1. *The Rules are posted on August 25, 2018. The Rules became effective from September 4, 2018*
2. *Change and additions approved by a decision of the Management Board of ATFBank JSC (minutes № 111 of a meeting on October 29, 2020). Change and additions are posted on November 6, 2020. Change and additions became effective from November 16, 2020*

Rules on E-banking via "ATF Online" System in ATFBank JSC

Subject:	These Rules regulate the procedure and terms of E-banking via "ATF Online" System in ATFBank JSC	
Code of the Document	ПР.7255.113	
Developer:	Cards and remote channels support department	
Regulation entites:	Security Department Corporate Department Corporate Department and Private Banking of the Central Region SME Department Digital Technologies Design Department	
Coordinated with:	Security Department Corporate Department and Private Banking of the Central Region Compliance Control Department Digital Technologies Design Department Strategic Risk Department Business Processes Support Unit Corporate development and support unit SME products design unit Legal Department	
Approved by:	Management Board of ATFBank JSC (Minutes № 76)	09.08.2018
Next update:	Upon expiration of 1 (one) year since entering into force	
Introduced amendments:	Management Board of ATFBank JSC (Minutes № 111)	29.10.2020
Cancelled documents:	Rules in E-banking via ATF Online System in ATFBank JSC	Approved by Management Board of ATFBank JSC (Minutes № 78 dd 15.12.2015)

Table of Contents

Chapter 1. General terms

Article 1. Main notions

1. The following notions and abbreviations are used in these Rules on E-banking via “ATF Online” System in ATFBank JSC (further – Rules):

1) **Authentication** is a confirmation of the authenticity and correctness of the preparation of e-document in accordance with the requirements of the Security Procedure upon connection to "ATF Online" System;

2) **The Bank** is ATFBank JSC;

3) **Bank account** is a method of reflecting and recording the movement of the Client's funds in the Bank, as well as contractual relationship between the Bank and the Client in respect of the Client's banking services. Under he Agreement, current and/or savings account are related to bank account;

4) **Website of the Bank:** http://www.atfbank.kz;

5) **Agreements** is an Agreement on E-banking via “ATF Online” System, concluded between the Bank and the Client;

6) **Private(secret) key** is a sequence of electronic digital symbolds, known to the User/Authorized person of the Client and designated for EDS creation with the use of the means of electronic digital signature;

7) **Application for access** is an application for accessing ATF Online System, executed in accordance with the form specified in Appendix No 1 hereto. Propertly executed and accepted applications for access are an integral part of the Agreement;

8) **Identification** is procedure for establishing authenticity of the User/Authorized person of the Client for unambiguous confirmation of his rights to receive E-banking;

9) **Username (login)** is a unique name of the User/Authorized person of the Client in «ATF Online» System provided by the Bank for registration in " ATF Online" System and subsequent access to E-Banking through "ATF Online" System;

10) **Information bank services** are the services of the Bank maintaining the bank account upon providing the information to the Client or third party by order and with the Client's consent on the balances and (movement) of money on the bank account, on payments and(or) transfers of funds made on the account and other information on request of the Client or under the Agreement;

11) **Client** is referred to the following clients of the Bank:

a) legal entities (their branches and representative offices);

b) individual entrepreneurs and individuals engaged in private practice (private notaries, PEO, lawyers who are residents of the Republic of Kazakhstan, professional mediator);

c) foreign diplomatic and consular missions;

d) liquidation commissions of accumulative pension funds, banks, insurance (reinsurance) entities;

12) **Key device** is an electronic device (USB token) used by the User/Authorized person of the Client to store the primary initialization registration certificate/ registration certificate, primary initialization keys/private (secret) and public keys and performing cryptographic operations using cryptographic information protection facilities;

13) **Primary initialization keys** are the cryptographic keys (private (secret) and open(public) key) used by the Client to start working with ATF Online System intended for replacement by cryptographic keys (open (public) and private (secret) key) EDS by means of ATF Online System;

14) **Contact details are** the contact numbers and addresses of the Bank for referring on the issues related to E-banking specified in Article 7 of the Rules;

15) **Account manager** is an employee of the Branch/CC of the Bank (Account manager, Senior account manager, Universal service manager, Leading/Chief specialist), whose duties include entering into and supporting the Agreement, as well as entering the data of the User/Authorized person of the Client into "ATF Online" System according to the application for access;

15-1) **Head of Business Service Center/Banking Service Outlet/Manager of Corporate Center** – head of Business Service Centre/ Banking service outlet of Branches/ Manager of Corporate Business center, whose functional responsibilities include signing the Acceptance Certificate of the User Name (login) and the Password for entering ATF Online System, token with the Registration Certificate of primary Initialization and primary token / OTP-token;

16) **Open (public) key** is a sequence of electronic digital characters available to any person and designed to confirm authenticity of the digital signature in the e-document;

17) **Password for logging in ATF Online System** is a secret word and/or set of characters intended to confirm the identity or authority of the User/Authorized person of the Client at the entrance to the ATF Online" System;

18) **Key device password** is a secret word and/or a set of symbols intended for access of the User/Authorized person of the Client to the primary initialization registration certificate/registration certificate, primary initialization keys / private(secret) and open (public) keys, and known to the Client;

