

1. Правила размещены 25 августа 2018 года. Вступили в силу с 04 сентября 2018 года.



## Правила предоставления электронных банковских услуг посредством системы «ATF Online» в АО «АТФБанк»

Предмет:	настоящие Правила регламентируют порядок и условия предоставления электронных банковских услуг клиентам посредством системы «ATF Online» в АО «АТФБанк»	
Код документа	ПР.7255.113	
Разработчик:	Управление разработки продуктов МСБ	
Субъекты регулирования:	Департамент безопасности Департамент корпоративного бизнеса Департамент корпоративного бизнеса и Private Banking Центрального региона Департамент малого и среднего бизнеса Департамент развития цифровых технологий	
Согласованы с:	Департаментом безопасности Департаментом корпоративного бизнеса и Private Banking Центрального региона Департаментом комплаенс-контроля Департаментом развития цифровых технологий Департаментом стратегических рисков Департаментом HR Управлением поддержки бизнес процессов Управлением развития и поддержки КБ Управлением разработки продуктов МСБ Юридическим департаментом	
Утверждены:	Правлением АО «АТФБанк» (протокол № 76)	09 августа 2018 года
Следующее обновление:	по истечении 1 (одного) года с момента вступления в силу	
Внесенные изменения:	нет	
Отмененные документы:	Правила предоставления Электронных банковских услуг посредством системы «АТФ Online» в АО «АТФБанк»	Утверждены Правлением АО «АТФБанк» (протокол № 34 от 24 июня 2015 года)

## Оглавление

<b>Глава 1.</b>	<b>Общие положения</b>	<b>3</b>
Статья 1.	Основные понятия	3
Статья 2.	Общие положения	5
<b>Глава 2.</b>	<b>Предоставление Электронных банковских услуг</b>	<b>5</b>
Статья 3.	Перечень Электронных банковских услуг	5
Статья 4.	Порядок, способ и условия предоставления Электронных банковских услуг	6
Статья 5.	Приостановление/возобновление и прекращение предоставления Электронных банковских услуг	10
Статья 6.	Процедуры безопасности при подключении к Системе «ATF Online»	10
<b>Глава 3.</b>	<b>Заключительные положения</b>	<b>11</b>
Статья 7.	Контактные данные Банка	11
Статья 8.	Заключительные положения	11
Приложение 1.	Заявка на предоставление доступа в Системе «ATF Online»	12
Приложение 2.	Акт приема-передачи Ключевого устройства с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации/ОТР-токена	19
Приложение 3.	Акт приема-передачи Имени пользователя (логина) и Пароля для входа в Систему «ATF Online»	21
Приложение 4.	Правила эксплуатации Ключевого устройства и ОТР-токена	23

## Глава 1. Общие положения

### Статья 1. Основные понятия

1. В настоящих Правилах предоставления электронных банковских услуг посредством Системы «ATF Online» в АО «АТФБанк» (далее – Правила) используются следующие понятия и сокращения:

1) **Аутентификация** – подтверждение подлинности и правильности составления Электронного документа в соответствии с требованиями Процедуры безопасности при подключении к Системе «ATF Online»;

2) **Банк** – АО «АТФБанк»;

3) **Банковский счет** – способ отражения и учета движения денег Клиента в Банке, а также договорных отношений между Банком и Клиентом по банковскому обслуживанию Клиента. В рамках Договора к Банковскому счету относится Текущий и/или Сберегательный счет;

4) **Веб-сайт Банка** – <http://www.atfbank.kz>;

5) **Договор** – Договор об оказании электронных банковских услуг посредством Системы «ATF Online», заключенный между Банком и Клиентом;

6) **Закрытый (секретный) ключ** – последовательность электронных цифровых символов, известная Пользователю/Уполномоченному лицу Клиента, и предназначенная для создания ЭЦП с использованием Средств электронной цифровой подписи;

7) **Заявка на доступ** – заявка на предоставление доступа к Системе «ATF Online», оформленная по форме, предусмотренной Приложением 1 к Правилам. Надлежащим образом оформленные Клиентом и принятые Банком Заявки на доступ являются неотъемлемой частью Договора;

8) **Идентификация** – процедура установления подлинности Пользователя/Уполномоченного лица Клиента с целью однозначного подтверждения его прав на получение Электронных банковских услуг;

9) **Имя пользователя (логин)** – уникальное имя Пользователя/Уполномоченного лица Клиента в Системе «ATF Online», предоставляемое Банком в целях регистрации в Системе «ATF Online» и последующего доступа к Электронным банковским услугам через Систему «ATF Online»;

10) **Информационные банковские услуги** – услуги Банка, обслуживающего Банковский счет, по предоставлению Клиенту или третьему лицу по приказу и с согласия Клиента информации об остатках и (движении) денег по его Банковскому счету, о платежах и (или) переводах денег, осуществленных по этому счету, и иной информации по запросу Клиента либо по Договору;

11) **Клиент** – клиенты Банка:

а) юридические лица (их филиалы и представительства);

б) индивидуальные предприниматели и лица, занимающиеся частной практикой (частные нотариусы, частные судебные исполнители, адвокаты, являющиеся резидентами Республики Казахстан, профессиональный медиатор);

в) иностранные дипломатические и консульские представительства;

г) ликвидационные комиссии накопительных пенсионных фондов, банков, страховых (перестраховочных) организаций;

12) **Ключевое устройство** – электронное устройство (USB-токен), используемое Пользователем/Уполномоченным лицом Клиента для хранения Регистрационного свидетельства первичной инициализации/Регистрационного свидетельства, Ключей первичной инициализации/Закрытого (секретного) и Открытого (публичного) ключей и выполнения криптографических операций с использованием средств криптографической защиты информации;

13) **Ключи первичной инициализации** – криптографические ключи (Закрытый (секретный) и Открытый (публичный) ключ), используемые Клиентом для начала работы с Системой «ATF Online», предназначенные для замены на криптографические ключи (Открытый (публичный) и Закрытый (секретный) ключ) ЭЦП посредством Системы «ATF Online»;

14) **Контактные данные** – контактные телефоны и адреса Банка для обращения по вопросам, связанным с предоставлением Электронных банковских услуг, указанные в статье 7 Правил;

15) **Менеджер счета** – работник филиала/ЦКБ Банка (Менеджер счета, Старший менеджер счета, Универсальный сервис менеджер, Ведущий/Главный специалист), в функциональные обязанности которого входит заключение и сопровождение Договора, а также внесение данных Пользователя/Уполномоченного лица Клиента в Систему «ATF Online» согласно Заявке на доступ;

16) **Открытый (публичный) ключ** – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности ЭЦП в Электронном документе;

17) **Пароль для входа в Систему «ATF Online»** – секретное слово и/или набор символов, предназначенный для подтверждения личности или полномочий Пользователя/Уполномоченного лица Клиента при входе в Систему «ATF Online»;

18) **Пароль Ключевого устройства** – секретное слово и/или набор символов, предназначенный для доступа Пользователя/Уполномоченного лица Клиента к Регистрационному свидетельству первичной инициализации/Регистрационному свидетельству, Ключам первичной инициализации/Закрытому (секретному) и Открытому (публичному) ключам, и известный Клиенту;

