

ПРАВИЛА электронного документооборота при заключении Генерального Соглашения и Депозитарного договора

1 ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩИХ ПРАВИЛАХ:

Указанные ниже термины применяются дополнительно к терминам, установленным Регламентом. В случае расхождений между определениями терминов, установленным настоящими Правилами и основным текстом Регламента, для целей настоящих Правил применяются термины, установленные настоящими Правилами.

Владелец Ключа – лично Клиент;

Номер телефона Клиента – номер телефона сотовой связи Клиента, указанный Клиентом Банку перед подписанием Электронных документов Клиента. Клиент несет ответственность за актуальность указанных Банку Номеров телефонов Клиента.

Клиент – физическое лицо, являющееся гражданином Российской Федерации, намеревающееся заключить или заключившее с Банком Генеральное Соглашение и Депозитарный Договор в порядке, предусмотренном настоящими Правилами.

Интернет-канал – ресурс Банка в сети Интернет, доступ к которому осуществляется по ссылке из SMS-сообщения по адресу <https://anketa.alfabank.ru/ONLC/rb-sign-ui/>, посредством которого с применением Простой электронной подписи в соответствии с настоящими Правилами Клиент может оформить и подписать определенные Банком Электронные документы Клиента

Ключ Простой электронной подписи (Ключ) – известная только Владельцу Ключа последовательность цифровых символов, предназначенная для формирования Простой электронной подписи, полученная Владельцем Ключа в виде Одноразового пароля.

Одноразовый пароль – известная только Владельцу Ключа последовательность цифровых символов, направленных Банком на Номер телефона Клиента.

Простая электронная подпись (ПЭП) – простая электронная подпись, отвечающая требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Электронный документ Клиента – в целях настоящих Правил это Электронный документ, подписанный Владельцем Ключа от имени Клиента Простой электронной подписью, сформированной с применением Ключа, принадлежащего этому Владельцу Ключа.

Электронный журнал – взаимосвязанный набор электронных записей, отражающий действия Владельца Ключа при подписании Электронного документа Клиента. Электронный журнал хранится в Банке. Данные, полученные из информационных систем Банка, в том числе, из Электронных журналов, являются подтверждением подлинности Простой электронной подписи Владельца Ключа на подписанных Электронных документах Клиента.

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила устанавливают порядок подписания Клиентами Электронных документов Простой электронной подписью, а также порядок обмена с Банком Электронными документами:

- 1) в целях заключения Клиентом с Банком Генерального Соглашения (включая соглашение об использовании Простой электронной подписи на условиях, предусмотренных настоящими Правилами);
 - 2) в целях заключения Клиентом с Банком Депозитарного Договора одновременно с заключением Генерального Соглашения;
 - 3) при подписании Клиентом Соглашения на обработку персональных данных;
- в случаях, когда заключение указанных выше договоров (соглашений) и подписание указанных выше документов осуществляется Клиентом до заключения иных соглашений с Банком.

2.2. Подписание Клиентом Простой электронной подписью Генерального Соглашения, приложением к которому являются настоящие Правила, означает подписание Клиентом соглашения об использовании Простой электронной подписи, условия которого определены настоящими Правилами.

2.3. Настоящие Правила не регулируют подписание Электронных документов и обмен ими после заключения между Клиентом и Банком Генерального Соглашения и Депозитарного Договора. Последующий обмен Электронными документами регламентируется соответствующими положениями Генерального Соглашения, Депозитарного Договора и/или иными соглашениями между Банком и Клиентом.

2.4. Перед подписанием Электронного документа Владелец Ключа обязан ознакомиться с Электронным документом и быть согласным с его содержанием в полном объеме.

2.5. Формирование Простой электронной подписи осуществляется Владельцем Ключа с использованием Ключа. Настоящим Владельца Ключа соглашается использовать Ключ для подписания Электронных документов Клиента своей Простой электронной подписью.

2.6. Простая электронная подпись Владельца Ключа удостоверяет факт подписания Электронного документа Клиента Владельцем Ключа.

2.7. Простая электронная подпись Владельца Ключа содержится в самом Электронном документе Клиента. Простая электронная подпись Владельца Ключа содержит сведения, указывающие на Владельца Ключа, подписавшего Электронный документ Клиента, (фамилия, имя и отчество (если оно имеется)), дату и время подписания Электронного документа Клиента.

2.8. Для проверки Простой электронной подписи Владельца Ключа используются программно-технические и иные средства Банка. Банк отказывает в приеме Электронного документа Клиента в случае отрицательного результата проверки Простой электронной подписи Владельца Ключа.

2.9. Факт создания Электронного документа Клиента, подписанного Простой электронной подписью Владельца Ключа, а также факт и результат проверки Простой электронной подписи Владельца Ключа и иные действия Банка и Клиента фиксируются в Электронных журналах.