19) **User** is the person indicated by the Client in the application for access who, in accordance with the Agreement, is granted the right of access to the "ATF Online" System and possibility of taking the necessary actions for the Client to receive Information banking services and other services, with the exception of e-payment services ;

20) **Representative of the Client** is the person authorized by the Client to receive from the Bank all necessary information, devices and documents for proper use of «ATF Online» System by the Client, as well as perform other actions for obtaining services under the Agreement and the Rules;

21) **Security procedure upon connection to ATF Online System** is a set of organizational measures and software and hardware to protect information intended for Identification, Authentication in the compilation, transfer and receipt of e-documents for establishing the rights to receive e-payment services and detect errors and (or) changes in the content of transmitted and received e-documents;

21-1) **ICD employee** – employee of Operational control unit/section of Internal Control Department, whose functional responsibilities include recording of the Registration Certificate of primary initialization and primary tokens to the key device of the User / Authorized Person of the Client;

22) **Business days are** the days that are not weekend or holiday, in accordance with the legislation of the Republic of Kazakhstan;

23) **Registration certificate** is an electronic document issued by the Certifying Center to confirm the compliance of the public key with the private(secret) key and the requirements established by the legislation of the Republic of Kazakhstan on e- document and electronic digital signature;

24) **Primary initialization registration certificate** is an electronic document sent by the Bank to the User/Authorized person of the Client to start working with "ATF Online" System, intended to receive the registration certificate at the Certification Center through " ATF Online" System;

25) **Savings account** is a bank account opened by the Bank in any currency to the Client on the basis of bank deposit agreement for rendering the services provided for by the legislation of the Republic of Kazakhstan and the aforesaid contract;

26) **ATF Online System** is a software, protected E-banking web-service for the Clients. Access to ATF Online System is done via: https://www.atfonline.kz;

27) **Electronic digital signature means** is related to the combination of software and hardware used to create and verify the authenticity of EDS;

28) **E-payment services (transactional services)** are the electronic banking services related to execution of payments and (or) money transfers, exchange transactions with foreign currency using the bank account and other types of banking operations not related to Information banking services;

29) **Current account** is a bank account in any currency opened by the Bank to the Client on the basis of bank account agreement for services provided for by the legislation of the Republic of Kazakhstan and the aforesaid agreement;

30) **Certification center** is related to "Kazakhstan Interbank Settlement Center" RSE , which is a legal entity that certifies that open (public) key corresponds to private (secret) key, and also confirms authenticity and non-recognition of the registration certificate;

31) **Authorized person of the Client** is the person indicated in the document with samples of signatures and seal imprint (if any) of the Client provided to the Bank in accordance with the legislation of the Republic of Kazakhstan when opening a bank account that has the right to sign and forward e-documents to the Bank on behalf of the Client. Also, the Authorized person, in accordance with the agreement, is granted the right of access to "ATF Online" System and an option of implementing necessary actions for E-banking by the Client;

32) **Corporate center (CC)** is a center of corporate business of the Bank, part of Corporate department and Private Banking of the Central region;

33) **E-banking** are the services related to Clients' access of own bank accounts via ATF Online System for e-payment sercvices and information bank services;

34) **E-document** is a document in which the information is presented in electronic digital form and certified by identification means compiled by the sender and not containing distortions and (or) changes made to it after compiling, in the manner prescribed by the legislation of the Republic of Kazakhstan;

35) **Electronic digital signature/EDS** is a set of electronic digital symbols created by means of electronic digital signature and confirming the authenticity of e-document, its ownership and consistency of content. EDS allows identifying the author of the e-document and/or authentication tool, through which it was transmitted and confirmed that the e-document has not been changed since it was signed;

36) **OTP-token** is a device for generating session codes, provided only for the authorized person of the Client;

37) **TLS** is a standard protocol designed to create secure web connections in the Internet or intranets. Allows authentication of servers and servers in turn can check authentication of Cients (if necessary). This protocol also provides a secure channel by encrypting the transmitted data. The TLS protocol is the latest version of SSL protocol.

Article 2. General terms

2. The Rules are developed in accordance with the legislation of the Republic of Kazakhstan, the Charter and CND of the Bank and provide for the procedure and conditions for E-banking to the Clients via ATF Online System.

Chapter 2. E-banking

Article 3. List of electronic banking services

3. The Bank provides electronic banking services to the Client pusuant to the procedure and conditions specified by the Agreement and the Rules.

4. E-banking include:

1) Information bank services:

a) granting access to the Client's bank accounts connected to "ATF Online" System in accordance with the application for access (including providing information on balances and money flow on the Client’s bank accounts, viewing information the bank deposits opened in "ATF Online" System);

b) setup of the list of payments recipients, including introduction of necessary amendments;

c) creation of the templates for homogeneous payments and transfers in the future;

2) E-payment services:

a) sending e-documents to the Bank for making payments and transfers from the current accounts;

b) sending e-documents to the Bank for purchasing and selling foreign exchange;

c) sending e-documents to the Bank for opening and top up of the deposits;

d) sending e-documents to the Bank in other cases.

5. The list of transactions specified in p.4 of the Rules is not exhaustive and may be supplemented by the Bank at its own discretion. Notification of changes in the list of operations offered by the Bank in "ATF Online" System is made by posting relevant information on the Bank's website and/or "ATF Online" System.

