register, withdrawing money through an ATM and Automated Cash Register, including online power of attorney;

14) accepting an electronic application for issuing a corporate card, including a digital one;

15) setting up the automatic account balancing off - creation of a standing order (transfer from the current account to the Customer's current account in automatic mode);

16) acceptance of electronic applications for current accounts in different currencies (the list of currencies for opening a current account is placed on the Bank's website);

17) acceptance of an application for credit limit;

18) acceptance of an application for lifting of limits on corporate cards;

19) acceptance of an application for accepting payments via Halyk QR;

20) acceptance of application for remote EDS key reissue;

21) acceptance of an application for changing the Customer's data at the Bank;

- 22) receiving public authorities' services State Services section;
- 23) order formation and payment on the OnlineDukon Halyk platform;
- 24) notifications of receipt/crediting of currency;
- 25) 1C Direct Bank – integration with the Customer's 1C-Accounting;
- 26) providing Customers with the opportunity to use the Obuhgalter service to generate and send invoices (with the option of integration with the Customer's accounting system), generate and conclude agreements with counterparties in electronic form, conclude escrow account agreements, and signing them using an electronic digital signature, as well as generating and sending work completion reports and invoices, if technically possible;

27) web service – integration with the accounting/bookkeeping system of the Customer through API technology.

27-1) access to the Bank's web service (SOAP technology) is provided using the Customer's file certificate, which is issued to the Customer's Authorized Person in accordance with the cover letter. Integration with the Customer's accounting/bookkeeping or other system is carried out using the Customer's resources.

27-2) access to the Bank's web service (REST technology) is provided using an API key issued to the Customer's Authorized Person in accordance with the electronically signed API Key Creation Access Agreement. Integration with the Customer's accounting/bookkeeping or other system is carried out using the Customer's resources.

28) providing customers with an opportunity to use the functions of ESalyq Business mobile application of the State Revenue Committee of the Ministry of Finance of the Republic of Kazakhstan in terms of generating receipts in manual and automatic modes, receiving notifications on the assessed amounts of taxes and social payments and their settlement, generating certificates under the special tax treatment;

29) acceptance of electronic applications for connecting to Halyk Market system (acceptance of applications for creating a role to go to a personal account of Halyk Market);

30) acceptance of electronic applications for connection to Online Security (secure accountant's office);

31) acceptance of applications for increasing the cash withdrawal limit set by the State Revenue Committee;

32) acceptance of applications for POS terminal issue and replacement;

32-1) use of authorization and creation of an account via Halyk Business ID on services (mobile application and/or web service). To create an account and subsequently authorize it on Partner services, the Customer agrees to the transfer of data and the creation of an account for the Customer and Authorized Representative on the Partner's mobile application and/or web service and/or internet resource when switching to the Partner service via Halyk Business ID;

33) any other banking service or operation that can be additionally included in this list by posting information on the Bank's website at www.halykbank.kz, onlinebank.kz and <https://halyk.onlinebank.kz>.

The Customer may independently disable access in the Onlinebank System for Authorized Persons who do not have signing authority and a valid registration certificate.

In case of new operations becoming available or previously available operations being discontinued using the Onlinebank System, the Bank shall unilaterally (without consulting the Customer) change the list of operations available at www.halykbank.kz, onlinebank.kz and <https://halyk.onlinebank.kz>, and publish a new one.

The list of available operations depends on the version of the System chosen by the Customer.

The Customer can get information, consulting, and service on Onlinebank System in any bank subdivision servicing legal entities, in the Bank's Call Center by phone. The telephone numbers of the Bank's Call Center are located on the Bank's corporate website www.halykbank.kz, in the Business section.

In Onlinebank Business, transactions are available without limitation on the amounts and number of transactions, if EDS confirm them in the key medium.

Onlinebank Start offers tax, social and pension payments, viewing/uploading statements on own accounts, currency conversion and transfers between own accounts, transferring salaries and other payments to current/card accounts without restrictions, issuing corporate payment cards, and also making payments in favor of counterparties, including receiving and sending transfers to the Financial Number, within the limit on the total amount and on the number of payments per month. In addition, the followings are available to the Customer: conducting Electronic Documents in foreign currency, provision of electronic currency control, information on refunds of payments, and cash transactions for accepting and withdrawing cash from an account through the Automated Cash Register and ATM.

4.8. The list of conditions for conversions on Halyk FX platform:

1) Application for conversion sent via Halyk FX platform is confirmed by the customer at the time of saving/confirmation of the request and is recognized by the Bank as agreed with the Bank's Treasury;

2) When single customer initiates 2 applications for conversion with the same amount, currency and party to the transaction, the platform does not allow the creation of a 3rd application with the same conditions as the previous 2 applications;

3) The Bank may independently determine the period for the customer to sign a conversion request in Halyk FX system after confirmation of the exchange rate.

If several conversion requests submitted by one Customer are not signed and sent by the Customer to the Bank before the end of the current Operating Day, and if this is done systematically, the Bank may disable Halyk FX platform for such a customer;

4) The Bank is entitled to set limits for conversions initiated by the Customer outside of the operating time.

4.9. The Bank provides for the possibility of integrating the Customer's accounting/bookkeeping system for the transfer and receipt of Electronic Documents through the use by the Customer of the registration certificate in the form of an Electronic Document – a file certificate, while the document is transferred to the Customer without it being recorded on the Key Carrier. The file certificate is issued after the Customer signs the Agreement in the form of Annex 7 hereto. Since the file certificate is protected only by a password, all risks associated with the possible unauthorized use, and upon the transfer to third parties, of file certificates registered and used to sign the Customer's Electronic Documents are borne by the Customer.

The Bank transfers the file certificate to the Customer within 10 (ten) business days from the date of its issue by the Certifying Center, under the File Certificate Acceptance and Transfer Certificate between the Customer and the Bank, the form whereof is given in Annex 1 hereto.

4.10. The electronic document generates the obligations of the Parties in accordance with this Agreement, if it is duly executed, certified by EDS and/or confirmed by one of the Authentication Methods, delivered through telecommunication system specified herein by the transmitting Party, and verified and accepted by the receiving Party.

The Bank does not accept Electronic Documents and messages (instructions) for processing in the following cases:

- if the document is not signed;
- if the document is not encrypted;
- if the document is not encrypted for the receiving Party;
- if the document is distorted after the signature;
- if the status "withdrawn" is assigned for registration certificate of the document's signatory;
- if the owner's registration certificate validity has expired.

4.11. Electronic documents, messages shall not be processed by the Bank in the following cases:

- if the value date is earlier than the date of actual sending of the document;
- insufficiency of money on the Account;
- any third party claims to the account (List 2);
- garnishment of Account by the Authorized bodies;
- sending payment document to the countries with the highest credit card fraud;
- incorrect completion of the Electronic Document;
- other cases provided for by internal regulatory documents of the Bank and/or by the applicable legislation.

4.12. The Parties mutually undertake to assume in full all obligations arising from Electronic Documents and messages signed by one of the Dynamic Authentication Methods and/or by their EDS private keys, registration certificates registered in the Certifying Center if the EDS verification was successful and by the time of receipt of the document there was no formal declaration of the signatory about the compromise of its EDS private key or software. Failure of either Party to do so shall constitute grounds for withdrawal by the other Party.

4.13. The Customer acknowledges that EDS private keys are on a key carrier (Cloud EDS – in the Certex Cloud base) and issued in a single copy.

4.14. The Bank keeps Electronic Documents in the format in which they were generated, sent or received in compliance with their integrity and unchanged from the date of Customer connection to the Onlinebank System. The Bank is entitled not to store documents for more than one year, taking into account the requirements of the Applicable Legislation.

The Bank does not print out Electronic Documents on paper with the purpose of storing or transferring them to the Customer. The Bank prints out Electronic Documents on paper on Customer's request, for each copy the Bank charges fee in accordance with the current tariffs.

4.15. The Customer can use the Mobile Application as an additional option of remote control of the Account within the framework of electronic banking services, which the Customer can connect independently through the settings in the System under the Onlinebank HALYK Business version or automatically when the System is connected under the Onlinebank HALYK Start version.

4.16. When accessing the Onlinebank System via the Mobile Application, the Customer shall ensure the independent availability of a mobile device that meets the following parameters:

- mobile OS version not lower than Android 5.X and iOS 13.0;
- minimum screen size of at least 800 x 480 (hdpi) for devices powered by mobile Android OS;
- access to the Internet.

The Cloud EDS can be used in the Mobile Application only after the mobile device Verification. Without mobile device Verification, the functionality of the Mobile Application can be used with the Bank's daily limit for Electronic Documents sent to the Bank for execution.

Upon verification of the Mobile Device, a Cloud EDS is issued and subsequently used, which enables the Customer to sign Electronic Documents sent to the Bank for execution within the increased daily limit on the amount of transactions. The information on limits is posted at www.halykbank.kz. It is possible to verify a mobile device through the video identification process or by scanning a QR code at the Bank's outlets.

4.17. The Customer acknowledges that Mobile Application is an integral part of the Onlinebank System and its operation is impossible without connecting to the Onlinebank System.

4.18. In the event that the Customer has not contacted the Bank to receive the Key Carriers and/or the device required for the Dynamic Authentication Method within 30 calendar days after the issue of the Registration Certificate for connection to the Onlinebank System, the Bank does not issue Key Carriers and/or the device necessary for selected Dynamic Authentication Method, but charges fee for connecting to the Onlinebank System in accordance with the Bank Tariffs. The Customer shall apply to the Bank again to issue a new Registration Certificate.

Clause 5. Security

5.1. The Customer agrees to follow security procedures and any other instructions provided by the Bank to the Customer regarding the Onlinebank System security.

5.2. The Customer undertakes not to take any actions that may cause violations of the Bank's cyber security, or failures in the operation of information systems and violations of security thereof, caused by the Customer's actions/inaction and/or interference of third parties through the Customer's fault.