19) **Пользователь** – лицо, указанное Клиентом в Заявке на доступ, которому, в соответствии с Договором, предоставляется право доступа к Системе «ATF Online», и возможность осуществления необходимых действий для получения Клиентом Информационных банковских услуг, а также иных услуг, за исключением Электронных платежных услуг;

20) **Представитель Клиента** – лицо, уполномоченное Клиентом соответствующей доверенностью получать от Банка все необходимые сведения, устройства и документы для надлежащего использования Системы «ATF Online» Клиентом, а также выполнять иные действия в целях получения услуг в рамках Договора и Правил;

21) **Процедура безопасности при подключении к Системе «ATF Online»** – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для Идентификации, Аутентификации при составлении, передаче и получении Электронных документов с целью установления прав на получение Электронных платежных услуг и обнаружения ошибок и (или) изменений в содержании передаваемых и получаемых Электронных документов;

22) **Рабочие дни** – дни, не являющиеся выходными либо праздничными, в соответствии с законодательством Республики Казахстан;

23) **Регистрационное свидетельство** – электронный документ, выдаваемый Удостоверяющим центром для подтверждения соответствия Открытого (публичного) ключа Закрытому (секретному) ключу и требованиям, установленным законодательством Республики Казахстан об электронном документе и электронной цифровой подписи;

24) **Регистрационное свидетельство первичной инициализации** – электронный документ, передаваемый Банком для Пользователя/Уполномоченного лица Клиента для начала работы с Системой «ATF Online», предназначенный для получения в Удостоверяющем центре Регистрационного свидетельства посредством Системы «ATF Online»;

25) **Сберегательный счет** – банковский счет в любой валюте, открываемый Банком Клиенту на основании договора банковского вклада, для оказания услуг, предусмотренных законодательством Республики Казахстан и указанным договором;

26) **Система «ATF Online»** – программное обеспечение, защищенный веб-сервис для Клиентов позволяющее (-ий) Банку предоставлять Электронные банковские услуги. Доступ к Системе «ATF Online» осуществляется через интернет посредством веб-адреса Системы «ATF Online»: <https://www.atfonline.kz>;

27) **Средства электронной цифровой подписи** – совокупность программных и технических средств, используемых для создания и проверки подлинности ЭЦП;

28) **Электронные платежные услуги (транзакционно-банковские услуги)** – Электронные банковские услуги, связанные с проведением платежей и (или) переводов денег, обменных операций с иностранной валютой с использованием Банковского счета и

осуществлением иных видов банковских операций, не относящихся к Информационным банковским услугам;

29) **Текущий счет** – банковский счет в любой валюте, открываемый Банком Клиенту на основании договора банковского счета, для оказания услуг, предусмотренных законодательством Республики Казахстан и указанным договором;

30) **Удостоверяющий центр** – РГП «Казахстанский центр межбанковских расчетов» – юридическое лицо, удостоверяющее соответствие Открытого (публичного) ключа Закрытому (секретному) ключу, а также подтверждающее достоверность и неотозванность Регистрационного свидетельства;

31) **Уполномоченное лицо Клиента** – лицо, указанное в документе с образцами подписей, предоставляемом Клиентом Банку в соответствии с законодательством Республики Казахстан при открытии Банковского счета, которое вправе подписывать и направлять Электронные документы Банку от имени Клиента. Также Уполномоченному лицу, в соответствии с Договором, предоставляется право доступа к Системе «ATF Online», и возможность осуществления необходимых действий для получения Клиентом Электронных банковских услуг;

32) **ЦКБ** – Центр Корпоративного Бизнеса Банка, входящий в состав Департамента корпоративного бизнеса, Департамента корпоративного бизнеса и Private Banking Центрального региона;

33) **Электронные банковские услуги** – услуги, связанные с доступом Клиента к своему Банковскому счету посредством Системы «ATF Online» для получения Электронных платежных услуг и Информационных банковских услуг;

34) **Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме и удостоверена идентификационными средствами, составленный отправителем и не содержащий искажений и (или) изменений, внесенных в него после составления, в порядке, предусмотренном законодательством Республики Казахстан;

35) **Электронная цифровая подпись/ЭЦП** – набор электронных цифровых символов, созданный Средствами электронной цифровой подписи и подтверждающий достоверность Электронного документа, его принадлежность и неизменность содержания. ЭЦП позволяет установить автора Электронного документа и/или средство Аутентификации, с использованием которого осуществлена его передача и подтверждение, что Электронный документ не был изменен с момента его подписания;

36) **ОТР-токен** – устройство для генерации сеансовых кодов, предоставляемое только для Уполномоченного лица Клиента;

37) **TLS** – стандартный протокол, предназначенный для создания безопасных веб-соединений в сети интернет или интрасетях. Позволяет выполнять проверку подлинности серверов, а серверам – проверку подлинности клиентов (при необходимости). Данный протокол также обеспечивает защищенный канал путем шифрования передаваемых данных. Протокол TLS является последней версией протокола SSL.

## **Статья 2. Общие положения**

2. Правила разработаны в соответствии с законодательством Республики Казахстан, Уставом и корпоративными нормативными документами Банка, и предусматривают порядок и условия предоставления Электронных банковских услуг Клиентам посредством Системы «ATF Online».

## **Глава 2. Предоставление Электронных банковских услуг**

### **Статья 3. Перечень Электронных банковских услуг**

3. Банк оказывает Клиенту Электронные банковские услуги в порядке и на условиях, установленных Договором и Правилами.

4. Электронные банковские услуги включают в себя:

1) Информационные банковские услуги:

а) предоставление доступа к Банковским счетам Клиента, подключенным к Системе «ATF Online» согласно Заявке на доступ (в т.ч. предоставление информации об остатках и

движении денег по Банковским счетам Клиента, просмотр информации по банковским вкладам, открытым в Системе «ATF Online»);

б) настройка списков получателей платежей, включая внесение необходимых изменений;

в) создание шаблонов для осуществления однотипных платежей и переводов в будущем;

2) Электронные платежные услуги:

а) направление Электронных документов Банку для осуществления платежей и переводов с Текущих счетов;

б) направления Электронных документов Банку для осуществления покупки, продажи иностранной валюты;

в) направление Электронных документов Банку для открытия и пополнения банковских вкладов;

г) направление Электронных документов Банку в иных случаях.

5. Перечень операций, указанный в пункте 4 Правил, не является исчерпывающим и может дополняться Банком по своему усмотрению. Уведомление об изменении перечня операций, предлагаемых Банком в Системе «ATF Online», производится путем размещения соответствующей информации на Веб-сайте Банка и/или в Системе «ATF Online».

#### **Статья 4. Порядок, способ и условия предоставления Электронных банковских услуг**

6. Доступ Пользователю/Уполномоченному лицу Клиента к Электронным банковским услугам предоставляется удаленно через Систему «ATF Online» по защищенным каналам связи посредством сети интернет в соответствии с Процедурой безопасности при подключении к Системе «ATF Online».