Article 4. Procedures and terms of E-banking

6. Access to the User/Authorized person of the Client to E-banking is provided remotely via "ATF Online" System under secure Internet communication channels in accordance with the Security procedure upon connection to "ATF Online" System.

7. Access to the User/Authorized person of the Client to E-banking is possible only after conclusion of the Agreement, acceptance of the application for access by the Bank and registration of one of the Users/Authorized persons of the Client, specified in the application for access, in “ATF

Online” System. At the same time, granting e-payment services is provided only if Authorized person(s) of the Client have necessary and sufficient rights to provide e- documents to the Bank in "ATF Online" System. The right to receive information banking services is determined by the application for access.

8. Granting information bank services is carried out under the condition of Identification in accordance with the Security procedure upon connection to "ATF Online" System.

9. Granting e-payment services is carried out under the condition of Identification abd authentication in accordance with the Security procedure upon connection to "ATF Online" System.

10. For working in “ATF Online” System User/Authorized person fo the Client shall independently ensure availability of the following software and hardware:

1) PC must meet the following minimum system requirements: processor - Celeron 800 MHz, RAM - from 512 MB, hard disk with free capacity of at least 300 MB for installation of "ATF Online" system and 500 MB for stable operation;

2) OS: Windows 7, Windows 8, 2003 R2 x 64, 2008 x 86, 2008 R2, 2012, 2012 R2;

3) Browser: Microsoft Internet Explorer 9.0 or newer versions, Mozilla Firefox – updated version, Google Chrome – updated version, Opera– updated version;

4) Internet access: 33,6 Kb/s and higher;

5) if the proxy server is used, port 443 must be opened for access;

6) presence of connected network or local printer;

7) availability of anti-virus software with updated databases;

8) availability of free USB-port version 2.0 and higher;

9) Java application interpreter - Oracle Java Runtime Environment (JRE) 1.7_51 and higher;

10) TUMAR CSP (Tumar installation under the administrator’s profile, further work – withour administrator’s rights) 5.2;

11) Software for documents: Adobe Acrobat Reader 9.0 и выше, OpenOffice.org Writer 3.0 и выше, Microsoft Word, 2007, 2010, 2013, Office 365, Office:Mac 2011, Microsoft Excel, 2007, 2010, 2013, Office 365, Office:Mac 2011.

11. Connection of the Client to "ATF Online" System is the registration of the User/Authorized person of the Client in accordance with the application for access.

12. Procedire of Identification upon connection to "ATF Online" System:

1) Identification in "ATF Online" System is carried out via the Internet. At the same time, User/Authorized person fo the Client must comply with the Security procedure upon connection to "ATF Online" System, set by the Rules;

2) For logging in "ATF Online" System, Client shall do the following:

a) To receive the key device with primary initialization registration certificate and primary initialization keys from the Head of BSC/BSC/CC/ICD employee;

b) To sign and receive acceptance act for the key device with primary initialization registration certificate and primary initialization keys from the Head of BSC/BSC/CC, compiled in the form specified in Appendix No 2 hereto;

c) To familiarize with the Rules of operation of the key device specified in Appendix 4 hereto;

d) After receipt of the key device in the Bank, User/Authorized person of the Client shall independently change the password of the key device (installed by the manufacturer of the key device) to a new password. The modified password of the key device will be used by the User/Authorized person of the Client in "ATF Online" System for Identification and/or Authentication;

3) In case of loss/ breakdown of the key device, the Client is entitled to receive a new key device by contacting the Bank with the application for access. The application for access must be signed by the CEO of the Client or the Client's representative, sealed by the Client's (if seal is available) and transferred to the Bank in hard copy;

4) The Client may receive new key device with primary initialization registration certificate and primary initialization keys issued in the name of the User/Authorized person of the Client after signing the transfer and acceptance act of the key device with the primary primary initialization registration certificate and the primary initialization keys, compiled in accordance with Appendix 2 hereto and transfer and acceptance act of the User name(login) and the password for logging in "ATF Online" System, compiled according to the form specified in Appendix No 3 hereto. Upon receipt of new key device, previously issued registration certificates and primary initialization keys are cancelled by the Bank without the participation of the User/Authorized person of the Client. The

User/Authorized person of the Client may receive the new key device itself with the primary initialization registration certificate and the primary initialization keys issued in its name. In this case, new primary initialization registration certificate and primary initialization keys are issued. Also, the Client's representative, CEO of the Client may receive new key device with primary initialization registration certificate and primary initialization keys issued in the name of the User/Authorized person of the Client;

5) The Username(login) and the password for logging in "ATF Online" System are generated by the Bank independently without the participation of the User/Authorized person of the Client. Change of the password for logging in "ATF Online" System is performed by the User/Authorized person of the Client independently upon the first login and in the future User/Authorized person of the Client shall change the login password once every 30 (thirty) calendar days;

6) in case of loss of the username(login) and/or password for logging in to "ATF Online" System, User/Authorized person of the Client has the right to receive new username (login) and/or login password in " ATF Online" System on the basis of written application to the Bank, signed by the CEO of the Client or the Client's representative, and sealed by the Client (if seal is available). Receipt of new username (login) and password for logging in to "ATF Online" System is carried out by the User/Authorized person of the Client or the Client's representative or the Client's CEO in the Bank under the transfer and acceptance certificate of the key device with the primary initialization registration certificate, compiled in accordance with the Appendix No 2 hereto and the transfer and acceptance certificate of the username(login) and the password for logging in to "ATF Online" System, compiled in accordance with Appendix No 3 hereto;