5.3. The Customer assumes full responsibility for the installation, maintenance and regular monitoring of the security and the use of authentication devices, as well as information stored in Customer's computer and communication systems, mobile devices, and in particular, password control for logging on to the Onlinebank System, control over passwords to access the Mobile Device (Face ID/Touch ID, access code).

5.4. The Customer undertakes to promptly notify the Bank of any unauthorized access to the Onlinebank System, including the Mobile Application, to the Workstation or an unauthorized transaction, which is known or suspected.

The Customer undertakes not to disclose the PIN code to third parties, as well as ensure that it is impossible to access it.

5.5. The Customer agrees to hold the Bank harmless from all claims and litigation, reimburse the Bank for any costs, damages and losses of any kind, to which the Bank may be exposed as a result of the Customer's failure to perform or improper performance of the obligations under this clause.

5.6. The Customer undertakes to treat with due care the devices transferred thereto by the Bank:

- the Key Carrier, in case it was used to connect to the Onlinebank System;
- the Card Reader, in case of selecting a smart card as a Key Carrier;
- the eToken PASS device, if the Customer selects this dynamic authentication method.

The Customer also undertakes to avoid mechanical disturbance (fall, shake, vibration, etc.), not to disassemble on its own, to protect from sudden temperature changes, prevent dust, dirt, moisture, not to expose to high voltage and other factors that may adversely affect operation of the above devices.

5.7. The Customer confirms that the Key Carrier and/or the Card Reader is connected only to the serviceable equipment (USB ports, USB hubs with auxiliary power supply), it is extracted correctly, does not remain connected to the computer when the latter is turned off, rebooted and goes into sleep mode. The Customer can learn more about security measures on the Onlinebank System page: <https://halyk.onlinebank.kz/wiki/> or <https://halykbank.kz>

5.8. The Customer undertakes to comply with the Bank's recommendations in terms of security, including, but not limited to the list of measures contained herein, on the devices used to work with Onlinebank System (Mobile Device and/or Workstation):

- not install any remote administration programs (e.g. TeamViewer, AmmyyAdmin, AnyDesk, RustDesk, etc.) on their device used to log in to Onlinebank System;
- never visit the website of Onlinebank System using the links provided in e-mails, or open files received from unreliable sources via the Internet or removable media, without first checking them for viruses, plug-ins or malicious programs;
- not leave the computer unattended with the power on, software loaded, and the Key Carriers connected to the Workstation;
- when completing work with Onlinebank System, exit by pressing the "Exit" button;
- when working with Onlinebank System, not open other websites in this browser, to exclude visiting websites with doubtful content, or any other Internet resources (forums, social networks, chat rooms) from the Workstation.

It is prohibited to work with Onlinebank System from Workstations that are not trustworthy (Internet cafes, other people's Workstations), or using public communication channels (free Wi-Fi).

5.9. The Customer undertakes to adhere to the recommendations of the password policy when setting the PIN for the Key Carrier:

- use Latin letters and numbers. The password shall contain at least 6 characters, at least 1 upper case letter, at least 1 lower case letter, at least 1 digit and at least one special character;
- when changing the password, not use the last 5 passwords used before;
- not use the same passwords for Online Banking of different second-tier banks and organizations performing certain types of banking operations;
- not use as a password the first name, surname, birthday and other memorable dates, telephone number, user's IIN or company's IIN/BIN, residence address, short name of a legal entity or other data that can be picked up by an intruder by analyzing information about the user;
- not use automatic password saving in browsers;
- not use as a password a combination of characters typed in a regular order on the keyboard (qwerty, 123456, etc.);
- perform independent quarterly password change, mandatory password change upon dismissal or change of employees.

5.10. The Customer undertakes to always set a password for the account on the Workstation when working with Onlinebank System, and to contact the Bank through available communication channels in case of detection of any anomalies, darkening of screens, loss of control of the Workstation, to interrupt the work on the computer, disconnect it from the power supply, and immediately notify the Bank through available communication channels.

5.11. When working with Onlinebank System, the Customer shall make sure that the secure connection via https protocol is established exactly with the official website <https://onlinebank.kz/> or <https://halyk.onlinebank.kz/>. It is strongly not recommended to go to this page using a link from Internet resources or e-mails received (except for the official website of the Bank <https://halykbank.kz/>).

5.12. When using the mechanism of importing/uploading documents from public access catalogs, it is necessary to ensure the security of the same. Access rights to those catalogs should be the minimum necessary to ensure transport functionality. The documents uploaded from public access catalogs shall necessarily pass the stage of visual control by users uploading and signing those documents.

5.13. When using the Mobile Device to work with Onlinebank Mobile App, the Customer undertakes to follow the following security rules and recommendations:

- when working with Onlinebank Mobile App, it is obligatory to set the Mobile Device lock in the settings (PIN, password, graphic key or Touch ID/Face ID biometric data), and to set the automatic locking of the Mobile Device;
- install apps and updates thereof only through official stores: Google Play, Apple Store, AppGallery. Installation of apps from third-party sources is prohibited;
- install antivirus software or other anti-malware software on the Mobile Device and update it regularly;
- not use hacked Mobile Devices with activated super-user rights (root for Android Mobile Device, or jailbreak for iOS Mobile Device);
- not to open doubtful e-mails, links, multimedia content and SMS messages received from unknown persons on the Mobile device and/or Workstation used to work with Onlinebank System;
- not to install unknown software at the request of third parties on the Mobile Device and/or the Workstation used to work with Onlinebank System;
- not store confidential information, PIN of bank payment cards, PIN of key carriers on the Mobile Device, account passwords;
- immediately block the SIM-card in case of loss or theft of the Mobile Device by contacting the mobile operator, and to block the user of Onlinebank System by contacting the Contact Center of the Bank.

Clause 6. SMS Informing

6.1. In order to receive information on payments via SMS informing to the Trusted Number, the Customer independently sends a request for connection via the Onlinebank System.

6.2. SMS informing on payments is carried out through telecommunication networks provided by Republic of Kazakhstan cellular communication operators under the separate contracts/agreements concluded with the Bank that stipulate compliance by operators with the Bank's customer data confidentiality requirements.

6.3. The Customer hereby gives consent to the Bank to disclose to Republic of Kazakhstan cellular communication operators of the information constituting the Bank's banking secrecy, which the Bank possesses legally and which are required to connect the Customer to SMS informing service and dispatch SMS messages within these services. In doing so, the Customer represents that this written consent to the Bank to disclose information constituting bank secrecy has been submitted to the Bank when signing the application as per the form set forth in Annexes 1, 2 or 3 hereto, or the Application Form.

Clause 7. Commission Fee of the Bank

7.1. The Bank may withdraw by direct debiting of the Account the commission fee payable to the Bank for the services rendered under the Agreement, in the manner and within the terms stipulated by the internal documents of the Bank.

The Customer provides the Bank with unconditional consent for the Bank to withdraw commission fees for the services rendered by the Bank under the Agreement, as well as all costs incurred by the Bank in connection with the execution of the Customer's instructions under the Agreement, other debts of the Customer to the Bank, which the Customer may incur under the Agreement, by direct debiting of the Account by the Bank.

7.2. Tariffs are posted on the Bank's website at www.halykbank.kz. The Bank shall notify the Customer of changes, additions to the tariffs by posting information on the Bank's website at www.halykbank.kz at least 10 (ten) business days before such changes or additions enter into force, indicating in the notification the Customer's right to repudiate the Agreement (terminate the Agreement) without paying an additional fee for the termination, before the date when such changes or additions are put into effect.

7.3. The Bank may suspend or terminate the provision of services under the Agreement if it is impossible to retain a fee from the Customer. The Bank shall notify the Customer thereof in writing or by e-mail within 10 (ten) business days from the date of suspension/termination of the provision of services under the Agreement. If the Customer pays for the services, the Bank may resume the provision of services to the Customer, having notified the Customer thereof in writing or by e-mail.

Clause 8. Rights and Obligations of the Parties. Personal Information

8.1. The Parties shall:

- use systems of telecommunication, information processing, storage and protection only on operable and serviceable equipment, checked for computer viruses, Trojan virus programs, plug-ins, and programs capable of damaging the Onlinebank System and the Parties;
- not disclose to a third party (except for cases stipulated by the Applicable Law or supplementary agreement of the Parties) the specific methods of information protection used in the Onlinebank System, and the Bank also shall not disclose the information received from the Customer in the course of providing electronic banking services, except for disclosure of information stipulated by the Applicable Law;
- once a year (30 calendar days before expiration date), change the EDS private key and the registration certificate through the Onlinebank System, and if the EDS key is not changed before the expiration date, the Customer shall apply to the Bank for its re-issue on a paid basis according to the Tariffs of the Bank;
- immediately inform the other Party about all cases of suspicion of unauthorized access to telecommunication systems and to the EDS private key, Mobile Device, as well as about all cases of loss, theft of Authentication Devices, or damage of the software and hardware of telecommunication systems, information processing, storage and protection, for change of keys, password and other actions coordinated with another Party to keep the above mentioned software and hardware operable;
- if the Customer compromises its EDS private key, the Customer shall apply to the Bank for withdrawal of the registration certificate, or block the user who the key was issued for, by contacting the Internet Banking Support Service or the Bank's servicing subdivision;
- in case of receipt of notification from the Customer about suspicion of unauthorized access to the Onlinebank System, detection of suspicions of unauthorized access to the Customer's Workstation and/or the Customer's mobile device, the Bank shall immediately block all non-performed operations with Electronic Documents, messages (instructions) pending clarification of all circumstances;
- ensure the confidentiality of information contained in Electronic Documents, messages (instructions) in the course of providing and receiving electronic banking services.