2.10. Клиент вправе получить в Банке копию подписанного Владельцем Ключа Электронного документа Клиента на бумажном носителе, на которой отображаются сведения о подписании Электронного документа Клиента Простой электронной подписью Владельца Ключа, и проставляется штамп Банка «копия верна» и собственноручная подпись работника Банка.

2.11. Владелец Ключа обязан:

- подписывать Электронные документы Клиента Простой электронной подписью Владельца Ключа в соответствии с настоящими Правилами только лично и только в присутствии работника Банка;
- хранить в тайне Ключ, принимать все возможные меры, предотвращающие нарушение его конфиденциальности;
- в случае нарушения конфиденциальности/компрометации Ключа, незамедлительно обратиться с соответствующим заявлением в Банк.

2.12. Нарушением конфиденциальности/компрометацией Ключа считается:

- утрата Владельцем Ключа Номера телефона Владельца Ключа;
- получение Ключа и/или возможности формировать Ключ третьими лицами с ведома или без ведома Владельца Ключа.

2.13. Клиент признает и соглашается с тем, что существуют риски нарушения конфиденциальности данных, используемых Банком для идентификации и аутентификации Клиента, а также Ключа.

2.14. Клиент несет ответственность, в том числе гражданско-правовую, за негативные последствия, наступившие в результате несоблюдения Клиентом обязанностей, установленных настоящими Правилами.

2.15. Банк не несет ответственности:

- за недоставку SMS-сообщения на Номер телефона Владельца Ключа, в случае если это обусловлено причинами, не зависящими от Банка;
- за возможные убытки, причиненные Клиенту в результате исполнения Банком Электронных документов Клиента, подписанных Простой электронной подписью Владельца Ключа.

2.16. Электронные документы Клиента, подписанные в Интернет-канале Простой электронной подписью Владельца Ключа, после положительных результатов проверки Ключа, введенного Владельцем Ключа в соответствии с настоящими Правилами, признаются Банком и Клиентом равнозначными документам на бумажном носителе, подписанными собственноручной подписью Клиента, удовлетворяют требованию совершения сделки в простой письменной форме в соответствии с Гражданским кодексом Российской Федерации, и влекут аналогичные им юридические последствия.

2.17. Предпринятые Банком меры электронной защиты не гарантируют абсолютную защиту информации от повреждения или перехвата, а также от иных возможных негативных последствий. Клиент признает и соглашается с тем, что существуют риски, связанные с передачей информации в электронном виде, в том числе риск неуполномоченного использования третьими лицами персональных данных, используемых в целях идентификации и аутентификации Клиента, нарушения конфиденциальности Ключа и использования Ключа третьими лицами.

3 ОСОБЕННОСТИ ФОРМИРОВАНИЯ И ПОДПИСАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

3.1. Для ознакомления с Электронными документами Клиента на Номер телефона Владельца Ключа поступает уведомление в виде SMS-сообщения, содержащее уникальную ссылку для доступа в Интернет-канал в целях ознакомления в нем Владельца Ключа с содержанием Электронного документа Клиента и для его последующего подписания Простой электронной подписью Владельца Ключа. Ссылка для доступа в Интернет-канал является персональной для конкретного Владельца Ключа. Владелец Ключа не вправе сообщать реквизиты ссылки или пересылать ссылку на Интернет-канал из SMS-сообщения третьим лицам. Направленная в SMS-сообщении ссылка для доступа в Интернет-канал прекращает действовать по факту подписания Владельцем Ключа своей Простой электронной подписью Электронного документа Клиента, либо при отмене заявки работником Банка в случае отказа Владельца Ключа от подписания Электронного документа Клиента.

3.2. По указанной в предыдущем пункте настоящих Правил ссылке Владелец Ключа переходит к началу процесса подписания Электронного документа Клиента.

3.3. Владельцу Ключа отображается сформированный Банком на основании его волеизъявления проект Электронного документа Клиента, с которым он обязан ознакомиться. Ознакомившись с проектом Электронного документа Клиента, Владелец Ключа может подписать его своей Простой электронной подписью или отказаться от подписания.

3.4. По отдельным видам Электронных документов Клиента до отображения Владельцу Ключа сформированного Банком проекта Электронного документа Клиента, Банк направляет на Номер телефона Владельца Ключа SMS-сообщение с Одноразовым паролем для верификации и аутентификации в Интернет-канале. В этом случае Владельцу Ключа отображается сформированный Банком на основании его волеизъявления проект Электронного документа Клиента, с которым он обязан ознакомиться, только после успешной проверки Банком этого Одноразового пароля.

3.5. После ознакомления Владельца Ключа с Электронным документом Клиента Банк направляет ему на Номер телефона сотовой связи Владельца Ключа Одноразовый пароль для подписания Электронного документа Клиента в Интернет-канале. Данный Одноразовый пароль является Ключом Простой электронной подписи Владельца Ключа. Одноразовый пароль вводится Владельцем Ключа самостоятельно в экранной форме Интернет-канала после ознакомления и согласия с содержанием Электронного документа Клиента.