7) User/Authorized Person of the Client enters "ATF Online" System by means of appropriate web address by connecting the key device to the USB port of PC, entering the username/Authorized person of the Client username(login), the password for entering the System and password of the key device. If the username (login) and/or password are incorrectly entered to "ATF Online" System for more than 5 (five) times in a row, entry to "ATF Online" System is blocked.
If the password of the key device is incorrectly entered for more than 5 (five) times in a row, the key device is blocked, and if there is an OTP token and an incorrect entry of the session code 5 (five) times in a row, the OTP token is blocked. In case of blocking an account or a key device/OTP-token, Authorized person of the Client must contact the Bank's Branch. The account can not be unlocked by phone call;

8) Validity period of primary initialization keys and primary initialization registration vertificate is 30 (thirty) calendar days from the date of issue, without the option to sign documents. If User/Authorized person of the Client does not pass the procedure of re-issue of primary initialization keys and primary initialization registration vertificate within 30 calendar (thirty) days, the validity period of the primary initialization keys and the registration certificate expires and access to "ATF Online" System will not be possible. In this case, the User/Authorized person of the Client must apply to the Bank for obtaining a new set of primary initialization keys and primary initialization registration certificate on the basis of a new application for access

9) For complying with the Security procedure upon connection to "ATF Online" System, after the receipt of the key device, the User/Authorized person of the Client is obliged to re-issue the primary initialization registration certificate and primary initialization keys to the Annual кegistration certificate and keys open(public) and private(secret) keys) through "ATF Online" System. The validity period of the annual keys (open (public) and private (secret) keys and registration certificate, with the exception of the primary initialization keys) is 1 (one) year from the date of issue. The User/Authorized Pperson of the Client is obliged, upon receipt of the notification in "ATF Online" System, but no later than 30 (thirty) calendar days prior to the expiration of the keys (open(public) and private (secret) keys) and the registration certificate, send the electronic request via "ATF Online" System to Certification authority for the generation of new set of keys (open(public) and private(secret) keys) and the issue of the registration certificate to them. If the User/Authorized person of the Client does not pass the procedure of re-issue of keys (open(public) and private(secret) keys) and the registration certificate within the specified period, the validity of the keys (open(public) and private(secret) keys) and the registration certificate will expire and access to "ATF Online" System will not be possible. The Client will need to apply to the Bank for receiving new set of primary initialization keys and primary initialization registration certificate on the basis of the application on

access, signed by the CEO or Representative of the Client and sealed by the Client (if there is a seal available);

10) Bank accounts of the Client are connected to ATF Online System for receiving/excluding E-banking on the basis of the application for access and/or letter, presented by the Client to the Bank, signed by the CEO or Representative of the Client and sealed by the Client (if seal is available).

13. Procedure and terms of rendering information bank services via “ATF Online” System:

1) Information bank services are rendered subject to Client’s User/Authorized person Identification;

2) After receiving the access to ATF Online System, User/Authorized person of the Client is entitled to individual receipt of information bank services via ATF Online System.

14. Procedure and terms of rendering e-payment services via “ATF Online” System:

1) E-payment services are rendered subject to Identification and Authentication;

2) for establishing the authenticity and correctness of compilation of e-documents, authentication is performed by connecting the key device to the USB port of the PC and entering the username(login) and the key device password;

3) E-payment services are provided on e-documents of the Client's Authorized person provided they are accepted for execution by the Bank. When receiving e-payment services, the Authorized persons of the Client use the forms of e-documents available in "ATF Online" System;

4) E-documents are signed only by the Authorized person of the Client. In cases where e-documents are to be signed by several Authorized persons of the Client who have the right to sign, e-documents are deemed to be duly provided to the Bank only after they have been signed by the respective Authorized persons of the Client in accordance with the instructions of the Client and the requirements of the legislation of the Republic of Kazakhstan.

If the Client specifies in the application for access that the e-documents should be additionally approved by affixing "signature" (authorized) by third party (User/Authorized person of the Client), then e-documents are deemed to be properly provided to the Bank only after their approval by such persons. At the same time, the Bank reserves the right to refuse to execute e-documents that have not been additionally approved by a third party (User/Authorized person of the Client);

5) The Client fills e-documents in ATF Online System in accordance with the legislation of the Republic of Kazakhstan and also taking into account the terms and conditions contained in the ATF Online instruction, posted on the Bank's website, with all liability, including possible damage caused for improper execution of e-documents, is assigned to the Client;

6) Payments and transfers via ATF Online System are done only from the current acounts of the Client;

7) Payments and transfers in foreign exchange via "ATF Online" System are carried out in compliance with the legislation of the Republic of Kazakhstan on currency regulation and foreign exchange control, at the exchange rate established in the Bank;

8) Actions on e-documents are executred by the Bank in accordance with the legislation of the Republic of Kazakhsta, Rules, Agreement and/or relevant Agreement, governing the relations between the Bank and the Client in part of bank account transactions;

9) The Bank refuses to accept e-documents for execution, in the cases provided for by the legislation of the Republic of Kazakhstan, by the Agreement and/or the relevant agreement, governing the relations between the Bank and the Client in part of bank account transactions;

10) After sending the e-document to the Bank via "ATF Online" System, the status of the sent e-document is displayed (sent to the Bank, accepted, denied by the Bank, etc.);

11) Bank's operational day is established by the Bank and changed unilaterally by the Bank. Information on the Bank's operational day is posted on the Bank's website and/or in the Bank's Branches.