8.2. The Bank may:

- refuse to accept Electronic Documents for execution on the grounds stipulated in the clauses of the Agreement;
- make changes in the mechanisms of the Onlinebank System protection at its own discretion;
- make changes to the Security Levels and the list of Key Carrier required devices and/or the Dynamic Authentication Method;
- without any additional consent of the Customer, make changes/additions to the list of documents required for operation in the Onlinebank System;
- block the Customer's access to the Onlinebank System in the event that the Customer's registration certificate expires;
- block the Customer's access to the Onlinebank System in the event of no Account activity and no funds on the Customer's Account for three consecutive months (on current accounts). Upon no Account activity and no funds on the Account for more than six consecutive months, terminate the Agreement by repudiation thereof;
- block the Customer's access to Onlinebank System in case of detection of suspicious/fraudulent transactions not confirmed by the Customer, following the results of the Bank's callback procedure;

- block the Customer's access to Onlinebank System in case of suspicion of fraud or unauthorized access to the Workstation and/or Mobile Device of Onlinebank System users;
- block all operations with the Customer's Electronic Documents, messages (instructions) in case of suspicion of unauthorized access to the Customer's accounts as a result of malware, until all circumstances are clarified;
- block access of the Customer's Authorized Person to Onlinebank System on available grounds without notification;
- block the Customer's access to the Onlinebank System in case of several successive attempts to enter the wrong PIN Code (the exact number of attempts to enter is determined by the Bank) and the value of the one-time password generated by the eToken PASS device, SMS authentication or Onlinebank authentication;
- block access of the Customer's Authorized Persons excluded according to the Customer's application from the signature specimen document;
- block the access of the Customer's Authorized Representative to the Onlinebank System in the event of a request from the Customer's founders/CEO regarding the refusal to grant access to the Customer's Authorized Person subject to the provision of documents confirming the change of the Authorized Representative (resolution, appointment order, application for disconnecting the user from the Onlinebank System), during the Operating Day from the moment of blocking access. Once the supporting documents have been submitted, the Bank shall revoke the certificate. If the supporting documents have not been submitted within the specified period, the Bank may unblock access for the Customer's Authorized Representative;
- block the Customer's access to Onlinebank System and subsequently disconnect the Customer from Onlinebank System, terminate the Agreement in case of suspicion of fraudulent or other illegal actions, in using their bank accounts opened with the Bank for this purpose, and/or in analyzing the transactions carried out through the Customer's bank accounts opened with the Bank. If the Customer's access to the System is blocked or the Customer is disconnected from the System, a notice shall be sent to the Customer in Onlinebank System;
- debit the Customer's accounts opened with the Bank for the amounts of compensation received by the Customer as a result of fraudulent transactions by the Customer, third parties when participating in the promotions under the Bank's bonus loyalty programs, in case of insufficient money on the accounts to issue payment requests for the Customer's accounts opened with other banks, organizations involved in certain types of banking operations;
- carry out any activities aimed at improving Onlinebank System security, including by requesting confirmation from the Customer of the details of Electronic Documents, messages (instructions), using the TUMAR CSP program and collecting data to identify suspicious activity, as well as by other means;
- inspect and test the Customer's equipment used to work in Onlinebank System, in case of suspicion of malicious programs implemented as a result of hacker attacks, viruses and other factors, due to lack of proper level of protection and non-compliance with the requirements for software and hardware, which attracted attempts of unauthorized access to the Customer's accounts. If the Customer refuses to provide equipment for its inspection and testing, the Bank shall not be liable for losses incurred by the Customer as a result of the incident;
- disconnect the Customer from Onlinebank System, terminate the Agreement in case of liquidation of the legal entity or discontinuation of the Customer's activities;
- disconnect the Customer and its Authorized Persons from Onlinebank System, terminate the Agreement if all the Customer's accounts with the Bank are closed;
- disconnect the Customer from Onlinebank System, terminate the Agreement in case of death of the Customer (individual entrepreneur, head of a peasant (farm) economy established on the basis of personal entrepreneurship, private notary, private bailiff, attorney, professional mediator), whose IIN was used to open the contract in the System;
- block the Customer's Authorized Person's access to Onlinebank System in case of the Customer's death;
- refuse to establish/continue business relations with the Customer if it is impossible to take measures to properly verify/update the information required by applicable law and/or the Bank's internal documents, as well as if there are suspicions that the business relations may be used by the Customer for the purpose of legalizing (laundering) of proceeds from crime or for the financing of terrorism, as well as in violation of the requirements of international economic sanctions;
- require the Customer (representative thereof) to submit information and documents necessary to identify the Customer (representative thereof), identify the beneficial owner, as well as provide information on tax residency, type of activities and source of financing of the transactions made;
- require that the Customer (representative thereof) provide other information and documents stipulated by the Bank's internal regulatory documents and procedures on anti-money laundering and counter-terrorism financing and (or) as part of compliance with the requirements established by international economic sanctions;
- refuse to accept Electronic Documents for execution on the grounds stipulated by the Bank's internal regulatory documents and procedures on anti-money laundering and counter-terrorism financing, as well as if the Bank has reasons to believe that the Customer's/Counterparty's operations fall under international economic sanctions or are aimed at evading international economic sanctions in the Agreement

- refuse to conduct the Customer's operation in case of identification of unusual/suspicious operations aimed at money laundering and terrorism financing, as well as the operation falling under international economic sanctions or aimed at evading international economic sanctions;
- refuse to conduct the Customer's operation if the Bank suspects that the Bank is used for the purposes of money laundering and terrorist financing, as well as for the purposes of violation/avoidance of international economic sanctions;
- refuse to accept Electronic Documents for execution on the grounds provided for in the Agreement;
- not accept Electronic Documents for processing on the grounds, but not limiting itself, provided for in the terms of the Agreement;
- set limits on the amount of money transfers to third parties and on payments to Trade/Service Providers in order to prevent fraudulent transactions and protect the Customer from unauthorized access to the account and independently determine the methods of authentication to confirm such transactions in Onlinebank System;
- suspend the execution of debit transactions on the account in case of suspicion that such transactions are being made for the purpose of legalizing (laundering) of illegally gained income or financing of terrorism, and for the purpose of violating/avoiding the requirements of international economic sanctions;
- refuse to accept for servicing a currency contract and/or addendum thereto if the Bank has grounds to believe that the contractual relations under the currency contract are used for the purposes of money laundering or terrorism financing, and/or fall under international economic sanctions, or are aimed at evading international economic sanctions;
- terminate business relationship with the Customer by unilateral repudiation of the Agreement in the following cases:
 - occurrence in the process of studying transactions of suspicions that the business relationship is used by the Customer for the purpose of legalizing (laundering) of illegally gained income or financing of terrorism and/or in violation of/bybypassing international economic sanctions;
 - repeated refusals to conduct debit transactions on the Account or suspension of all transactions on the Customer's bank accounts;
 - sanctions against the Customer and (or) affiliates, beneficial owners thereof imposed in accordance with the jurisdiction of any country (for example, USA, EU, UK and other) or an international organization (including, but not limited to, FATF¹, UN² and other), including in cases when the terms and conditions and business relations under the Agreement may entail application of restrictions and (or) sanctions to the Bank;
 - the Bank having reason to believe that the transactions of the Customer/Customer's counterparty, including agreements, are used for the purposes of money laundering or terrorism financing and/or subject to international economic sanctions or are aimed at evading international economic sanctions;
 - cases provided for by the Bank's internal documents and procedures on combating the legalization (laundering) of illegally gained income and the financing of terrorism;
- enjoy other rights provided in the Agreement, the Applicable Law.

8.3. The Bank shall:

- after entering into this Agreement and paying by the Customer of the appropriate fees in accordance with the Bank's Tariffs, register the Customer in the Onlinebank System, transfer to the Customer the Key Carrier, Card Reader in case the smart card is selected as a Key Carrier, and the eToken PASS device in case the Customer selects this Dynamic Authentication Method, to start operating with the Onlinebank System;
- provide electronic banking services and other services under the Agreement, in accordance with the terms of the Agreement, as well as execute Customers' instructions to transfer funds from the Account given to the Bank by means of telecommunications, decrypted and certified by the Customer's EDS, verified with the Certifying Center and/or confirmed by a one-time code generated with the Dynamic Authentication Method;
- provide the Customer with technical support on the Onlinebank System issues in accordance with the Bank Tariffs;
- not disclose information received from the Customer when providing electronic banking services (except as required by law);
- fulfill other obligations stipulated by the Agreement, the Applicable Law.

8.4. The Customer shall:

- read the terms and conditions of this Agreement and follow the recommendations of the Bank described therein;
- at its own expense provide access to the Internet and independently pay for the services of communication providers;

¹ FATF – Financial Action Task Force on Money Laundering – an intergovernmental organization that develops global standards for combating money laundering and terrorism financing (AML/CFT) and assesses the compliance of national AML/CFT systems with these standards.

² UN (United Nations) – an international organization established to maintain and strengthen international peace and security, to develop cooperation between states.