7. Доступ Пользователю/Уполномоченному лицу Клиента к Электронным банковским услугам возможен только после заключения Договора, принятия Банком Заявки на доступ и прохождения регистрации одного из Пользователей/Уполномоченных лиц Клиента в Системе «ATF Online», указанных в Заявке на доступ. При этом, предоставление Электронных платежных услуг осуществляется только при условии регистрации в Системе «ATF Online» Уполномоченного(-ых) лица (лиц) Клиента, обладающего (-их) необходимыми и достаточными правами для предоставления Электронных документов Банку. Право на получение Информационных банковских услуг определяется Заявкой на доступ.

8. Предоставление Информационных банковских услуг осуществляется при условии Идентификации в соответствии с Процедурой безопасности при подключении к Системе «ATF Online».

9. Предоставление Электронных платежных услуг осуществляется при условии Идентификации и Аутентификации в соответствии с Процедурой безопасности при подключении к Системе «ATF Online».

10. Для работы с Системой «ATF Online» Пользователь/Уполномоченное лицо Клиента должен обеспечить самостоятельно наличие следующих программно-технических средств:

1) персональный компьютер должен соответствовать следующим минимальным системным требованиям: процессор – Celeron 800 МГц, ОЗУ – от 512 Мб, жесткий диск со свободным объемом не менее 300 Мб для установки Системы «ATF Online» и 500 Мб для стабильной работы;

2) операционная система Windows 7, Windows 8, 2003 R2 x 64, 2008 x 86, 2008 R2, 2012, 2012 R2;

3) браузер Microsoft Internet Explorer 9.0 или более новые версии, Mozilla Firefox – актуальная версия, Google Chrome – актуальная версия, Opera – актуальная версия;

4) доступ в сеть интернет на скорости от 33,6 Кб/с и выше;

5) в случае использования прокси-сервера должен быть открыт порт 443 для доступа;

6) наличие подключенного сетевого или локального принтера;

7) наличие антивирусного программного обеспечения с актуальными обновленными базами;

8) наличие свободного USB-порта версии 2.0 и выше;

9) интерпретатор приложений Java - Oracle Java Runtime Environment (JRE) 1.7\_51 и выше;

- 10) ТУМАР CSP (установка Тумар – под учетной записью администратора, дальнейшая работа - без администраторских прав) 5.2;
- 11) программное обеспечение для работы с документацией – 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. Подключение Клиента к Системе «ATF Online» представляет собой регистрацию Пользователя/Уполномоченного лица Клиента согласно Заявке на доступ.
12. Порядок и условия Идентификации при подключении к Системе «ATF Online»:
- 1) Идентификация в Системе «ATF Online» осуществляется посредством сети интернет. При этом Пользователь/Уполномоченное лицо Клиента обязан соблюдать Процедуры безопасности при подключении к Системе «ATF Online», установленные Правилами;
  - 2) для входа в Систему «ATF Online» Клиенту необходимо в Банке осуществить следующие действия:
    - а) получить Ключевое устройство с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации у Начальника ЦОБ/ЦБО/Руководителя ЦКБ;
    - б) подписать и получить Акт приема-передачи Ключевого устройства с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации у Начальника ЦОБ/ЦБО/Руководителя ЦКБ, составленного по форме согласно Приложению 2 к Правилам;
    - в) ознакомиться с Правилами эксплуатации Ключевого устройства, указанными в Приложении 4 к Правилам;
    - г) после получения Ключевого устройства в Банке Пользователь/Уполномоченное лицо Клиента должен самостоятельно изменить Пароль Ключевого устройства (установленный производителем Ключевого устройства), на новый пароль. Измененный Пароль Ключевого устройства будет использоваться Пользователем/Уполномоченным лицом Клиента в Системе «ATF Online» для Идентификации и(или) Аутентификации;
  - 3) в случае утери/поломки Ключевого устройства Клиент вправе получить новое Ключевое устройство, обратившись в Банк с Заявкой на доступ. Заявка на доступ должна быть подписана первым руководителем Клиента или Представителем Клиента, скреплена оттиском печати (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства) и передана в Банк на бумажном носителе;
  - 4) Клиент может получить новое Ключевое устройство с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации, выпущенными на имя Пользователя/Уполномоченного лица Клиента, после подписания Акта приема-передачи Ключевого устройства с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации, составленного по форме согласно Приложению 2 к Правилам и Акта приема-передачи Имени пользователя (логина) и Пароля для входа в Систему «ATF Online», составленного по форме согласно Приложению 3 к Правилам. При получении нового Ключевого устройства, ранее выданные Регистрационные свидетельства и Ключи первичной инициализации аннулируются Банком без участия Пользователя/Уполномоченного лица Клиента. Пользователь/Уполномоченное лицо Клиента может получить сам новое Ключевое устройство с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации, выпущенными на его имя. При этом выдаются новые Регистрационные свидетельства первичной инициализации и Ключи первичной инициализации. Также Представитель Клиента, первый руководитель Клиента могут получить новое Ключевое устройство с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации, выпущенными на имя Пользователя/Уполномоченного лица Клиента;
  - 5) Имя пользователя (логин) и Пароль для входа в Систему «ATF Online» формируется Банком самостоятельно без участия Пользователя/Уполномоченного лица Клиента. Смена Пароля для входа в Систему «ATF Online» осуществляется Пользователем/Уполномоченным лицом Клиента самостоятельно при первом входе, и в дальнейшем Пользователь/Уполномоченное лица Клиента должен поменять Пароль для входа в Систему «ATF Online» один раз в 30 (тридцати) календарных дней;

6) в случае утери/утраты Имени пользователя (логина) и/или Пароля для входа в Систему «ATF Online» Пользователь/Уполномоченное лицо Клиента вправе получить новое Имя пользователя (логин) и/или Пароль для входа в Систему «ATF Online» на основании письменного обращения Клиента в Банк, подписанного первым руководителем Клиента или Представителем Клиента, и скрепленного оттиском печати Клиента (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства). Получение нового Имени пользователя (логин) и Пароля для входа в Систему «ATF Online» осуществляется Пользователем/Уполномоченным лицом Клиента или Представителем Клиента или первым руководителем Клиента в Банке по Акту приема-передачи Ключевого устройства с регистрационным свидетельством первичной инициализации, составленного по форме согласно Приложению 2 к Правилам и Акту приема-передачи Имени пользователя (логина) и Пароля для входа в Систему «ATF Online», составленного по форме согласно Приложению 3 к Правилам;

7) вход в Систему «ATF Online» Пользователем/Уполномоченным лицом Клиента осуществляется через соответствующий веб-адрес путем подключения Ключевого устройства в USB-порт персонального компьютера, ввода Пользователем/Уполномоченным лицом Клиента Имени пользователя (логина), Пароля для входа в Систему «ATF Online» и Пароля Ключевого устройства. При неверном указании Имени пользователя (логина) и/или Пароля для входа в Систему «ATF Online» более 5 (пять) раз подряд вход в Систему «ATF Online» блокируется.