Article 5. Suspension/renewal and termination of E-banking

15. The Bank shall block access (suspends E-banking) to the User/Authorized person of the Client in the "ATF Online" System in case of written request from the User/Authorized person of the Client to the Bank or by contacting the Bank with further submission of written application.

16. Blocking of access to the User/Authorized person of the Client to "ATF Online" System is carried out by the Bank during the business days within 15 (fifteen) minutes from the moment of application of the User/Authorized person of the Client and its Identification. If User/Authorized person of the Client applies during non-working hours of the Bank, blocking of access to the " ATF Online" System takes place on the first business day after the weekend within 15 (fifteen) minutes after the start of the business day. Identification for the specified purposes is carried out according to the following parameters of the the User/Authorized person of the Client: Client's business identification number (BIN), Client's name, surname, first name, patronymic (if available) of the User/Authorized person of the Client, number and validity period of the identity document of the User/Authorized person of the Client). The procedure and conditions for suspension/renewal/termination of E-banking are established by the Agreement.

Article 6. Securities procedure upon connection to "ATF Online" System

17. For ensuring confidentiality of transmitted and received information in "ATF Online" System, 128/256 bit TLS encryption (Transport Layer Security - Secure Sockets Layer or Secure Connection Protocol) is used. Encryption converts the Client's data in "ATF Online" System into an encrypted code before sending it through the Internet and ensures confidentiality of the Client's information on the way between the Bank's computer system and Internet browser of the Client.

18. In case of Identification and Authentication in "ATF Online" System on the Bank's website, the Client's Internet browser requests confirmation of the Bank's Website with its identification information through digital certificates. The Internet Browser of the Client shall verify the digital certificate and notify the Client if this Website does not belong to the Bank. In the course of Identification, the Client must ensure that the verification of the digital certificate by the Internet browser has been successful.

19. For identification purposes, when accessing "ATF Online" System, the following identifying information is provided when logging in to ""ATF Online" System: Username (login), password for logging in to "ATF Online" System, connection of the key device to the USB port of the personal computer and entering the key device password belonging to this User/Authorized person of the Client.

20. For Authentication process when the Client receives e-payment services, it is mandatory to connect the key device (use of the private(secret) key) to the USB port of the Personal Computer of the Client's Authorized person and to enter the key device password.

21. The User/Authorized person of the Client has no right to disclose/transfer to a third party the username (login), password for entering "ATF Online" System, OTP Token /session code, the key device password, the key device. To store the username (login), the password for entering "ATF Online" System, password of the key device, key device, OTP token in conditions that exclude unauthorized persons from accessing them.

22. For security purposes, "ATF Online" System provides for the automatic disconnection of the current session of the Client in "ATF Online" System. Under automatic disconnection of the current session of the Client, "ATF Online" System means the refusal to provide E-Banking in the event of prolonged (more than 10 consecutive minutes) absence of active Client actions in "ATF Online" System (failure to perform any operations and actions, etc.) . At the same time, it is prohibited to leave personal computer with an open session in the absence of the User/Authorized person of the Client.

23. For confirming the data specified in the application for access, Bank has the right to receive/clarify necessary information through telephone communication related to execution of the Client's application for access.

24. For protecting against third-party access to "ATF Online" System and the key device, "ATF Online" System login password and the key device password must satisfy the following minimum requirements:

1) cannot contain the username (login) or any part of it;
2) must consist of at least 8 (eight) characters;
3) must contain symbols of three categories from among the following four:
a) capital letters of the English alphabet from A to Z;
b) lowercase letters of the English alphabet from a to z;

c) decimal digits (from 0 to 9);
d) non-alphabetic characters (for example,!, $, #,%).

Chapter 3. Final clauses

Article 7. Contact details of the Bank

25. Client may refer to the following contact details on the matters related to E-banking: telephones 8-8000-800-283 (Kazakhstan toll-free number), +7 (727) 258-30-00 and +7 (727) 258 30 38 in Almaty.

26. Legal address of the Bank: 36, Al-Farabi ave., A25D5F7, Medeuskiy district, Almaty. Addresses of the Bank’s Branches can be found on the Bank’s website.

27. The Bank has the right to unilaterally amend the contact details, specified in p.25 hereto with Client notification thereon on the Bank's website.

Article 8. Final clauses

28. The Bank has the right to unilaterally amend the Rules and post it on the Bank's website within 5 (five) business days before the effective date.

29. Other issues not regulated by the Rules are resolved in accordance with the legislation of the Republic of Kazakhstan, CND of the Bank, the Agreement and customs of business turnover adopted in the banking practice.