- execute payment documents in accordance with the Applicable Law and this Agreement;
- not modify, decompile, replicate or transfer software and hardware to a third party;
- at its own expense maintain its software and hardware used in accordance with this Agreement in proper working order;
- correctly disconnect the Key Carrier, if it is selected when using the Onlinebank System;
- at the end of the working session in the Onlinebank System – immediately retrieve the key carrier;
- notify the Bank of the termination/change of the powers of the Authorized Persons or their mobile phone numbers indicated in the applications submitted to the Bank for registration of the user in the System, and immediately revoke their registration certificates by filing the application. The Customer hereby gives the consent to the Bank to disclose to the persons indicated in the application, whose powers have been terminated, but of which the Bank has not received the relevant notice from the Customer, the information relating to bank secrecy and indicated in the SMS informing;
- timely disable access to Onlinebank System of Authorized Persons who do not have the right to sign or issued registration certificate;
- use the System in full compliance with the operating instructions provided by the Bank;
- immediately apply to the Bank for revocation of the registration certificate or blocking of the user in case of loss, disclosure, distortion of its private key or use thereof by other persons;
- not transfer the Key Carrier to third parties;
- provide the Bank with the equipment used to work in Onlinebank System for inspection and testing in case of suspicion of malicious programs implemented as a result of hacker attacks, viruses and other factors;
- prevent undue dissemination of information about its EDS private key;
- not disclose the EDS key PIN Code, not indicate it on the Key Carrier, at the Workplace, and/or not disclose the generated one-time code;
- after the first login to the Onlinebank System, change the EDS key PIN Code and not use the standard PIN Code in work;
- not make copies of the Key Carrier, not write third-party information on it;
- keep the Key Carriers in a safe place excluding access thereto by unauthorized persons;
- take all possible measures to prevent the loss of Key Carrier devices and/or the Dynamic Authentication Method, disclosure of information contained therein, distortion and unauthorized use of such information;
- not leave the EDS key unattended in the immediate vicinity of the Workstation;
- protect their computers and workstations used to connect to Onlinebank System, namely:
 - use strong passwords on the operating system of the computer/server;
 - not transfer passwords from the operating system account to any third party;
 - ensure restrictions on network connection from other computers in the local area network;
 - prohibit remote access by means of the operating system and other software for remote work (Radmin, AnyDesk, TeamViewer, etc.);
 - use only licensed software and operating system;
 - not install any programs on the computer used to work in Onlinebank System that are not used for working with Onlinebank System;
 - if any anomalies are detected, interrupt work on the computer, disconnect it from power supply, and immediately notify the Bank through available communication channels;
 - not modify the code of the web application of Onlinebank System;
 - allow Onlinebank System to check the security settings of the operating system of the computer which is used to perform transactions;
 - not use a password generator obtained outside the Bank;
 - not later than 30 (thirty) working days before the expiry of the EDS keys and the registration certificate validity, send via the Onlinebank System an electronic request to the Certifying Center for automatic prolongation of the term;
- in the event of a change in the information specified in the documents provided by the Customer when submitting an application for connection, the Customer is obliged to submit documents confirming such changes;
- provide the Bank with information and documents necessary for the Bank to fulfill its obligations stipulated by the Applicable Law and internal documents of the Bank, including information on beneficial owners;
- make transactions and receive cash/replenish the account through the Automated Cash Register and (or) Cash by code only directly by the Customer itself or by Authorized Persons thereof, that is, persons who have an EDS in accordance with the procedure established by the Applicable Law, as well as who have passed the identification procedure with the Bank and who themselves authorized the transaction in the Onlinebank System by signing the application with their EDS or by the Customer's authorized persons under a power of attorney issued through Onlinebank HALYK System by the Customer's Authorized Person;
- not transfer to third parties, whether personally or via Authorized Persons, the right to use the generated code/barcode for the Cash by code, Automated Cash Register products;

- immediately notify the Bank on authorizing the Authorized Person/Authorized Persons to manage the Account;
- indicate the trade name of the business and the logo when registering the Financial Number, and not use words/word combinations that could harm the business reputation of the Bank and/or third parties, in accordance with the legislation of the Republic of Kazakhstan;
- fulfill other obligations stipulated by the Agreement, the Applicable Law, and/or another contract/agreement concluded with the Bank.

8.5. The Customer may:

- to be serviced in the Onlinebank System in accordance with the terms of this Agreement;
- select a version of the Onlinebank System, suitable for its business;
- change the PIN Code in accordance with the requirements for the length and complexity of the password, set out in the operation manual provided by the Bank;
- in consultation with the Bank, if necessary, obtain additional eToken PASS devices, Card Reader and/or Key Carrier, in accordance with the current Tariffs;
- demand from the Bank the proper execution of the terms of this Agreement;
- enjoy other rights provided for by the Agreement, the Applicable Law.

8.6. The Customer agrees to the transfer by the Bank of information related to bank secrecy to law enforcement agencies, other competent government agencies, mobile operators, in case of detection of signs of money theft from the Customer's account (including by fraud), other illegal actions against the Customer, as well as to prevent such illegal actions (including in the future) and localize effects of such actions.

8.7. The Customer hereby certifies that with respect to the personal data of personal data subjects transferred and subject to transfer in the future by the Customer to the Bank, including those stated in Applications from Annexes 1, 2, 3 hereto, and subsidiaries of the Bank (the "Organizations") under the Agreement, as well as in other cases where, in accordance with the Applicable Law and (or) internal documents of the Bank and (or) Organizations, it is necessary to collect, process such personal data, the Customer has previously received from personal data subjects their consent to the collection and processing of personal data, transfer of personal data to a third party, including the Bank and (or) Organizations, processing of personal data by the Bank and (or) Organizations.

8.8. If necessary, as determined by the Bank and (or) Organizations, the Customer shall provide the Bank and (or) Organizations with documentary evidence of consents collected by the Customer from the personal data subjects to the collection and processing of personal data, transfer of personal data to a third party, including the Bank and (or) Organizations, and if it is impossible to provide the documentary evidence, will collect such consents, and then confirm the receipt thereof to the Bank and (or) Organizations.

8.9. Responsibility for unavailability of consents to the collection and processing of personal data, transfer of personal data to a third party, including the Bank and (or) Organizations, processing by the Bank and (or) Organizations of personal data is assigned to the Customer. In the event that any measures are applied to the Bank and (or) Organizations for violation of the legislation of the Republic of Kazakhstan on personal data and their protection, the Customer undertakes to reimburse the Bank and (or) Organizations, at the request of the Bank and (or) Organizations, any expenses and losses incurred by the Bank and (or) Organizations.

8.10. The Customer hereby provides the Bank with its consent for the Bank to disclose information constituting the Customer's banking secrecy to the money sender, when crediting the Customer's bank account with the money received from the sender through a transfer to the Customer's Financial Number. The disclosure by the Bank of the above information shall mean the indication of the Customer's account number (IIC) in the receipt issued to the money sender after the transfer amount sent thereby to the Customer's bank account has been credited.

Clause 9. Liability of the Parties

9.1. For failure to perform or improper performance of obligations hereunder, the Parties shall be liable in accordance with the terms of the Agreement and the Applicable Law.

9.2. Each Party shall not be liable for losses incurred by the other Party not through the fault of the first party as a result of the use of Electronic Documents, messages (instructions), including in execution of erroneous Electronic Documents, messages (instructions), if these documents, messages (instructions) have been prepared, confirmed and delivered by one Party, and verified and accepted by the other Party.

9.3. The Bank shall be liable for the timely and correct execution of transactions on the basis of Electronic Payment Documents, messages (instructions), in accordance with the Agreement.

9.4. The Bank shall be held fully liable for the safety and protection from unauthorized access of third parties to the Cloud EDS certificates stored on the Bank's server in the Certex Cloud System cloud storage facility, in accordance with the terms of the Agreement.

9.5. The Bank shall not be liable for losses incurred by the Customer as a result of any actions of third parties, including but not limited to, the Customer's counterparties/employees, who for any reason have approached to the Workstation, Mobile Device with activated Cloud EDS, Key Carrier, if connecting to the Onlinebank System using it, the Card Reader if smart card has been selected as a Key Carrier, and the eToken PASS Device if the Customer

has selected this Dynamic Authentication Method, information about PIN Code, if it has become possible through carelessness, negligence and/or willful intent of the Customer.

9.6. The Bank shall not be liable for any losses incurred by the Customer because of the Bank's compliance with anti-money laundering and anti-terrorist financing legislation, as well as the requirements of international economic sanctions;

9.7. The Bank shall not be liable for the execution/non-execution/accuracy of the execution of Electronic Documents, messages (instructions) of the Customer in case the Customer has not timely notified/has not notified the Bank of termination or change of the powers of the persons indicated in the application for connecting users, those authorized to initiate, confirm, send messages (instructions) through the Onlinebank System.

9.8. The Bank shall not be liable for the Customer's losses caused by the refusal of the Bank's correspondent bank involved in the transaction to execute or terminate execution of Electronic Payment Documents due to violation of international economic sanctions, including for the Customer's losses resulting from the blocking of transaction amounts by OFAC³ on the side of the Bank's correspondent bank due to signs of violation of international economic sanctions in the transfer.

9.9. The Parties hereby confirm that each Party assumes all and any risk of using any means of operational communication for the purpose of sending and/or receiving notifications (including, but not limited to, the risk of any intentional actions of third parties, including fraud, unauthorized access to the information sent, and loss of such information before its receipt by the Customer/Bank, caused by problems in operational communication means, service providers or equipment used to transmit notifications).

9.10. Reimbursement of damages, including real damages, lost profits resulting from the disclosure by the Customer's Authorized Person of the PIN Code, transmission regardless of the reasons to third parties of the Key Carrier in case the Onlinebank System is connected with its use, the Card Reader in case of selecting the smart card and eToken PASS device as the Key Carrier, if the Customer selects this Authentication Method, shall be settled between the Customer and the Customer's Authorized Person without the Bank being involved.

9.11. The Customer shall be liable for the lack of consents to the collection and processing of personal data for the transfer thereof to a third party, including the Bank, the Organizations. The Customer shall be liable for the lack of consents of the personal data subjects to cross-border transfer by the Bank of their personal data. If any measures are applied to the Bank for violation of the current legislation of the Republic of Kazakhstan on personal data and their protection, the Customer shall reimburse the Bank, at the request of the latter, for any costs and losses incurred thereby.

9.12. The Customer shall be held fully liable for the losses incurred in the event of unauthorized access to the certificate holder's Mobile Device, which is used to enter the Mobile Application and send Electronic Documents.