При неверном вводе Пароля Ключевого устройства более 5 (пяти) раз подряд Ключевое устройство блокируется, а при наличии ОТР-токена и неверном вводе Сеансового кода – 5 (пять) раза подряд, ОТР-токен блокируется. В случае блокировки учетной записи либо Ключевого устройства/ОТР-токена Уполномоченному лицу Клиента необходимо обратиться в отделение Банка. Разблокировка учетной записи по телефонному звонку не осуществляется;

8) срок действия Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации составляет 30 (тридцать) календарных дней с даты выпуска, без возможностей подписывать документы. При не прохождении Пользователем/Уполномоченным лицом Клиента процедуры перевыпуска Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации в течение 30 календарных (тридцати) дней, срок действия Ключей первичной инициализации и Регистрационного свидетельства истекает, и доступ к Системе «ATF Online» будет невозможен. В этом случае Пользователю/Уполномоченному лицу Клиента необходимо обратиться в Банк для получения нового комплекта Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации на основании новой Заявки на доступ;



9) в целях соблюдения Процедуры безопасности при подключении к Системе «ATF Online», после получения Ключевого устройства, Пользователь/Уполномоченное лицо Клиента обязан (-о) провести перевыпуск временного Регистрационного свидетельства первичной инициализации и Ключей первичной инициализации на годовое Регистрационное свидетельство и ключи (Открытый (публичный) и Закрытый (секретный) ключи) посредством Системы «ATF Online». Срок действия годовых ключей (Открытого (публичного) и Закрытого (секретного) ключей) и Регистрационного свидетельства, за исключением Ключей первичной инициализации), составляет 1 (один) год с даты выпуска. Пользователь/Уполномоченное лицо Клиента обязан при получении уведомления в Системе «ATF Online», но не позднее, чем за 30 (тридцать) календарных дней до истечения срока действия ключей (Открытого (публичного) и Закрытого (секретного) ключей) и Регистрационного свидетельства отправить посредством Системы «ATF Online» электронный запрос в Удостоверяющий центр на генерацию нового комплекта ключей (Открытого (публичного) и Закрытого (секретного) ключей) и выпуска Регистрационного свидетельства к ним. При не прохождении Пользователем/Уполномоченным лицом Клиента процедуры перевыпуска ключей (Открытого (публичного) и Закрытого (секретного) ключей) и Регистрационного свидетельства в указанный срок, срок действия ключей (Открытого (публичного) ключа и Закрытого (секретного) ключей) и Регистрационного свидетельства истечет, и доступ к Системе «ATF Online» будет невозможен. Клиенту необходимо будет обратиться в Банк для получения нового комплекта Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации на основании Заявки на доступ, подписанной первым руководителем или Представителем Клиента и скрепленная оттиском печати Клиента (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства);

10) подключение Банковских счетов Клиента к Системе «ATF Online» для получения Электронных банковских услуг и исключение их из Системы «ATF Online» осуществляется на основании Заявки на доступ и/или письма, предоставленной (-го) Клиентом Банку, подписанной (-го) первым руководителем или Представителем Клиента, и скрепленное оттиском печати Клиента (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства).

13. Порядок и условия предоставления Информационных банковских услуг в Системе «ATF Online»:

1) Информационные банковские услуги предоставляются при условии Идентификации Пользователя/Уполномоченного лица Клиента;

2) после получения доступа к Системе «ATF Online» Пользователь/Уполномоченное лицо Клиента вправе самостоятельно получать Информационные банковские услуги, посредством Системы «ATF Online».

14. Порядок и условия предоставления Электронных платежных услуг в Системе «ATF Online»:

1) предоставление Электронных платежных услуг осуществляется при условии Идентификации и Аутентификации;

2) в целях установления подлинности и правильности составления Электронных документов производится Аутентификация путем подключения Ключевого устройства в USB-порт персонального компьютера и ввода Имени пользователя (логина) и Пароля Ключевого устройства;

3) Электронные платежные услуги предоставляются по Электронным документам Уполномоченного лица Клиента при условии их принятия на исполнение Банком. При получении Электронных платежных услуг Уполномоченное лицо Клиента использует формы Электронных документов, имеющиеся в Системе «ATF Online»;

4) Электронные документы подписываются только Уполномоченным лицом Клиента. В случаях, когда Электронные документы должны быть подписаны несколькими Уполномоченными лицами Клиента, обладающими правом подписи, Электронные документы считаются надлежащим образом предоставленными Банку только после подписания их соответствующими Уполномоченными лицами Клиента в соответствии с поручениями Клиента и требованиями законодательства Республики Казахстана.

В случае если Клиентом в Заявке на доступ указывается о том, что Электронные документы должны быть дополнительно одобрены путем проставления «Визы» (санкционированы) третьим лицом (Пользователем/Уполномоченным лицом Клиента), то

Электронные документы считаются надлежащим образом предоставленными Банку только после их одобрения такими лицами. При этом Банк оставляет за собой право отказать в исполнении Электронных документов, которые не были дополнительно одобрены третьим лицом (Пользователем/Уполномоченным лицом Клиента);

5) Клиент заполняет Электронные документы в Системе «ATF Online» в соответствии с законодательством Республики Казахстан, а также учитывая условия, содержащиеся в инструкции ATF Online, размещенной на Веб-сайте Банка, при этом вся ответственность, включая возможный причиненный ущерб за неправильное оформление Электронных документов, возлагается на Клиента;

6) платежи и переводы через Систему «ATF Online» осуществляются только с Текущих счетов Клиента;

7) платежи и переводы в иностранной валюте через Систему «ATF Online» осуществляются с соблюдением законодательства Республики Казахстан о валютном регулировании и валютном контроле, по курсу обмена валют, установленному в Банке;

8) осуществление действий по исполнению Электронных документов производится Банком в соответствии с законодательством Республики Казахстан, Правилами, Договором и/или соответствующим договором, регулирующим отношения между Банком и Клиентом в части проведения операций по Банковскому счету;

9) Банк отказывает в принятии на исполнение Электронных документов, в случаях, предусмотренных законодательством Республики Казахстан, Договором и/или соответствующим договором, регулирующим отношения между Банком и Клиентом в части проведения операций по Банковскому счету.

10) после отправки Клиентом Электронного документа в Банк по Системе «ATF Online» отображается статус по направленному Электронному документу (отправлен в Банк, принят, отказан Банком и др.);

11) операционный день Банка устанавливается Банком и изменяется Банком в одностороннем порядке. Информация об операционном дне Банка размещена на Веб-сайте Банка и(или) в отделениях Банка.

## **Статья 5. Приостановление/возобновление и прекращение предоставления Электронных банковских услуг**

15. Банк блокирует доступ (приостанавливает предоставление Электронных банковских услуг) Пользователю/Уполномоченному лицу Клиента в Систему «ATF Online» в случае письменного обращения Пользователя/Уполномоченного лица Клиента в Банк либо обращения по телефону в Банк по Контактным данным с дальнейшим предоставлением письменного заявления.