Appendix No 1
to the Rules on E-banking via ATF Online in ATFBank JSC

Form

Application for access to ATF Online System

ATFBank JSC (further- Bank) is hereby requested to accept this application for access to ATF Online System (further- Application) under the below terms:

1. Client information:

(i) to specify the name for legal entities:	
(ii) to specify full name and entity(if available) for IE/notary/legal counsellor/PEO/professional mediator:	
Legal address:	
BIN/INN:	
Telephone/Fax:	
Contact person:	
Mobile number of the contact person:	
Email address:	

2. Information on the CEO of the Client:

Position name:	
Full name:	
IIN:	
Identity document (ID/passport/resident permit/etc.), issuing authority:	
Signature rights:	
Telephone (landline and mobile):	
Email address:	
Acting on the basis:	

3. Information on Users/Authorized persons of the Client to be connected:

3.1. Authorized person:

Full name:	
IIN:	
Identity document (ID/passport/resident permit/etc.),	

issuing authority:		
Position:		
Nationality:		
Telephone (landline and mobile):		
Email address:		
Specify if Authorized person of the Client is registered in ATF Online System and holds key device as a User/Authorized person of other Client of the Bank or is a Client of the Bank, who uses E-banking via ATF Online System:	Yes: □ Specify the name/Full name and BIN/IIN of such Client of the Bank: Name/Full name:_____ BIN/IIN:_____	No: □
Below line is filled in if necessary:		
Client wishes to use primary initialization registration certificate, primary initialization keys, registration certificate, private(secret) and open(public) keys, which were issued for the other Client of the Bank, where Authorized person of the Client is a User/Authorized person of the other Client of the Bank. Specify the name/Full name and BIN/IIN of such other Client of the Bank: _____, _____. _____/_____ *signature* *Full name* stamp		

To select:
□ registration of the Authorized person of the Client in ATF Online System and issue of the key device;
□ registration of the Authorized person of the Client in ATF Online System and issue of the key device and OTP-token;
□ second manufacture of primary initialization keys and primary initialization registration certificate (specify the reason) _____;
□ second issue of OTP-token (specify the reason) _____;
□ to delete using OTP-token for Authorized person of the Client;
□ to delete Authorized person of the Client from ATF Online System.

Note: Signature right of the Authorized person of the Client in ATF Online System is specified in accordance with signature and stamp samples of the Client, presented to the Bank.

3.2. User:

Full name:	
IIN:	

Identity document (ID/passport/resident permit/etc.), issuing authority:		
Position:		
Nationality:		
Telephone (landline and mobile):		
Email address:		
Specify if User is registered in ATF Online System and holds key device as a User/Authorized person of other Client of the Bank or is a Client of the Bank, who uses E-banking via ATF Online System:	Yes: □ Specify the name/Full name and BIN/IIN of such Client of the Bank: Name/Full name:_____ BIN/IIN:_____	No: □
Below line is filled in if necessary:		
Client wishes to use primary initialization registration certificate, primary initialization keys, registration certificate, private(secret) and open(public) keys, which were issued for the other Client of the Bank, where Authorized person of the Client is a User/Authorized person of the other Client of the Bank. Specify the name/Full name and BIN/IIN of such other Client of the Bank: _____, _____. _____/_____ *signature* *Full name* stamp		

To select:
□ registration of the User in ATF Online System and issue of the key device;
□ second manufacture of primary initialization keys and primary initialization registration certificate (specify the reason) _____;
□ to delete the User from ATF Online System.

If User is already registered in the System and holds key device as User/Authorized person of the other Client of the Bank or is a Client of the Bank, who uses E-banking, specify the name and BIN/IIN of such other Client of the Bank: _____
_____.

3.3. Bank accounts to be connected to ATF Online System:

Bank accounts of the Client	Numbers of the bank accounts of the Client

Current:	
Savings:	

3.4. Limits for funds disposal in ATF Online System:

Table № 1:

№	Current account number	Maximum amount per one payment/transfer	Maximum amount of payments/transfers per day
1.			
2.			
3.			

Table № 2:

№	Current account number	Full name of the person (User/Authorized person), who will sign the relevant documents for payments /transfers of the Client:	Amount of one payment /transfer, excess of which requires signing the payment document of the Client:	Total amount of payments /transfers per day, excess of which requires signing the payment document of the Client:
1.				
2.				
3.				

3.5. Information on access rights:

№	Full name of the User of the Client	Bank account number	☑ receipt of statements	☑ Creation of the templates of payment documents, except for templates specified further	☑ Creation of the templates of documents for exchange transactions	☑ Receipt and sending of the letters to the Bank	☑ Review of incoming payments / transfers	☑ Creation of the templates of documents for transactions on payment of the salaries to employees	☑ Creation of the templates of documents for opening and(or) top up of the deposits*
1.									
2.									
3.									

* Only the savings accounts on deposits, opened in ATF Online System are reflected.

№	Full name of the Authorized person of the Client	Bank account number	☑ receipt of statements	☑ Creation of the templates of payment documents, except for templates specified further and submission of payment documents to the Bank	☑ Creation of the templates of documents for exchange transactions and submission of such payment documents to the Bank	☑ Receipt and sending of the letters to the Bank	☑ Review of all incoming payments / transfers	☑ Creation of the templates of documents for transactions on payment of the salaries to employees and submission of such payment documents to the Bank	☑ Creation of the templates of documents for opening and(or) top up of the deposits* and submission of such documents to the Bank
1.									
2.									
3.									

* Only the savings accounts on deposits, opened in ATF Online System are reflected.