9.13. The Customer shall be held fully liable in case of unauthorized access by third parties to the generated code/barcode for making transactions on the Cash by code/Automated Cash Register product, as well as for the withdrawal of cash by third parties/replenishment of the Account by means of the generated code/barcode, including in case of loss of the generated barcode (application ticket with barcode) by the Customer or the Customer's Authorized Person. In case of non-compliance with this condition, the Bank shall not be liable for the losses incurred by the Customer, including due to actions or omissions by the Customer's authorized person, neither shall it reimburse them to the Customer.

9.14. Selected issues of losses, damage may be regulated in other clauses of the Agreement, by the Applicable Law.

Clause 10. Dispute Settlement

10.1. The Parties shall take measures to resolve the disputes, controversies and disagreements that have arisen through negotiations and through consideration by the committee established in accordance with this clause of the Agreement.

10.2. If it is impossible to negotiate or resolve the disputes, controversies and disagreements through negotiations, they are resolved in a judicial procedure established by the legislation of the Republic of Kazakhstan.

10.3. All issues related to the Agreement, directly or indirectly, and not settled herein shall be resolved and regulated by the Parties in accordance with the Agreement, and all matters not regulated by the Agreement shall be resolved in accordance with the Applicable Law, as well as internal regulatory documents of the Bank. The disputes arising between the Parties in relation to the application of the EDS and/or the Authentication Method shall be resolved by the expert and technical committee established for the resolution of each individual dispute.

10.4. The Customer shall submit to the Bank an application containing the essence of the claim with the indication of the Electronic Document, the document authorizing the Bank's performance of the Account transactions. The Bank shall, within no more than 7 (seven) business days from the date the Customer submitted an application, establish the expert and technical committee for consideration of the application. The committee includes representatives of the Customer, the Bank, the Certifying Center (if an Electronic Document was used), a

³ Office of Foreign Assets Control of the United States Department of the Treasury

representative of the Onlinebank System developer (if the message (instruction) was initiated without the use of the Key Carrier) and, if necessary, a representative of the Onlinebank System developer, independent experts. The Expert and Technical Committee shall be legally competent to consider the Customer's application with obligatory presence in its composition of one representative from the Customer, the Bank, and the Certifying Center/the Onlinebank System developer.

10.5. The Expert and Technical Committee shall consider the Customer's application by means of a technical examination of the Customer's EDS public key and the disputed Electronic Document, or a message (instruction) initiated without the use of the Key Carrier, including the following stages:

- establish the time of transaction;
- verify the integrity of the Onlinebank System software of both Parties by calculating the checksum and comparing it with the reference one;
- verify the ownership of the EDS private key of the Customer/the procedure for providing the Customer by the Bank with access to the service using dynamic identification of the Customer by the Bank;
- check the status of the registration certificate of the relevant private key of the Customer and its validity at the time of issue of the document/ operability of the eToken PASS device or other Dynamic Authentication Method selected by the Customer;
- conduct a test transaction for one tenge using the presented Key Carrier to verify the operability thereof. The test transaction data shall be extracted from the database, and the EDS is checked;
- conduct a test transaction for one tenge using dynamic identification of the Customer by the Bank when the Customer initiates the message (instruction) using the Authentication Method;
- extract the data and the Electronic Document EDS from the Onlinebank System database archive, and authenticate the Customer's EDS/extract the message (instruction) from the Onlinebank System database archive, and check the proper procedure for initiating and confirming the message (instruction).

Based on the technical expertise, an act is prepared and signed by all members of the Expert and Technical Committee.

10.6. If the Parties accept the resolution of the Expert and Technical Committee, it shall be executed not later than the next business day.

10.7. In case of refusal to execute the resolution of the Expert and Technical Committee, the Parties shall transfer the dispute that has arisen between them to the court in accordance with the Applicable Law of the Republic of Kazakhstan.

Clause 11. Force Majeure

11.1. If either Party's obligations hereunder are interfered with or delayed due to any events of force majeure described below, then the performance of the obligations by the Party shall be suspended pro rata to the time during which force majeure events last and to the extent that they interfere with or delay the performance of obligations hereunder. An affected party shall notify the other Party in writing within three (3) business days after the occurrence of force majeure and undertake all possible actions in order to reduce loss or damage to the other Party and to restore its ability to fulfill obligations hereunder.

11.2. Failed or untimely notice deprives the Party of the right to refer to any force majeure as a to a ground exempting from liability for non-fulfillment of obligations hereunder, except for cases when such failed or untimely notice is directly caused by the relevant force majeure event.

11.3. Force majeure means any acts of God, including but not limited to: fires (except for events happening due to criminal carelessness or negligence of the Parties), floods, earthquakes, wars (whether declared or not), insurrections, strikes, civil wars or riots.

In case a Party disputes the existence of force majeure circumstances, attribution of circumstances to force majeure, the other Party shall be entitled to apply for an opinion to a state body, organization, which are competent in matters of establishing the existence and duration of force majeure circumstances.

Clause 12. Validity. Language

12.1. The Agreement shall come into force after the Customer accedes to the terms and condition of the Agreement by signing of the Application for connection to the System (Annex 1 hereto) and/or the Application-Questionnaire.

12.2. The Agreement is concluded for an indefinite period.

12.3. The Agreement shall:

- 12.3.1. be terminated at any time by mutual agreement between the Bank and the Customer;
- 12.3.2. be deemed terminated in the event of termination of all agreements and closure of the last Customer's bank account opened with the Bank under agreements within which transactions were made using the Onlinebank System, from the date of closure of the last account and termination of the last agreement. In this case, the Parties shall make mutual settlements hereunder no later than 10 (ten) business days from the date of termination of the Agreement;

12.3.3. be terminated in case of repudiation of the Agreement by either Party, which notified (in the form of a written notification) the other Party to this end not later than 10 (ten) business days prior to the date of termination of the Agreement, except for cases when each of the Parties may terminate business relations with the other Party by unilateral repudiation of the Agreement, in accordance with the terms and conditions of the Agreement, the Applicable Law, in a shorter period of time.

12.4. Upon termination of the Agreement, the Parties shall perform all previous obligations to each other assumed and not terminated by the date of termination of the Agreement, and make settlements not later than the date of termination specified in the written notice of termination, unless otherwise provided for by the Applicable Law.

12.5. The Agreement is posted at www.halykbank.kz in the state and Russian languages.

Clause 13. Final Provisions

13.1. The Customer is not entitled to assign or transfer any rights or obligations under the Agreement without the prior written consent of the Bank. Any attempt of such assignment or transfer in violation of this Clause shall be void and have no consequences.

13.2 The Agreement represents a complete mutual understanding of the Parties and supersedes all previous written or oral agreements and arrangements that existed between them in respect of providing the Customer with electronic banking services and other services under the Agreement using the Onlinebank System.

13.3. The Bank reserves the right to make amendments to the Agreement unilaterally, informing the Customer thereof (except for changes in Tariffs in the list of transactions provided when using the Onlinebank System, the procedure whereof is regulated by other provisions of the Agreement) at least 10 (ten) business days before the effective date of the resolution of the authorized body of the Bank that has made amendments to the Agreement. Informing is made by sending by the Bank of a written notice to the Customer via Onlinebank System (confirmation of receipt of such notification by the Customer is not required), and by posting by the Bank of amendments to the Agreement (setting out the revised version of the Agreement and/or amendments to individual terms and conditions and/or supplements to the Agreement) on the Bank's website at www.halykbank.kz. After such notification or posting of amendments and in case the Customer does not agree with the amendments, the Customer should notify the Bank thereof in writing not later than the effective date of the amendments. In this case, the Customer has the right to repudiate the Agreement without penalty if those are not directly provided for in this Agreement. Potential risks associated with the Customer's failure to receive information about the amendments to the Agreement shall be borne by the Customer.

In the event that the Customer does not submit objections by the effective date of the amendments to the Agreement specified by the Bank, or if the Customer sends a written notice of consent to amendments to the Agreement to the Bank in one of the ways specified in this clause before the expiry of the term specified in part one of this clause, the Agreement continues to have effect subject to the amendments.

Written notification sent by the Customer in accordance with this clause shall be deemed received by the Bank:

- 1) on the day of receipt with the appropriate mark – when sent by courier;
- 2) on the 4th (fourth) calendar day after sending (according to the date of the document issued by the postal organization upon dispatch) – when sent by registered mail);
- 3) the day of dispatch – when sent by email;
- 4) on the day of dispatch – when sent via Onlinebank System.

13.4. Any costs incurred by the Bank in the event of its involvement in litigation between the Customer and third parties, as well as any other costs of the Bank that may arise as a result of the Bank's relations with the Customer and which are not regulated by tariffs, shall be charged to the Customer's account. The Bank shall issue an invoice to the Customer for payment, with an indication of the amount of costs. The Customer immediately after receipt of the specified invoice is obliged to make payment thereunder.

13.5. All documents related to this Agreement shall be executed in the state and/or Russian language as agreed between the Bank and the Customer, or other agreement between the Bank and the Customer, the service which the Customer has access to through Onlinebank System. If the Parties agree to execute the documents in two languages, in the event of possible disagreement regarding the content of such documents, the Parties shall be guided by the text of the corresponding document drawn up in Russian.