16. Блокирование доступа Пользователю/Уполномоченному лицу Клиента в Систему «ATF Online» осуществляется Банком в Рабочие дни в течение 15 (пятнадцати) минут с момента обращения Пользователя/Уполномоченного лица Клиента и его Идентификации. При обращении Пользователя/Уполномоченного лица Клиента в не рабочее время Банка блокирование доступа к Системе «ATF Online» осуществляется в первый Рабочий день после выходных в течение 15 (пятнадцати) минут после начала Рабочего дня. Идентификация в указанных целях осуществляется по следующим параметрам Пользователя/Уполномоченного лица Клиента: бизнес-идентификационный номер (БИН) Клиента, наименование Клиента, фамилия, имя, отчество (при наличии) Пользователя/Уполномоченного лица Клиента, номер и срока действия документа, удостоверяющего личность Пользователя/Уполномоченного лица Клиента). Порядок и условия приостановления/возобновления/прекращения предоставления Электронных банковских услуг, устанавливаются Договором.

## **Статья 6. Процедуры безопасности при подключении к Системе «ATF Online»**

17. В целях обеспечения конфиденциальности передаваемой и получаемой информации в Системе «ATF Online» используется шифрование 128/256 bit TLS (Transport Layer Security – уровень защищенных сокетов или протокол безопасных соединений). Шифрование преобразует данные Клиента в Системе «ATF Online» в зашифрованный код

перед их отправкой через сеть интернет и обеспечивает конфиденциальность информации Клиента на пути между компьютерной системой Банка и интернет-браузером Клиента.

18. При Идентификации и Аутентификации в Системе «ATF Online» на Веб-сайте Банка интернет-браузер Клиента запрашивает подтверждение Веб-сайта Банка своей идентификационной информацией посредством цифровых сертификатов. Интернет-Браузер Клиента должен проверить цифровой сертификат и предупредить Клиента, если данный Веб-сайт не принадлежит Банку. При Идентификации Клиент должен удостовериться в том, что проверка цифрового сертификата интернет-браузером прошла успешно.

19. В целях Идентификации при осуществлении доступа в Систему «ATF Online» предусматриваются следующие идентифицирующие данные при входе в Систему «ATF Online»: Имя пользователя (логин), Пароль для входа в Систему «ATF Online», подключение Ключевого устройства в USB-порт персонального компьютера и ввод Пароля Ключевого устройства, принадлежащие данному Пользователю/Уполномоченному лицу Клиента.

20. В целях Аутентификации при получении Клиентом Электронных платежных услуг предусматривается обязательное подключение Ключевого устройства (использование Закрытого (секретного) ключа) в USB-порт персонального компьютера Уполномоченного лица Клиента и введение Пароля Ключевого устройства.

21. Пользователь/Уполномоченное лицо Клиента не вправе разглашать/передавать третьим лицам Имя пользователя (логин), Пароль для входа в Систему «ATF Online», OTP-токен/Сеансовый код, Пароль Ключевого устройства, Ключевое устройство. Хранить Имя пользователя (логин), Пароль для входа в Систему «ATF Online», Пароль Ключевого устройства, Ключевое устройство, OTP-токен необходимо в условиях, исключающих доступ к ним неуполномоченных лиц.

22. В целях безопасности в Системе «ATF Online» предусмотрена функция автоматического отключения текущей сессии Клиента в Системе «ATF Online». Под автоматическим отключением текущей сессии Клиента в Системе «ATF Online» понимается отказ в предоставлении Электронных банковских услуг в случае продолжительного (более 10 последовательных минут) отсутствия активных действий Клиента в Системе «ATF Online» (неосуществление любых операций и действий и т.д.). При этом, запрещается оставлять персональный компьютер с открытой сессией в отсутствие Пользователя/Уполномоченного лица Клиента.

23. В целях подтверждения данных, указанных в Заявке на доступ, Банк вправе посредством телефонной связи получить/уточнить необходимые сведения, связанные с исполнением Заявки на доступ Клиента.

24. В целях защиты от доступа третьих лиц к Системе «ATF Online» и Ключевому устройству Пароль входа в Систему «ATF Online» и Пароль ключевого устройства должны удовлетворять следующим минимальным требованиям:

- 1) не должны содержать Имя пользователя (логин) или какую-либо его часть;
- 2) должны состоять не менее чем из 8 (восьми) символов;
- 3) должны содержать символы трех категорий из числа следующих четырех:
  - а) прописные буквы английского алфавита от А до Z;
  - б) строчные буквы английского алфавита от а до z;
  - в) десятичные цифры (от 0 до 9);
  - г) неалфавитные символы (например, !, \$, #, %).

### **Глава 3. Заключительные положения**

#### **Статья 7. Контактные данные Банка**

25. По вопросам, связанным с предоставлением Электронных банковских услуг Клиент может обратиться по следующим Контактным данным: телефоны: 8-8000-800-283 (звонок по Казахстану бесплатный), +7 (727) 258-30-00 и +7 (727) 258 30 38 по г. Алматы.

26. Юридический адрес Банка: Республика Казахстан, А25D5F7, г. Алматы, Медеуский район, проспект Аль-Фараби, 36. Адреса филиалов Банка указаны на Веб-сайте Банка.

27. Банк вправе в одностороннем порядке изменять Контактные данные, указанные в пункте 25 Правил, с уведомлением Клиента о таких изменениях на Веб-сайте Банка.

## **Статья 8. Заключительные положения**

28. Банк вправе в одностороннем порядке вносить изменения в Правила и за 5 (пять) Рабочих дней до даты их вступления в силу размещать на Веб-сайте Банка.

29. Иные вопросы, не урегулированные Правилами, разрешаются в соответствии с законодательством Республики Казахстан, корпоративными нормативными документами Банка, Договором и обычаями делового оборота, принятыми в банковской практике.

форма

### Заявка на предоставление доступа к Системе «ATF Online»

Прошу АО «АТФБанк» (Банк) принять настоящую Заявку на предоставление доступа к Системе «ATF Online» (далее – Заявка) на условиях, указанных ниже:

#### 1. Информация о Клиенте:

(i) для юридического лица указать наименование:	
(ii) для индивидуального предпринимателя/нотариуса/адвоката/ частного судебного исполнителя указать/профессионального медиатора ФИО и наименование (если таковое имеется):	
Юридический адрес:	
БИН/ИНН:	
Телефон/Факс:	
Контактное лицо:	
Мобильный номер контактного лица:	
Адрес электронной почты:	

#### 2. Информация о руководителе Клиента:

Наименование должности:	
ФИО:	
ИИН:	
Указать вид документа удостоверяющего личность (удостоверение личности/паспорт/вид на жительство/другое), кем и когда выдан:	
Права подписи:	
Телефон (городской и мобильный):	

Адрес электронной почты:	
Действующий на основании:	

### 3. Информация о подключаемых Пользователях/Уполномоченных лицах Клиента:

#### 3.1. Уполномоченное лицо:

ФИО:		
ИИН:		
Указать вид документа удостоверяющего личность (удостоверение личности/паспорт/вид на жительство/другое), кем и когда выдан:		
Должность:		
Гражданство:		
Телефон (городской и мобильный):		
Адрес электронной почты:		
Зарегистрировано ли Уполномоченное лицо Клиента в Системе «ATF Online» и имеет ли Ключевое устройство как пользователь/уполномоченное лицо другого клиента Банка или сам является клиентом Банка, который пользуется Электронными банковскими услугами через Систему «ATF Online»:	Да: <input type="checkbox"/>	Нет: <input type="checkbox"/>
	Указать наименование/ФИО и БИН/ИИН такого клиента Банка: Наименование/ФИО: _____ БИН/ИИН: _____	
<i>Нижеуказанная строка заполняется при необходимости:</i>		
Клиент желает использовать Регистрационное свидетельство первичной инициализации, Ключи первичной инициализации, Регистрационное свидетельство, Закрытый (секретный) и Открытый (публичный) ключи, которые были выпущены для другого клиента Банка, где Уполномоченное лицо Клиента является пользователем/уполномоченным лицом другого клиента Банка. Указать наименование/ФИО и БИН/ИИН такого клиента Банка: _____, _____.		
_____ / _____ <i>подпись</i> / <i>ФИО</i>		
М.П. (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства)		

*выбрать необходимое:*

- регистрация Уполномоченного лица Клиента в Системе «ATF Online» и выдача Ключевого устройства;
- регистрация Уполномоченного лица Клиента в Системе «ATF Online» и выдача Ключевого устройства и OTP-токена;

- повторное изготовление Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации (указать причину) \_\_\_\_\_;
- повторная выдача ОТР-токена (указать причину) \_\_\_\_\_;
- удалить использование ОТР-токена для Уполномоченного лица Клиента;
- удалить Уполномоченное лицо Клиента из Системы «ATF Online».

**Примечание:** Права подписи Уполномоченного лица Клиента в Системе «ATF Online» указывается в соответствии с документом с образцами подписей Клиента, предоставленным Клиентом Банку.

### 3.2. Пользователь:

ФИО:		
ИИН:		
Указать вид документа, удостоверяющего личность (удостоверение личности/паспорт/вид на жительство/другое) кем и когда выдан:		
Должность:		
Гражданство:		
Телефон (городской и мобильный):		
Адрес электронной почты:		
Зарегистрирован ли Пользователь в Системе «ATF Online» и имеет ли Ключевое устройство как пользователь/уполномоченное лицо другого клиента Банка или сам является клиентом Банка, который пользуется Электронными банковскими услугами через Систему «ATF Online»:	Да: <input type="checkbox"/>  Указать наименование/ФИО и БИН/ИИН такого клиента Банка: Наименование/ФИО: _____ БИН/ИИН: _____	Нет: <input type="checkbox"/>
<i>Нижеуказанная строка заполняется при необходимости:</i>		
Клиент желает использовать Регистрационное свидетельство первичной инициализации, Ключи первичной инициализации, Регистрационное свидетельство, Закрытый (секретный) и Открытый (публичный) ключи, которые были выпущены для другого клиента Банка, где Пользователь является пользователем/уполномоченным лицом другого клиента Банка. Указать наименование/ФИО и БИН/ИИН такого клиента Банка: _____, _____.		
_____ подпись / ФИО Клиента		
М.П. (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства)		

выбрать необходимое:

- регистрация Пользователя в Системе и выдача Ключевого устройства;
- повторное изготовление Ключей первичной инициализации и Регистрационного свидетельства первичной инициализации (указать причину): \_\_\_\_\_;
- удалить Пользователя из Системы;

Если Пользователь уже зарегистрирован в Системе и имеет Ключевое устройство как пользователь/уполномоченное лицо другого клиента Банка или сам является клиентом Банка, который пользуется электронными банковскими услугами, указать наименование и БИН/ИИН такогоклиента Банка:

\_\_\_\_\_.

### 3.3. Подключаемые Банковские счета к Системе «ATF Online»:

Банковские счета Клиента	Номера Банковских счетов Клиента
Текущие:	
Сберегательные:	

### 3.4. Лимиты на распоряжение деньгами в Системе «ATF Online»:

Таблица № 1:

№	Номер Текущего счета	Максимальная сумма по одному платежу/переводу	Максимальная сумма платежей/переводов за один день
1.			
2.			
3.			



**Таблица № 2:**

№	Номер Текущего счета	Указать ФИО лица (Пользователя/Уполномоченного лица), которое будет проставлять «Визу» для проведения платежей/переводов Клиента:	Сумма одного платежа/перевода, при превышении которой требуется «Виза» на платежном документе Клиента:	Общая сумма платежей/переводов за один день, при превышении которой требуется «Виза» на платежном документе Клиента:
1.				
2.				
3.				

**3.5. Информация по правам доступа:**

№	ФИО Пользователя Клиента	Номер Банковского счет	<input checked="" type="checkbox"/> Получение Выписок	<input checked="" type="checkbox"/> Создание шаблонов платежных документов, за исключением шаблонов, указанных далее	<input checked="" type="checkbox"/> Создание шаблонов документов в для осуществления обменных операций	<input checked="" type="checkbox"/> Получение и отправка писем Банку	<input checked="" type="checkbox"/> Просмотр всех входящих платежей/переводов	<input checked="" type="checkbox"/> Создание шаблонов документов для осуществления операций по выплате зарплаты работникам	<input checked="" type="checkbox"/> Создание шаблонов документов для открытия и (или) пополнения Вкладов*
1.									
2.									
3.									

\* Отображаются только Сберегательные счета по вкладам, открытым в Системе «ATF Online».

№	ФИО Уполномоченного лица Клиента	Номер Банковского счет	<input checked="" type="checkbox"/> Получение Выписок	<input checked="" type="checkbox"/> Создание шаблонов платежных документов, за исключением шаблонов, указанных далее, а также направление платежных документов в Банк	<input checked="" type="checkbox"/> Создание шаблонов документов для осуществле ния обменных операций, а также направление таких платежных документов в Банк	<input checked="" type="checkbox"/> Получение и отправка писем Банку	<input checked="" type="checkbox"/> Просмотр всех входящих платежей/ переводов	<input checked="" type="checkbox"/> Создание шаблонов документов для осуществления операций по выплате зарплаты работникам, а также направление таких платежных документов в Банк	<input checked="" type="checkbox"/> Создание шаблонов документов для открытия и (или) пополнения Вкладов*, а также направление таких документов в Банк
1.									
2.									
3.									

\* Отображаются только Сберегательные счета по вкладам, открытым в Системе «ATF Online».

#### 4. Настоящим Клиент заверяет Банк в том, что:

(i) обладает необходимыми полномочиями по указанию в Заявке информации о физических лицах, указанных в ней, и передача такой информации Банку не будет нарушать прав таких лиц;

(ii) физические лица, указанные в Заявке в качестве Пользователей/Уполномоченных лиц согласны с тем, что на их имя будут предоставлены (выпущены) регистрационное свидетельство и закрытый ключ ЭЦП Удостоверяющего центра для работы в Системе «ATF Online» и выданы.

В случае если указанные заверения являются ничтожными (не действительными), что повлекло для Банка негативные последствия, включая но не ограничиваясь: претензии указанных лиц, в отношении которых была предоставлена информация Клиентом, вовлечение Банка в судебные процессы, возмещение указанным лицам ущерба и иных доказанных и обоснованных сумм, Клиент обязуется возместить суммы, подлежащие выплате (или выплаченные) таким лицам Банком.

#### 5. Настоящий раздел заполняется в случае, если Заявка будет подписана первым руководителем Клиента, обладающим правом подписывать/выдавать доверенности от имени Клиента:

Настоящим, \_\_\_\_\_ (указать наименование и БИН/ИИН Клиента), в лице \_\_\_\_\_ (ФИО, наименование должности первого руководителя) уполномочиваю \_\_\_\_\_ (указать ФИО и ИИН) Представителя Клиента на совершение следующих действий от имени \_\_\_\_\_ (указать наименование и БИН/ИИН Клиента):

получить от Банка: (i) Имя пользователя (логин), (ii) Пароль для входа в Систему «ATF Online» и (iii) Ключевое устройство, а также совершать все необходимые действия, связанные с данным поручением, включая подписание Акта приема-передачи.

**Клиент (подпись):** \_\_\_\_\_

**ФИО подписанта Клиента:** \_\_\_\_\_

*М.П. (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства)*

**Дата:** \_\_\_\_\_

**ОТМЕТКА Банка о принятии Заявки:**

ФИО работника Банка: \_\_\_\_\_

Подпись работника Банка: \_\_\_\_\_  
штамп работника Банка

**Дата:** \_\_\_\_\_

форма

**Акт приема-передачи  
Ключевого устройства с Регистрационным свидетельством первичной инициализации  
и Ключами первичной инициализации/ОТР-токена**

г. \_\_\_\_\_

«\_\_» \_\_\_\_\_ 20\_\_ г.

**Акционерное общество «АТФБанк»**, именуемое в дальнейшем «**Банк**», в лице г-на/г-жи \_\_\_\_\_ (указать должность и ФИО), и  
*Клиент – юридическое лицо:*

[ \_\_\_\_\_ « \_\_\_\_\_ » (указать организационно-правовую форму и наименование Клиента), именуемое в дальнейшем  
«**Клиент**», в лице г-на (г-жи) \_\_\_\_\_ (указать должность (при  
наличии) и ФИО (полностью)), действующего(-ей) на основании \_\_\_\_\_ (указать ),]

*Клиент – физическое лицо:*

[ \_\_\_\_\_ (указать ФИО и наименование (при наличии)), именуемый(-ая) в дальнейшем «**Клиент**»,]

далее совместно именуемые «**Стороны**», подписали настоящий Акт приема-передачи о нижеследующем:

Банк передает, а Клиент принимает на каждого Пользователя/Уполномоченного лица Клиента Ключевое устройство с Регистрационным свидетельством первичной инициализации и Ключами первичной инициализации (Открытый (публичный) и Закрытый (секретный) ключи) (на каждом Ключевом устройстве имеется Регистрационное свидетельство первичной инициализации и Ключи первичной инициализации (Открытый (публичный) и Закрытый (секретный) ключи) и/или ОТР токен согласно нижеуказанной таблице:

Ф.И.О. Пользователя/Уполномоченного лица Клиента	Серийный номер Ключевого устройства/ОТР-токена:	Номер Регистрационного свидетельства первичной инициализации на Ключевом устройстве:
1.		
2.		
3.		
4.		

**Подписи Сторон:**

Банк:	Клиент:
Передал:	Принял:

<p>Ф.И.О. Работника: _____ Должность: _____ Филиал АО "АТФБанк": _____</p> <p>Подпись: _____ <i>(штамп)</i></p>	<p>Ф.И.О. Клиента: _____ Должность: _____ Организация: _____ БИН/ИИН: _____</p> <p>Подпись: _____ <i>М.П. (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства)</i></p>
---	---

форма

**Акт приема-передачи  
Имени пользователя (логина) и Пароля для входа в Систему «ATF Online»**

г. \_\_\_\_\_

«\_\_\_» \_\_\_\_\_ г.

**Акционерное общество «АТФБанк»**, именуемое в дальнейшем **«Банк»**, в лице г-на/г-жи \_\_\_\_\_ (указать должность и ФИО), и  
*Клиент – юридическое лицо:*

[\_\_\_\_\_ «\_\_\_\_\_» (указать организационно-правовую форму и наименование Клиента), именуемое в дальнейшем  
**«Клиент»**, в лице г-на (г-жи) \_\_\_\_\_ (указать должность (при  
наличии) и ФИО (полностью)), действующего(-ей) на основании \_\_\_\_\_ (указать ),]

*Клиент – физическое лицо:*

[\_\_\_\_\_ (указать ФИО и наименование (при наличии)), именуемый(-ая) в дальнейшем **«Клиент»**,]

далее совместно именуемые **«Стороны»**, подписали настоящий Акт приема-передачи о нижеследующем:

Банк передает, а Клиент принимает на каждого Пользователя/Уполномоченного лица Клиента Имя пользователя (логин) и Пароль для входа в Систему «ATF Online»:

<b>Ф.И.О. Пользователя/Уполномоченного лица Клиента</b>	<b>Примечания:</b>
1.	
2.	
3.	
4.	

**Подписи Сторон:**

<b>Банк:</b>	<b>Клиент:</b>
--------------	----------------

Передал:  
Ф.И.О. Работника: \_\_\_\_\_  
Должность: \_\_\_\_\_  
Филиал АО "АТФБанк": \_\_\_\_\_

Подпись: \_\_\_\_\_  
(штамп)

Принял:  
Ф.И.О. Клиента: \_\_\_\_\_  
Должность: \_\_\_\_\_  
Организация: \_\_\_\_\_  
БИН/ИИН: \_\_\_\_\_

Подпись: \_\_\_\_\_  
*М.П.* (скрепляется оттиском печати если Клиент является юридическим лицом, которое не относится к субъектам частного предпринимательства)

### **Правила эксплуатации Ключевого устройства и ОTR-токена**

1. Ключевое устройство хранит Регистрационные свидетельства и Закрытые (секретные)/Открытые (публичные) ключи. В связи с этим необходимо хранить Ключевое устройство в местах, исключающих доступ к Ключевому устройству неуполномоченных лиц. При подозрении на компрометацию, необходимо незамедлительно уведомить Банк для блокирования доступа к Системе «ATF Online».
2. Доступ к Ключевому устройству Пользователя/Уполномоченного лица Клиента, должен быть доступен только тем, для которых они были выданы, а также Представителю Клиента только для целей их получения и передачи Пользователю/Уполномоченному лицу Клиента. Никто более, включая работников Банка, НЕ ДОЛЖЕН ИМЕТЬ ДОСТУП к Ключевому устройству.
3. Ключевое устройство следует подключать к персональному компьютеру только на время выполнения операций в Системе «ATF Online». Для работы с Ключевым устройством, необходимо подключить его в работающий USB-порт персонального компьютера.
4. При первичном подключении Ключевого устройства в персональный компьютер Уполномоченное лицо Клиента/Пользователь обязан (-о) сменить Пароль Ключевого устройства на новый. Смена Пароля ключевого устройства производится через средство криптографической защиты информации Tumar CSP. Для изменения Пароля Ключевого устройства зайдите: Пуск-Программы-GammaTech-TumarCSP-ТумарКонфигуратор. В верхней части окна Тумар CSP Конфигуратор найдите профайл JavaToken, кликните по нему правой кнопкой мыши и выберите «Изменить пароль на контейнере». Согласно политике безопасности Пароль Ключевого устройства должен содержать более 8 (восемью) символов. Введите текущий Пароль Ключевого устройства, далее новый Пароль Ключевого устройства и подтверждение нового Пароля Ключевого устройства. Нажмите «ОК». Пароль ключевого устройства успешно изменен. После выхода из Системы «ATF Online», необходимо отключать Ключевое устройство от персонального компьютера.
5. Проверяйте, что соединение установлено именно с сервером Банка.
6. Если Вы получили электронное сообщение с неизвестным вложением или со ссылкой на неизвестный Вам ресурс, удалите это сообщение, не открывая вложения и не активируя ссылку.
7. В случае, если персональный компьютер, с которого производится отправка и обработка платежей в Системе «ATF Online», неожиданно перестал запускаться или выдает непонятные сообщения, рекомендуется незамедлительно связаться с Менеджером счета Банка и заблокировать учетную запись Пользователя/Уполномоченное лицо Клиента (обратиться за приостановлением предоставления Электронных платежных услуг).
8. Никому, включая работников Банка, ни при каких условиях не сообщайте конфиденциальную информацию. Ни один работник Банка, ни при каких условиях не вправе потребовать от Вас информации о Пароле Ключевого устройства. При увольнении работника Клиента, являющегося Пользователем/Уполномоченным лицом Клиента, имевшего доступ в Систему «ATF Online», необходимо обратиться к Менеджеру счета в Банк и заблокировать доступ соответствующему Пользователю/Уполномоченному лицу Клиента к Системе «ATF Online».
9. Строго запрещается вскрывать корпус ОTR-токена и/или Ключевого устройства и подвергать иному воздействию.
10. При входе в Систему «ATF Online» после ввода Имени пользователя (логина) и Пароля выйдет окно ввода Сеансового кода. Нажмите на ОTR-токене кнопку генерации пароля. На дисплее появится комбинация из 6 цифр, которую необходимо ввести.
11. Сеансовый код представляет собой 6-значную комбинацию цифр, которую должно видеть Уполномоченное лицо Клиента.
12. Пароль Ключевого устройства представляет собой комбинацию цифр/букв, известную Пользователю/Уполномоченному лицу Клиента, владеющему данным устройством. Если



Пароль Ключевого устройства случайным образом становится известен третьим лицам, его надо незамедлительно сменить. В целях безопасности Пароль Ключевого устройства должен быть максимально сложным. Его надо запомнить (не записывать) и не раскрывать третьим лицам. Пароль Ключевого устройства используется при подписании Электронных документов в Системе «ATF Online».

13. Если все попытки (5 раз) ввода Пароля Ключевого устройства исчерпаны Ключевое устройство блокируется. Необходимо обратиться в Банк к Менеджеру счета для получения нового Регистрационного свидетельства первичной инициализации и Ключей первичной инициализации на основании новой Заявки на доступ.
14. В случае неверного ввода Сеансового кода (5 раза), OTP-токен блокируется. Необходимо обратиться в Банк к Менеджеру счета для проведения разблокировки.
15. В случае утери OTP-токена или Ключевого устройства незамедлительно обратитесь в Банк к Менеджеру счета или по Контактным данным для приостановления Электронных банковских услуг для Пользователя/Уполномоченного лица Клиента.
16. Чтобы обеспечить высокий уровень защиты информации для Клиентов, пользующихся Системой «ATF Online», применяются Ключевые устройства JaCarta производства Компании «Аладдин Р.Д.» и OTP-токены. JaCarta – новое поколение USB-токенов для строгой аутентификации, электронной подписи и безопасного хранения ключей и регистрационных свидетельств. OTP-токены – устройства генерации 6-ти значных Сеансовых кодов.

### Краткие технические характеристики Ключевого устройства JaCarta

Наименование атрибута	Функционал/Значение
Область применения	Обеспечение защищенной генерации и хранения закрытых ключей, а также сертификатов пользователей, предоставленных Удостоверяющим центром РГП «Казахстанский центр межбанковских расчетов» Национального Банка Республики Казахстан, для пользователей системы дистанционного банковского обслуживания юридических лиц. Обеспечение возможности двухфакторной аутентификации и электронной цифровой подписи.
Поддерживаемые алгоритмы и стандарты	Алгоритмы криптографического преобразования: <ul style="list-style-type: none"> <li>• ГОСТ 34.310-2004</li> <li>• ГОСТ 34.311-95</li> <li>• ГОСТ 28147-89</li> <li>• X509 V.3</li> </ul>
Токен должен функционировать под управлением следующих ОС	Для Microsoft Windows XP/Vista/7/8/8.1/2003/2008/2012, 32/64 бит - Linux; -Apple MacOS X;
Токен должен	- обеспечивать двухфакторную аутентификацию; - обеспечивать защиту от перебора ввода PIN – кода; - обеспечивать 2 уровня доступа к токену: Гость, Пользователь
Сертификация	Сертификация токена на соответствие 2 уровню безопасности СТ РК 1073-2007
Объем защищенной памяти	не менее 72 КБ
Количество циклов перезаписи в одну ячейку EEPROM-памяти	не менее 500 000
Характеристики производительности	Генерация ключевой информации (ГОСТ на подпись и ГОСТ на шифрование) – не более 4 секунд. Формирование ЭЦП – не более 1 секунды.
Поддерживаемые интерфейсы и	• PKCS#11 • Спецификация ISO - ISO7816

Наименование атрибута	Функционал/Значение
стандарты	<ul style="list-style-type: none"> <li>• CAPI</li> <li>• PC/SC</li> <li>• Хранение сертификатов X.509 v3</li> <li>• Microsoft CCID</li> <li>• Smartcard Minidriver</li> </ul>

#### Краткие технические характеристика OTP-токена

Наименование атрибута	Функционал/Значение
Область применения	Автономный генератор одноразовых паролей, применяется для дополнительной Аутентификации при входе в систему и при получении Клиентом Электронных платежных услуг.
Поддерживаемые алгоритмы и стандарты	<p>Алгоритмы криптографического преобразования:</p> <ul style="list-style-type: none"> <li>• ГОСТ 34.310-2004</li> <li>• ГОСТ 34.311-95</li> <li>• ГОСТ 28147-89</li> <li>• X509 V.3</li> </ul>
Сертификация	Сертификация токена на соответствие национальным стандартам Республики Казахстан должна быть подтверждена. Подтверждающий документ – сертификат соответствия 3 уровню безопасности СТ РК 1073-2007
Объем защищенной памяти	не менее 72 КБ
Рабочая температура	в диапазоне: 0°C - 70°C
Температура хранения	-40°C - 85°C
Срок хранения данных памяти	не менее 10 лет
Количество циклов перезаписи в одну ячейку EEPROM-памяти	не менее 500 000
Характеристики производительности	Генерация ключевой информации (ГОСТ на подпись и ГОСТ на шифрование) – не более 4 секунд. Формирование ЭЦП – не более 1 секунды.
Поддерживаемые интерфейсы и стандарты	<ul style="list-style-type: none"> <li>• PKCS#11</li> <li>• Спецификация ISO - ISO7816</li> <li>• CAPI</li> <li>• PC/SC</li> <li>• Хранение сертификатов X.509 v3</li> <li>• Microsoft CCID</li> <li>• Smartcard Minidriver</li> </ul>