3.6. Проверка ПЭП Владельца Ключа и факта подписания Электронных документов Клиента Владельцем Ключа осуществляется по Ключу. Проверка ПЭП Владельца Ключа и факта подписания Электронных документов Клиента Владельцем Ключа считается успешной, в случае если Ключ, введенный Владельцем Ключа в соответствующем поле Интернет-канала, совпал с Ключом, направленным Банком на Номер телефона Владельца Ключа, и срок действия Ключа не истек. При выполнении указанных условий операция не подлежит оспариванию Клиентом.

3.7. Ключом Простой электронной подписи Клиента является Одноразовый пароль, формируемый и направляемый Банком в составе SMS-сообщения на Номер телефона Владельца Ключа.

3.8. В случае отрицательного результата проверки Простой электронной подписи Владельца Ключа Клиент вправе также оформить и подписать равнозначный документ на бумажном носителе в установленном в Банке порядке.

4 ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ КЛИЕНТА, ПОДПИСАННЫЕ ПЭП ВЛАДЕЛЬЦА КЛЮЧА:

4.1. Клиент соглашается использовать Ключ, полученный Владельцем Ключа от Банка, для подписания Электронных документов Клиента ПЭП Владельца Ключа.

4.2. Формирование ПЭП осуществляется Владельцем Ключа с использованием Ключа.

4.3. ПЭП Владельца Ключа применяется для удостоверения факта подписания Электронного документа Клиента Владельцем Ключа.

4.4. Для проверки Ключа и для формирования ПЭП Владельца Ключа используются программно-технические средства Банка. Банк отказывает Клиенту в подписании Электронного документа Клиента ПЭП Владельца Ключа в случае отрицательного результата проверки Ключа.

4.5. Факт создания и направления Клиенту Электронного документа Клиента, подписание Электронного документа Клиента ПЭП Владельца Ключа, результаты проверки ПЭП Владельца Ключа/ Ключа и иные действия Банка и Клиента фиксируются в Электронном журнале.

5 СРОК ДЕЙСТВИЯ ПРАВИЛ И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ПРАВИЛА

5.1. Настоящие Правила действуют в течение неопределенного срока.

5.2. Настоящие Правила вступают в силу с момента подписания Клиентом Электронного документа, содержащего ссылку на настоящие Правила. При подписании Владельцем Ключа Электронного документа Клиента Владелец Ключа подтверждает ознакомление и согласие с настоящими Правилами.

5.3. Изменения и дополнения в настоящие Правила вносятся в порядке, предусмотренном для внесения изменений и дополнений в Регламент.

6 ПОРЯДОК РАССМОТРЕНИЯ СПОРОВ

6.1. Споры, связанные с установлением подлинности Электронных документов, разрешаются в установленном в Банке порядке. При разрешении споров, разногласий или конфликтных ситуаций Электронные документы могут предъявляться при рассмотрении спорных ситуаций, в том числе, в суде, в качестве доказательств.

6.2. Все споры, разногласия или требования, связанные с установлением подлинности Электронного документа Клиента, разрешаются на основании обращения Клиента в Банк с указанием реквизитов оспариваемого Электронного документа Клиента.

6.3. В случае возникновения споров, связанных с формированием и подписанием Электронного документа Клиента, Банк вправе запрашивать у Клиента все необходимые для рассмотрения обращения Клиента документы и(или) информацию, а Клиент обязуется представлять их в Банк.

6.4. Банк по факту получения обращения Клиента проводит проверку на наличие в информационных системах Банка сведений, указанных в п. 6.6 настоящих Правил.

6.5. Результат рассмотрения обращения доводится Банком до Клиента в установленном в Банке порядке.

6.6. При рассмотрении споров Банк самостоятельно определяет, в том числе следующее:

– предмет разногласий на основании обращения Клиента;

- операцию, относящуюся к предмету разногласий;
- факт ввода верного Ключа;
- дата и время ввода Ключа;
- введенный Ключ прошел проверку на правильность с положительным результатом, а именно: Одноразовый пароль был направлен на Номер телефона Владельца Ключа и время его ввода не истекло.

6.7. При отсутствии согласия Сторон спор между Банком и Клиентом – юридическим лицом или индивидуальным предпринимателем подлежит рассмотрению в Арбитражном суде города Москвы.

При отсутствии согласия спор между Банком и Клиентом – физическим лицом подлежит рассмотрению в Мещанском районном суде города Москвы. В случае если в соответствии с гражданским процессуальным законодательством РФ спор подсуден мировому судье, то он подлежит рассмотрению мировым судьей судебного участка № 381 Красносельского района г. Москвы.