APPLICATION FOR CUSTOMER/USER CONNECTION TO THE SYSTEM AND ACCESSION TO THE AGREEMENT AND REGULATIONS OF THE CERTIFYING CENTER OF HALYK BANK JSC

Customer full name: _____

BIN/IIN: _____

Customer's contact number (mobile)⁴:

+7										
----	--	--	--	--	--	--	--	--	--	--

Onlinebank version:

☐ **Business**

☐ **Start⁵**

☐ For remote access to all Customers accounts ⁶

Notes ⁷:

☐ Disconnect from the current version

☐ Transfer the archive

The Customer hereby confirms that:
 the Customer has read and understood all terms and conditions of the Onlinebank HALYK System Service Accession Agreement (the "Agreement") available at the Bank's official website, agrees with and undertakes to perform the same properly, and accepts the same in full by acceding to the Agreement, and gives the consent to the Bank to amend such terms and conditions in accordance with the procedure set forth in the Agreement;
 the Customer has read and understood all the terms of the Regulations of the Certifying Center of Halyk Bank JSC (the "Regulations") available at: Regulations of Halyk Bank's Certifying Center on the official website of the Bank www.halykbank.kz, agrees with and undertakes to perform the same properly, and accepts the same in full by acceding to the Regulations as a whole, and gives the consent to the Bank to amend such terms and conditions in accordance with the procedure set forth in the Regulations;
 the Customer has the software and hardware specified in clause 4.6 of the Agreement, and requests to provide the access to Onlinebank HALYK System.

Please provide access to the Onlinebank System and generate cryptographic keys and registration certificate of an open cryptographic key for the user:

Authorized person (in Latin characters for non-residents)	Surname _____ Name _____ Patronymic (if any) _____											
ID document	document type: _____ number: _____ series: _____ issuing authority: _____ issue date: _____ 20__ expiry date: _____ 20__ IIN: (if any) _____											
Contact details	Trusted number ⁸ : <table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"><tr><td style="width: 20px;">+7</td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td></tr></table> Email: _____	+7										
+7												
Select an authentication method and Key Carrier for Business version	Select the Key Carrier: ☐ Java Token ☐ Smart card Select the Dynamic Authentication Method: ☐ eToken PASS device ☐ Online authenticator											
Signatory right	☐ No signatory right ☐ _____ signatory right ⁹											
Power of Attorney details												

⁴ The Customer's mobile number to be indicated, to which an SMS will be sent about the activation and readiness of the Key Carriers.

⁵ Only at online connection to Onlinebank HALYK System.

⁶ In the case of providing remote access on individual terms, an additional letter from the Customer will be required.

⁷ These marks are put when the Customer switches to another version of the System.

⁸ The "Trusted number" field is mandatory, it is used for SMS-authentication, SMS-informing and receiving an OTP-password.

⁹ 1 to 3 levels of document signing may be indicated.

1. By signing this application, the Customer, the Customer's representative who has signed this application, in accordance with the Law of the Republic of Kazakhstan "On Personal Data and Protection thereof" (the "Law") provides the Bank with the consent to collect and process their personal data on the following terms and conditions:

- 1) operator of the base containing personal data (the "Operator") – Halyk Bank JSC (abbreviated name), Halyk Bank of Kazakhstan Joint Stock Company (full name), BIN 940140000385;
- 2) surname, first name, and patronymic (if any) of the Customer, representative of the Customer who signed this application, as a data subject are indicated in the application in accordance with the identity document;
- 3) the consent validity period - from the date the Operator accepts this application and until the date of expiration of the Agreement retention period after its termination as established by the Applicable Law, the Operator's documents;
- 4) the Operator shall be entitled to transfer the personal data of the Customer, the Customer's representative specified herein to third parties – the Operator's subsidiaries, and to other third parties specified in the Agreement, including government authorities of the Republic of Kazakhstan, correspondent banks, on the basis of their requests;
- 5) while processing the Customer's, Customer representative's personal data specified herein, the Operator shall be entitled to perform their trans-border transfer in accordance with Article 16.3 of the Law;
- 6) the list of personal data related to the Customer, Customer's representative, collected and processed by the Operator:
 surname, first name, patronymic (if any is indicated in the identity document), including those contained in the digital identity document;
 year, month, date and place of birth; citizenship;
 individual identification number;
 identity document details;
 gender;
 biometric data;
 place of residence, legal address (place of registration);
 postal and e-mail addresses, telephone number;
 photographic image and video image;
- 7) I give my consent to the Operator to receive information related to the Customer, Customer's representative, from state and non-state databases, including information that will be received in the future by the state and non-state databases.

The purposes of collection and processing of personal data shall be specified in the internal documents of the Operator.

2. The Customer hereby assures the Bank that:

the person who, in accordance with the application, the Customer grants the signatory right using an EDS, is properly authorized under the power of attorney issued by the Customer thereto to perform operations, actions, sign documents, including documents for making transactions between the Customer and the Bank, using the electronic digital signature,

the person to whom the Customer grants the right of first signature in accordance with the application may submit applications for connection of other users to Onlinebank HALYK System with granting the right of signature using EDS and/or one of the methods of dynamic authentication and is responsible for their actions as for their own,

the Customer has consent of the connected person to collect, process personal data with the possibility of transferring personal data to third parties.

The Customer hereby warrants to the Bank that upon first request of the Bank and within the time specified by the Bank, depending on the need determined independently by the Bank, will provide the Bank, including through the above person, with any of the above documents (power of attorney, resolution, permission, consent, approval, notification). The Customer hereby unconditionally agrees that, if it appears to be impossible for the Customer and/or the above person to submit the documents requested by the Bank, including the power of attorney, and/or if the above person concludes a transaction with the Bank without the power of attorney and without appropriate powers thereunder, the actions by the Customer, including by the above person, to exercise any of the rights, performance of any of the obligations stipulated by the transaction, acceptance by the Customer from the Bank and/or by the Bank from the Customer of any performance under the transaction, performance of any of the Bank's/Customer's requirements within the transaction by the Customer and/or by the Bank, accordingly, will imply that the transaction made by the above person with the Bank is considered approved by the Customer in accordance with Article 165 of the Civil Code of the Republic of Kazakhstan and valid for the Customer upon its execution, without the need for the Customer to submit a separate document on the approval of the transaction.

The Customer agrees that an authorized person who, in accordance with this application, has been provided with the signatory right using an EDS and/or one of the dynamic authentication methods, may perform operations, actions, sign documents, including for transactions, using the registration certificate of an individual – cloud EDS.

Areas of use of the registration certificate (object identifiers determining the relationship in which an electronic document with an electronic digital signature will have legal value):

1. Electronic signature
2. Non-repudiation

Validity of registration certificate	1 (one) year
--------------------------------------	---------------------

A card reader is required in the amount of _____ pieces.

First signature <i>Chief Executive Officer</i>	Position _____ Full name _____	Signature	L.S. (if any)
Second signature <i>Chief Accountant</i>	Position _____ Full name _____	Signature	
Application completion date	_____ 20_____ day month year		

Information on the means of electronic digital signature used to generate the corresponding private key of the electronic digital signature, and designation of the standard of the electronic digital signature algorithm: “TUMAR-CSP”; GOST 34.310-2004.

Bank marks

eToken PASS device number ¹⁰	
Application accepted by <i>Bank employee</i>	Full name _____ Signature _____
Branch	
Head	Full name _____ Signature _____

¹⁰ To be completed by the Bank employee when transferring an eTokenPASS device to the Customer.

Annex 2
to the Onlinebank HALYK System
Service Accession Agreement

ONLINEBANK APPLICATION

Customer full name: _____

BIN/IIN: _____

☐ **CONNECT**

☐ **RE-ISSUE¹¹**

☐ Remote access to all Customer's accounts¹²

Please provide access to Onlinebank System and generate cryptographic keys and registration certificate of an open cryptographic key for the user:

Authorized person (in Latin characters for non-residents)	Surname _____ Name _____ Patronymic (if any) _____										
ID document	document type: _____ number: _____ series: _____ issuing authority: _____ issue date: _____ 20__ expiry date: _____ 20__ IIN: (if any) _____										
Contact details	Trusted number ¹³ : <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td style="width: 20px; text-align: center;">+7</td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td><td style="width: 20px;"></td></tr></table> Email: _____	+7									
+7											
Select an authentication method and Key Carrier for Business version	Select the Key Carrier: ☐ Java Token ☐ Smart card ☐ No key to be issued Select the Dynamic Authentication Method: ☐ eToken PASS device ☐ Online authenticator										
Signatory right	☐ No signatory right ☐ _____ signatory right ¹⁴										
Power of Attorney details											

The Customer hereby assures the Bank that:

the person who, in accordance with the application, the Customer grants the signatory right using an EDS, is properly authorized under the power of attorney issued by the Customer thereto to perform operations, actions, sign documents, including documents for making transactions between the Customer and the Bank, using the electronic digital signature,

the person to whom the Customer grants the right of first signature in accordance with the application may submit applications for connection of other users to Onlinebank HALYK System with granting the right of signature using EDS and/or one of the methods of dynamic authentication and is responsible for their actions as for their own,

the Customer has consent of the connected person to collect, process personal data with the possibility of transferring personal data to third parties.

The Customer hereby warrants to the Bank that upon first request of the Bank and within the period specified by the Bank, depending on the need determined independently by the Bank, will provide the Bank, including through the above person, with any of the above documents (power of attorney, resolution, permission, consent, approval, notification). The Customer hereby unconditionally agrees that, if it appears to be impossible for the Customer and/or the above person to submit the documents requested by the Bank, including the power of attorney, and/or if the above person concludes a transaction with the Bank without the power of attorney and without appropriate powers thereunder, the actions by the Customer, including by the above person, to exercise any of the rights, performance of any of the obligations stipulated by the transaction, acceptance by the Customer from the Bank and/or by the Bank from the Customer of any performance under the transaction, performance of any of the Bank's/Customer's requirements within the transaction by the Customer and/or by the Bank, accordingly, will imply that the transaction made by the above person with the Bank is considered approved by the Customer in accordance with Article 165 of the Civil Code of the Republic of Kazakhstan and valid for the Customer upon its execution, without the need for the Customer to submit a separate document on the approval of the transaction.

The Customer agrees that an authorized person who, in accordance with this application, has been provided with the signatory right using an EDS and/or one of the dynamic authentication methods, may perform operations, actions, sign documents, including for transactions, using the registration certificate of an individual – cloud EDS.