4. Hereby Client certifies the Bank that:

(i) holds necessary powers to indicate in the application information about individuals specified in it and transfer of such information to the Bank will not violate the rights of such persons;

(ii) the individuals indicated in the application as Users/Authorized persons agree that registration certificate and EDS private key of the Certification Authority for work in "ATF Online" System will be provided (issued) and presented under their names.

In the event that these assurances are void (not valid), which entailed negative consequences for the Bank, including but not limited to: claims of the said persons for whom information was provided by the Client, involvement of the Bank in litigations, compensation to the said persons for damage and other proven and reasonable amounts, the Client undertakes to reimburse the amounts due (or paid) to such persons by the Bank.

5. This section shall be filled if the application is signed by the CEO of the Client, possessing the right to sign/issue PoA on behalf of the Client:

Hereby, _____ _____ (name and BIN/IIN of the Client), represented by _____ (full name, position of CEO) authorizes _____ (full name and IIN) of the Representative of the Client to perform the following actions on behalf of _____ _____ (name and BIN/IIN of the Client):

to receive from the Bank: (i) username (login), (ii) password for logging in ATF Online System and (iii) key device and perform all necessary actions related to the order, including signing the delivery and acceptance certificate.

Client (signature): _____

Full name of Client's signatory:_____

stamp (if available)

Date:_____

NOTES of the Bank on acceptance of the application:

Full name of the Bank's employee: _____

Signature of the Bank's employee: _____

Stamp of the Bank's employee

Date:_____

Appendix No 2
to the Rules on E-banking via ATF Online in ATFBank JSC

Form

Delivery and acceptance certificate
for key device with primary initialization registration certificate and primary initialization keys/OTP-token

_____ **_____ 20__**

ATFBank JSC, hereinafter referred to as the **Bank**, represented by Mr/Ms _____ *(position and full name)*, and

Client- legal entity:

[_____ «_____» *(form of entity and name of the Client)*, hereinafter referred to as **Client,** represented by Mr(Ms) _____*(position (if available) and full name(in full))*, acting on the basis of _____ *(specify)*,]

Client - individual:

[_____ *(full name and title (if available))*, hereinafter referred to as **Client**,]

hereinafter jointly referred to as **Parties**, signed this delivery and acceptance certificate as below:

The Bank transmits and the Client receives key device with the primary initialization registration certificate and the primary initialization keys (open(public) and private(secret) keys) for each User/Authorized person of the Client (each key device has primary initialization registration certificate and primary initialization keys (open(public) and private(secret) keys) and/or OTP token according to the table below:

Full name of the User/Authorized person of the Client	**Serial number of the device/OTP-token:**	**Number of primary initialization registration certificate on the key device:**
1.		
2.		
3.		
4.		

Signatories of the Parties:	
Bank:	**Client:**
Transferred: Full name of the employee: _____ Position: _____ Branch of ATFBank JSC: _____ Signature: _____ *(stamp)*	Accepted: Full name of the Client: _____ Position: _____ Entity: _____ BIN/IIN: _____ Position: _____ Stamp (if available)

Appendix No 3
to the Rules on E-banking via ATF Online in ATFBank JSC

Form

Delivery and acceptance certificate
for username (login) and password for logging in ATF Online System

_____ **_____ 20__**

ATFBank JSC, hereinafter referred to as the **Bank**, represented by Mr/Ms _____ *(position and full name)*, and
Client- legal entity:
[_____ «_____» *(form of entity and name of the Client)*, hereinafter referred to as **Client,** represented by Mr(Ms) _____*(position (if available) and full name(in full))*, acting on the basis of _____ *(specify)*,]
Client - individual:
[_____ *(full name and title (if available))*, hereinafter referred to as **Client**,]
hereinafter jointly referred to as **Parties**, signed this delivery and acceptance certificate as below:
The Bank transmits and the Client receives username(login) and password for logging in ATF Online System for each User/Authorized person of the Client:

Full name of the User/Authorized person of the Client	**Comments:**
1.	
2.	
3.	
4.	

Signatories of the Parties:	
Bank:	**Client:**
Transferred: Full name of the employee: _____ Position: _____ Branch of ATFBank JSC: _____ Signature: _____ *(stamp)*	Accepted: Full name of the Client: _____ Position: _____ Entity: _____ BIN/IIN: _____ Position: _____ Stamp (if available)

Appendix No 4
to the Rules on E-banking via ATF Online in ATFBank JSC

Operating procedures of the key device and OTP-token

1. The key device stores registration certificates and private (secret)/ open (public) keys. In this regard, it is necessary to store the key device in places that exclude access to the key device of unauthorized persons. If there is a suspicion of discredit, it is necessary to notify the Bank immediately to block access to "ATF Online" System.
2. Access to the key device of the User / Authorized person of the Client shall be available only to those for whom they were issued, as well as to the Client's Representative only for the purpose of their receipt and transfer to the User/Authorized person of the Client. No one else, including the Bank's employees, SHOULD HAVE ACCESS to the key device.
3. The key device should be connected to the personal computer only for the duration of operations in "ATF Online" System. To work with key device, it is necessary to connect it to the working USB port of the personal computer.
4. When the key device is first connected to the personal computer, the Authorized person of the Client/User is obliged to change the password of the key device to a new one. The key device's password is changed through the Tumar CSP cryptographic protection facility. To change the key device password, go to: Start-Programs-GammaTech-TumarCSP-TumarConfiguration. At the top of the Tumar CSP Configurator window, locate the JavaToken profile, right-click on it and select "Change Password on container". According to the security policy, the password of the key device must contain more than 8 (eight) characters. Enter the current password of the key device, then the new password of the key device and confirm the new password of the key device. Click OK. The password of the key device has been changed successfully. After exiting ATF Online System, it is necessary to disconnect the key device from the personal computer.
5. Check that the connection is established with the server of the Bank.
6. If you received an email with an unknown attachment or a link to an unknown resource, delete this message without opening the attachment and activating the link.
7. In the event that the personal computer from which payment is sent or processed in ATF Online System unexpectedly ceases to run or issues incomprehensible messages, it is recommended that you immediately contact the Account manager of the Bank and block the account of the User/Authorized person of the Client (apply for suspension of e-payment services).
8. Do not share confidential information with anyone, including the Bank's employees. No employee of the Bank, under any circumstances, has the right to require you to know the password of the key device. If the Client employee who is the User/Authorized person of the Client who has access to "ATF Online" System is dismissed, it is necessary to contact the Account manager in the Bank and block access to the appropriate User/ Authorized person of the Client for "ATF Online" System.
9. It is strictly forbidden to open the case of OTP-token and/or key device and to expose to different treatment.
10. When logging in "ATF Online" System after entering the username (login) and the password, the window for entering the session code will be displayed. Click on the OTP-token to generate a password. A combination of 6 digits appears in the display and you must enter it.
11. The session code is a 6-digit combination of numbers that the Authorized person of the Client should see.
12. The Password of the key device is a combination of numbers / letters known to the User / Authorized person of the Client, who owns this device. If the password of the key device is randomly known to third parties, it must be changed immediately. For security reasons, the password of the key device must be as complex as possible. It should be remembered (not written down) and not disclosed to third parties. The password of the key device is used when signing e-documents in "ATF Online" System.
13. If all attempts (5 times) to enter the password of the key device are exhausted, the key device is blocked. It is necessary to apply to the Account manager for new registration certificate of primary initialization and primary initialization keys on the basis of new application for access.
14. If the session code is incorrectly entered (5 times), the OTP token is blocked. You need to contact the Account manager for unlocking.
15. In case of loss of OTP-token or key device, immediately contact the Bank’s account manager or contact information for suspending e-banking for the User/Authorized person of the Client.
16. To ensure high level of information protection for Clients using ATF Online System, key JaCarta

devices manufactured by Aladdin RD and OTP tokens are used. JaCarta is a new generation of USB tokens for strong authentication, electronic signature and secure storage of the keys and registration certificates. OTP tokens are 6-digit session codes generation devices.

Short technical characteristics of JaCarta key device

Attribute name	Functionality/Meaning
Application area	Ensuring secure generation and storage of private keys, as well as user certificates provided by the Certification Center of Kazakhstan Interbank Settlement Center RSE of NBK to the users of the remote banking system for legal entities. Providing two-factor authentication and electronic digital signature.
Supported algorithms and standards	Encryption algorithm: • ГОСТ 34.310-2004 • ГОСТ 34.311-95 • ГОСТ 28147-89 • X509 V.3
Token shall function under the management of the following OS	For Microsoft Windows XP/Vista/7/8/8.1/2003/2008/2012, 32/64 bit - Linux; -Apple MacOS X;
Token shall	- ensure two-factor authentication; - ensure protection from overuse of PIN code entry; - ensure 2 level access to the token: Guest, User
Certification	Certification of the token for compliance with 2 level of the secutiry CT PK 1073-2007
Volume of protected memory	At least 72 Kb
Amount of re-recording cycles into one cell of EEPROM-memory	At least 500 000
Production capacity	Generation of key information (GOST for signature and GOST for encryption) – no more than 4 seconds. EDS formation – no more than 1 second.
Supported interface and standards	• PKCS#11 • Specification ISO - ISO7816 • CAPI • PC/SC • Certificates storage X.509 v3 • Microsoft CCID • Smartcard Minidriver

Short technical characteristics of OTP-token

Attribute name	Functionality/Meaning
Application area	Autonomous generator of one-time passwords for supplementary authentication upon logging in the system and receipt of e-payment services by the Client..
Supported algorithms and standards	Encryption algorithm: • ГОСТ 34.310-2004 • ГОСТ 34.311-95 • ГОСТ 28147-89 • X509 V.3
Certification	Certification of the token for compliance with national standards of the Republic of Kazakhstan shall be confirmed. Confirming document is a compliance certification

Attribute name	Functionality/Meaning
	corresponding to 3rd evel of the secutiry CT PK 1073-2007
Volume of protected memory	At least 72 Kb
Operating temperature	0˚C - 70˚C
Storage temperature	-40˚C - 85˚C
Storage term of the memory data	At least 10 years
Amount of re-recording cycles into one cell of EEPROM-memory	At least 500 000
Production capacity	Generation of key information (GOST for signature and GOST for encryption) – no more than 4 seconds. EDS formation – no more than 1 second.
Supported interface and standards	• PKCS#11 • Specification ISO - ISO7816 • CAPI • PC/SC • Certificates storage X.509 v3 • Microsoft CCID • Smartcard Minidriver