¹¹ When re-issuing the registration certificate, the current key will be canceled and a new one will be issued.

¹² If remote access is provided on individual terms and conditions, an additional letter from the Customer is required.

¹³ Trusted number field is mandatory, it is used for SMS-authentication, SMS-informing and receiving an OTP-password.

¹⁴ 1 to 3 levels of document signing may be indicated.

Areas of use of the registration certificate (object identifiers determining the relationship in which an electronic document with an electronic digital signature will have legal value): 1. Electronic signature 2. Non-repudiation	
Validity of registration certificate	1 (one) year

A card reader is required in the amount of _____ pieces.

First signature <i>Chief Executive Officer</i>	Position _____ Full name _____	Signature	L.S. (if any)
Second signature <i>Chief Accountant</i>	Position _____ Full name _____	Signature	
Application completion date	_____ 20_____ <i>day month year</i>		

Information on the means of electronic digital signature used to generate the corresponding private key of the electronic digital signature, and designation of the standard of the electronic digital signature algorithm: “TUMAR-CSP”; GOST 34.310-2004.

Bank marks

eToken PASS device number ¹⁵	
Number of agreement underlying the user connection ¹⁶	
Application accepted by <i>Bank employee</i>	Full name_____ Signature _____
Branch	
Head	Full name_____ Signature _____

¹⁵ To be completed by the Bank employee when transferring an eTokenPASS device to the Customer.

¹⁶ To be specified if the Customer has more than one agreement.

Customer Name: _____
BIN/IIN: _____

Authorized person (in Latin characters for non-residents)	Surname _____ Name _____ Patronymic (if any) _____ IIN: (if any) _____
Name, BIN of the organization the key was originally issued to	_____ _____
Signatory right	☐ No signatory right ☐ _____ signatory right ¹⁷
Reason for granting the signatory right	

- ☐
- For remote access to accounts listed below

No.	Account No.	Account currency
1		
2		
3		

First signature <i>Chief Executive Officer</i>	Position _____ Full name _____	Signature	L.S. (if any)
Second signature <i>Chief Accountant</i>	Position _____ Full name _____	Signature	
Application completion date	_____ 20_____ <i>day month year</i>		

Registration certificate serial No. and date of issue	_____
	“ ” _____
Application accepted by <i>Bank employee</i>	Full name _____ Signature _____
Branch	
Head	Full name _____ Signature _____

¹⁸ In the case the remote access is granted to all of the Customer's accounts, the account numbers are not specified.

Registration certificate serial No. and date of issue <i>(filled in only in case of revocation of user certificate)</i>	_____ “ ____ ” _____
Application accepted by <i>Bank employee</i>	Full name_____ Signature _____
Branch	
Head	Full name_____ Signature _____

Annex 5
to the Onlinebank HALYK System
Service Accession Agreement

APPLICATION FOR CHANGE/ADDITION OF THE AUTHENTICATION DEVICE

Customer full name: _____

BIN/IIN: _____

User _____
(full name, IIN)

Please select the authentication device you want to change or add:

☐ **Trusted (mobile) number** ☐ **eToken PASS**

☐ **TO BE CHANGED TO** **or** ☐ **TO BE ADDED**

☐ **Trusted (mobile) number:** ☐ **eToken PASS:**

+7

First signature <i>Chief Executive Officer</i>	Position _____ Full name _____	Signature	L.S. (if any)
Second signature <i>Chief Accountant</i>	Position _____ Full name _____	Signature	
Application completion date	_____ 20_____ _____ day _____ month _____ year		

Bank marks

eToken PASS device number ¹⁹	
Application accepted by <i>Bank employee</i>	Full name _____ Signature _____
Branch	
Head	Full name _____ Signature _____

¹⁹ To be completed by the Bank employee when transferring an eTokenPASS device to the Customer

Annex 6
to the Onlinebank HALYK System
Service Accession Agreement

ACCEPTANCE AND TRANSFER CERTIFICATE

_____ 20____

We, the undersigned, confirm the transfer of the Devices specified in the Application for connection of the user to Onlinebank HALYK system, Business version, (the “System”), according to Annex 2 to the Agreement (the “Annex”).

Key carrier _____ pcs

Card reader _____ pcs

eToken PASS device _____ pcs No. _____

Customer name: _____

BIN/IIN: _____

Customer’s authorized person:

Surname _____

Name _____

Patronymic (if any) _____

IIN _____

Transferred by:

Accepted by:

Bank employee transferring the Devices selected by the Customer to connect to the System, and registration certificate	Customer’s authorized person accepting the Devices selected by the Customer to connect to the System, and registration certificate
Position _____	(Power of Attorney No. _____ dated _____ 20 __)
Full name _____	Position _____
Signature _____	Full name _____
Position _____	Signature _____
Full name _____	
Signature _____	

Date and time of transfer: _____ 20____. _____
(time)

Customer CEO: _____
(full name)

Signature _____ L.S.
(if any)

Annex 7
to the Onlinebank HALYK System
Service Accession Agreement

FILE CERTIFICATE ISSUE AGREEMENT

_____ 20____

_____ **Halyk Bank of Kazakhstan Joint Stock Company** (the “**Bank**”), represented by _____, acting on the basis of _____, for the one party and _____, (the “**Customer**”), represented by _____ acting on the basis of _____, for the other party, hereinafter collectively referred to as the “**Parties**”, and individually as mentioned above, or the “**Party**”, taking into account that Onlinebank HALYK System Service Accession Agreement No. _____ dated _____ (the “**Agreement**”) concluded between the Parties provides for the possibility of using by the Customer of the registration certificate in the form of an electronic document, concluded this agreement for issue of the file certificate (the “**File Certificate Issue Agreement**”) as follows:

1. The Bank shall issue a registration certificate in the form of electronic document (the “**File Certificate**”) to each person authorized by the Customer in the manner specified by the Customer in the application, without recording it on the Key Carrier. The Key Carrier and PIN-code thereto, the Card Reader shall be neither used nor issued to the Customer.

2. The Customer unconditionally agrees that the File Certificate security level is lower than that of the registration certificates issued on the key carrier, as the file certificate is only protected by a password. Only the Customer’s authorized person, to whom the file certificate is issued, knows the password. All risks associated with possible unauthorized use of file certificates registered hereunder and used for signing the Customer’s electronic documents shall be borne by the Customer. Electronic documents signed with electronic digital signature generated with the use of file certificates are unconditionally deemed to have been sent by the Customer, unless prior to their sending the Bank has been notified of a threat of unauthorized access to the file certificate, of file certificate cancellation, or of termination of authority of the persons who the file certificates were issued to.

3. The Customer shall ensure that the authorized persons who the file certificates have been issued to, in a way as to restrict access thereto by third parties use the file certificate/file certificates. The Bank shall not be liable for improper protection of the file certificate by the Customer, regardless of the protection method(s) selected by the Customer.

To ensure the necessary level of security when working with the use of a file certificate, the Customer is additionally recommended to do the following:

- not leave the devices (usb-tokens) issued by the Bank unattended or connected to the computer in their absence. Never give them to third parties for use or as collateral;
- not leave the device connected to the computer when it is switched off, rebooted or in sleep mode;
- implement IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) systems that allow detecting facts and preventing attempts of unauthorized access to the corporate system;
- use a WAF (Web Application Firewall) solution to protect web applications published on the Internet. WAF allows you to effectively detect and counter attacks on web applications;
- in order to reduce cyber security risks, segment the network into server and user networks, and then provide access based on the principle of minimum sufficiency (IP address, port). Network segmentation will prevent unauthorized access to the organization’s servers in case of compromise of workstations of employees who do not need access to the server segment;
- when using remote connection, use certificates for RDP connections to the server part. It is desirable to connect via terminal servers;
- not use free e-mail services. Dedicate a server to implement Email Security Gateway class solutions to protect against phishing and spam attacks;

- use multi-factor authentication to access critical information systems in the organization for additional protection. Multi-factor authentication (MFA) requires two or more authentication factors for access, making it more secure. For example, in addition to a password, MFA may require a second factor, such as a one-time code that is sent to your cell phone.

4. Specifics of using the file certificate

To ensure web services security, the Certifying Center issues password-protected file certificates in .pfx format.

File certificate shall be used to perform any actions in a web service, including signing documents digitally. To use a file certificate, you shall get the key from the .pfx file. In addition, it is necessary to get a certificate from this file. For all these actions, there are APIs in different programming languages

In case of developing a “customer” for a web service using Java language, there are two ways to get the key:

- 1) Import the key and certificate into java keystore (key store). To import the key and certificate from .pfx file into the keystore, you need to use openssl and keytool applications;
- 2) Using the .pfx file as a repository directly from java code.

For example,

```
KeyStore pfx = KeyStore.getInstance("pkcs12");
pfx.load(new FileInputStream("somefile.pfx"), password);
```

If you use another programming language, such as C++, double-click on the file to store the key in Windows repository, and then use WinAPI to retrieve it from the repository in the code.

5. The Bank shall transfer the file certificate to the Customer within 10 (ten) business days upon its issue by the Certifying Center, based on the File Certificate Acceptance and Transfer Certificate, the form whereof is provided in Annex 1 hereto. The Acceptance and Transfer Certificate is executed by the Bank in two original copies, one for each Party, signed by authorized representatives of both Parties and sealed by the Bank. The Customer shall seal the Acceptance and Transfer Certificate with its seal, if any.

6. All terms used in this File Certificate Issue Agreement shall have the meaning ascribed to them in the Agreement concluded by the Parties.

7. When persons authorized by the Customer use file certificates, the terms of the Agreement shall be applied taking into account the specifics provided in this File Certificate Issue Agreement.

Those terms of the Agreement that are not affected by this File Certificate Issue Agreement shall remain in force unchanged and the Parties confirm their obligations thereunder.

8. This File Certificate Issue Agreement comes into force from the date of its conclusion and forms an integral part of the Agreement.

9. The File Certificate Issue Agreement is executed in two original copies each having equal legal force, one copy for each Party.

The Bank	The Customer
Halyk Bank JSC	
Bank address: _____ BIC: HSBKKZKX BIN: 940140000385	Legal address: _____ Tel./Fax _____ BIN (IIN): _____ IIC _____
For and on behalf of the Bank Position: _____ Full name _____ Signature _____ L.S.	For and on behalf of the Customer Position: _____ Full name _____ Signature _____ L.S. (if any)

**File Certificate
ACCEPTANCE AND TRANSFER CERTIFICATE**

_____ 20__

We, the undersigned, confirm the transfer of the File Certificate in accordance with the terms and conditions of the File Certificate Issue Agreement.

Customer name: _____

BIN/IIN: _____

Customer's authorized person:

Surname _____

Name _____

Patronymic (if any) _____

IIN _____

Serial number: _____

Transferred by:

Accepted by:

For and on behalf of the Bank	For and on behalf of the Customer
Position _____	(Power of Attorney No. _____ dated _____ 20 __)
Full name _____	Position _____
Signature _____	Full name _____
	Signature _____

Date and time of transfer: _____ 20__ . _____
(time)

Customer CEO: _____
(full name)

Signature _____ L.S.
(if any)

APPLICATION FOR CONNECTION OF ONLINEDUKEN AUTHORISED CASHIER TO ONLINEBANK SYSTEM

Customer name: _____

BIN/IIN: _____

Please provide access to the OnlineDuken Platform in the Onlinebank System and produce cryptographic keys and a registration certificate of the public cryptographic key for the user:

OnlineDuken Authorized Cashier (to be indicated in Latin for non-residents)	Surname _____ Name _____ Patronymic (if any) _____																				
Personal identification data	IIN: _____																				
Contact details	Trusted number ²⁰ : <table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">+7</td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> <td style="width: 20px;"></td> </tr> </table>	+7																			
+7																					
Right of signature	first signature																				

The Customer hereby confirms to the Bank that the person to whom the Customer grants the right to sign using EDS within the OnlineDuken Platform in accordance with the application has the necessary authorization to perform transactions, actions, sign documents, including documents for transactions between the Customer and the Bank, using electronic digital signature within the OnlineDuken Platform, including that the Customer has the consent from the person to collect, process personal data with the possibility of transferring personal data to third parties.

An authorized OnlineDuken cashier has the following authority:

- forming an order on the OnlineDuken Platform;
- making payments through the Customer's current account opened with the Bank for orders within the OnlineDuken Platform;
- directing the amounts of loans received under Facility Agreement for Deferred Payment Product (hereinafter referred to as "Agreement") only for the intended use - to purchase goods on the OnlineDuken Platform;
- adjustment of orders upon receipt of goods ordered on the OnlineDuken Platform;
- canceling the order before/at the time of receiving the goods ordered on the OnlineDuken Platform;
- acceptance of the goods ordered on the OnlineDuken Platform;
- conclusion, amendment of the Loan Application under the Agreement on behalf of the Customer

The Customer hereby warrants to the Bank that upon first request of the Bank and within the period specified by the Bank, depending on the need determined independently by the Bank, will provide the Bank, including through the above person, with any of the above documents (power of attorney, resolution, permission, consent, approval, notification). The Customer hereby unconditionally agrees that, if it appears to be impossible for the Customer and/or the above person to submit the documents requested by the Bank, including the power of attorney, and/or if the above person concludes a transaction with the Bank without the power of attorney and without appropriate powers thereunder, the actions by the Customer, including by the above person, to exercise any of the rights, performance of any of the obligations stipulated by the transaction, acceptance by the Customer from the Bank and/or by the Bank from the Customer of any performance under the transaction, performance of any of the Bank's/Customer's requirements within the transaction by the Customer and/or by the Bank, accordingly, will imply that the transaction made by the above person with the Bank is considered approved by the Customer in accordance with Article 165 of the Civil Code of the Republic of Kazakhstan and valid for the Customer upon its execution, without the need for the Customer to submit a separate document on the approval of the transaction.

The Customer agrees that the Authorized Cashier, who in accordance with this application has been granted the right to sign using EDS and/or one of the methods of dynamic authentication, may perform transactions, actions, sign documents, including for transactions, using the registration certificate of an individual - cloud EDS.

The Customer confirms that he/she will take all measures necessary to ensure that unauthorized persons cannot access the Onlinebank Halyk System.

If this confirmation becomes inaccurate, the Customer shall immediately notify the Bank.

The Customer shall be fully liable for the actions of its Authorized Cashiers, whose actions and circumstances indicate that such persons have the necessary authority. The circumstances evidencing that the persons have the necessary authorization include, in particular, submission of applications and/or other documents, including under the Agreement, via the Onlinebank Halyk System.

²⁰ Trusted number field is required, it is used for SMS-authentication, SMS-informing and receiving OTP.

Areas of use of the registration certificate (object identifiers determining the relationship in which an electronic document with an electronic digital signature will have legal value):	
1. Electronic signature 2. Non-repudiation	
Validity of the registration certificate	1 (one) year

Head	
Application date	20 Day Month Year

Signed using EDS

Data on electronic digital signature means used to create the corresponding private key of electronic digital signature and designation of the standard of electronic digital signature algorithm TUMAR-CSP; GOST 34.310-2004.

Bank marks

<i>The Bank's employee responsible for completeness of the Application and verification of information accuracy</i>	<u>Onlinebank HALYK</u>
Branch	

Annex 9
to the Onlinebank HALYK System
Service Accession Agreement

**APPLICATION FOR DISCONNECTION OF ONLINEDUKEN AUTHORIZED CASHIER FROM
ONLINEBANK SYSTEM**

Customer name: _____

BIN/IIN: _____

Please disconnect the user from the system:

OnlineDuken Authorized Cashier (to be indicated in Latin for non-residents)	Surname _____ Name _____ Patronymic (if any) _____
Personal identification data	IIN: _____

Head	
Application date	_____ 20_____ <i>Day Month Year</i>

Signed using EDS

Bank marks

<i>The Bank's employee responsible for completeness of the Application and verification of information accuracy</i>	<u>Onlinebank HALYK</u>
Branch	

Annex 10
to the Onlinebank HALYK System
Service Accession Agreement

API KEY CREATION APPLICATION

Customer name: _____

BIN/IIN: _____

I hereby ask you to issue a registration certificate in the form of an electronic document and create an API key in the name of _____

1. Provide an API key with access to the following services:

No.	List of possible accesses to services	Mark "Yes" to indicate the need to access services
1	Invoice service	
2	Payments and transfers in KZT service	
3	Currency transfers service	
4	Currency conversion service	
5	Account statements and balances service	
6	Acquiring statement service	
7	Payment order processing status service	

2. The Customer unconditionally agrees that the degree of protection of the API key is lower than the degree of protection of registration certificates issued on a key carrier. The Customer shall be liable for any risks related to the potential unauthorized use of the API key used to create the Customer's electronic documents. Electronic documents generated using the API key and signed with an electronic digital signature shall be unconditionally recognized as sent by the Customer if, prior to their sending to the Bank, no notification was sent regarding the threat of unauthorized access to the API key or the cancellation of the API key.

3. The Customer shall ensure that the API key(s) is/are used in such a way as to restrict access to them by third parties. The Bank shall not be liable for any failure by the Customer to adequately protect the API key, regardless of the protection method(s) chosen by the Customer.

4. To ensure the necessary level of security when using the API key, the Customer is additionally recommended:

- to implement IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) systems, which allow detecting and preventing unauthorized access attempts to the corporate system;
- to use a WAF (Web Application Firewall) solution to protect web applications published on the Internet. The presence of a WAF allows you to effectively detect and counter attacks on web applications.
- to segment the network into server and user segments in order to reduce information security risks, with subsequent access provided on the principle of minimum sufficiency (IP address, port). Network segmentation will prevent unauthorized access to the organization's servers in the event of compromise of workstations belonging to employees who do not need access to the server segment;
- to use certificates for RDP connections to the server side when using a remote connection. It is advisable to connect via terminal servers.
- not to use free email services. Allocate a server for the implementation of Email Security Gateway solutions to protect against attacks such as phishing emails containing malware and spam.
- to use multi-factor authentication to access critical information systems of the organization for additional protection. Multi-factor authentication (MFA) requires two or more authentication factors for access, making it more secure. For example, in addition to a password, MFA may require a second factor, such as a one-time code sent to your mobile phone.
- In the event of dismissal or replacement of the Authorized Representative to whom the API key was issued, the Customer shall independently delete the API key of that user. If this is not possible, the Customer shall provide the Bank with a letter requesting the deletion of the API key of that user.
- The Bank is not responsible for the transfer or compromise of the Customer's API key.

- In case of compromise of the API key, the Customer shall independently delete the API key, or apply to the Bank with a request to delete the API key, or block the user to whom the API key was issued by contacting the Online Banking Support Service or the servicing subdivision of the Bank.

5. Features of using the API key.

The API key is a secret key used only to send requests for creating payment documents and/or receiving information about accounts and documents.

An API key can be issued by a user with first signature rights. Only the user who generated the API key can use, copy, or delete it. Users without first signature rights will not be able to use it.

It is possible to issue/generate an API key only in the authorized area of Onlinebank.kz in My Account. It is also possible to manage the generated API key in this section.

The API key is required to send requests in accordance with the technical documentation.

The process of signing documents generated using API keys remains unchanged. If amendments to the process of signing documents created using API keys are required, the terms and conditions will be discussed on a case-by-case basis.

Signatures:

CEO:

Chief Accountant:

EDS document information: