РЕГЛАМЕНТ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ БАНКА «НЕЙВА» ООО

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем «Регламенте взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО» (далее - Регламент) термины и определения имеют следующие значения:

Аутентификация – процедура проверки подлинности ЭП в ЭД путем установления принадлежности участнику корпоративной ИС предъявляемых им средств подтверждения ЭД (ключа электронной подписи) в целях подтверждения его прав на доступ в корпоративную ИС и на обмен ЭД от имени Клиента .

Владелец ключа ЭП — физическое лицо, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи, используемый для обмена электронными документами, подтвержденными усиленной электронной подписью, и\или предоставлены средства подтверждения для формирования в электронном документе простой электронной подписи.

Владелец корпоративной ИС - БАНК «НЕЙВА» ООО (далее — Банк).

Владелец сертификата — физическое лицо, на имя которого сертификационным центром выдан сертификат ключа проверки ЭП.

Динамический пароль — OTP-код (One Time Password) - одноразовый пароль в виде последовательности числовых символов, предоставляемый Банком по запросу участника корпоративной ИС посредством SMS-уведомления на мобильный телефон и/или e-mail - сообщения на электронный адрес, указанный Клиентом, введение которого требуется для получения доступа в корпоративную ИС и/или подтверждения ЭД простой электронной подписью.

Договор комплексного банковского обслуживания физических лиц — договор между Банком и участником корпоративной ИС - физическим лицом, предусматривающий оказание Банком услуг комплексного банковского обслуживания физическим лицам, в том числе предоставление услуг обмена электронными документами посредством корпоративной ИС.

Идентификация – процедура присвоения участникам корпоративной ИС уникальных идентификаторов, позволяющих однозначно определить каждого участника корпоративной ИС и/или сопоставление предъявляемого участником корпоративной ИС уникального идентификатора с перечнем зарегистрированных в корпоративной ИС действительных уникальных идентификаторов с целью однозначного установления обращающегося участника корпоративной ИС.

Ключевой носитель – бумажный, электронный носитель информации, на котором записана ключевая информация.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для установления авторства и проверки подлинности электронной подписи.

Компрометация ключа — наличие оснований полагать, что доверие к тому, что используемые ключи электронной подписи обеспечивают безопасность информации, утрачено. К событиям, связанным с компрометацией ключей электронной подписи относятся, включая, но не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;
- утеря, передача третьим лицам мобильного телефона, SIM-карты с абонентским номером, который используется для направления динамического пароля посредством SMS-уведомлений;
- наличие подозрений, что средства подтверждения ЭД стали известны третьим лицам;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- несанкционированное копирование (подозрение на копирование);
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).

Корпоративная информационная система БАНКА «НЕЙВА» ООО (далее - корпоративная ИС) это совокупность технического, программного и организационного обеспечения, предназначенная для реализации возможности создания, передачи, приема, проверки, обработки и защиты электронных документов, участниками которой может быть ограниченный круг лиц, определенный владельцем корпоративной ИС.

Корпоративный клиент (Клиент) — юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством РФ порядке частной практикой, иностранная структура без образования юридического лица, обслуживающиеся в Банке в рамках договоров, предусматривающих обмен электронными документами.

Лимиты на совершение операций — установленные ограничения сумм или количества операций по банковскому счету или по банковской карте.

Логин (Уникальный идентификатор) - имя учетной записи, уникальная последовательность буквенно-цифровых символов, используемая совместно со статическим паролем для аутентификации участника корпоративной ИС и предоставления определенных прав доступа в корпоративную ИС.

Отзыв сертификата ключа проверки ЭП - необратимая операция, при которой ключ электронной подписи признается недействительным, а владелец сертификата ключа проверки ЭП утрачивает возможность принимать участие в обмене ЭД в корпоративной ИС с данным ключом электронной подписи. Сертификаты ключей проверки ЭП хранятся в течение всего срока хранения ЭД, для подтверждения подлинности которых они могут быть использованы.

Операция по банковскому счету — перевод денежных средств по банковскому счету, внесение Клиентом наличных денежных средств на свой банковский счет, получение Клиентом наличных денежных средств со своего банковского счета.

Операция по банковской карте — осуществление операции с использованием банковской карты либо ее реквизитов.

Подтверждение подлинности простой электронной подписи в ЭД - положительный результат аутентификации - проверки принадлежности электронной подписи в ЭД участнику корпоративной ИС путем сопоставления предъявляемых участником корпоративной ИС средств подтверждения участника корпоративной ИС на момент получения Банком ЭД со средствами подтверждения, которые соответствуют оспариваемому ЭД.

Подтверждение подлинности усиленной электронной подписи в ЭД - положительный результат аутентификации - проверки соответствующим средством электронной подписи с использованием сертификата ключа проверки ЭП принадлежности электронной подписи в ЭД участнику корпоративной ИС (владельцу сертификата) и отсутствия искажений в подписанном данной электронной подписью ЭД.

Порядок - порядок разрешения конфликтных ситуаций при обмене ЭД (Приложение 1 к настоящему Регламенту).

Простая электронная подпись - электронная подпись, которая содержится в самом ЭД и создана посредством использования кодов, паролей, иных средств подтверждения факта формирования электронной подписи определенным лицом.

Сертификат ключа проверки электронной подписи (сертификат ключа проверки ЭП) - электронный документ или документ на бумажном носителе, выданный сертификационным центром, и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификационный центр - организационная структура Банка, предназначенная для управления единой инфраструктурой ключей проверки электронной подписи с целью обеспечения юридической значимости электронных документов и контроля целостности информации, защищенной усиленной электронной подписью.

Согласительная комиссия - комиссия, создаваемая для разрешения разногласий, возникающих при обмене ЭД.

Средство подтверждения ЭД (ключ электронной подписи) – уникальная последовательность символов, позволяющая создавать электронную подпись для подтверждения ЭД. В качестве средства подтверждения ЭД в корпоративной ИС используются: для создания простой электронной подписи – статический пароль, динамический пароль; для создания усиленной электронной подписи — ключ усиленной электронной подписи.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Статический пароль - секретная последовательность буквенно-цифровых символов, соответствующая присвоенному ему логину, и использующаяся для удостоверения правомочности обращения участника корпоративной ИС в корпоративную ИС.

Тарифы Банка:

- ТАРИФЫ БАНКА «НЕЙВА» ООО за услуги, оказываемые в рублях и иностранной валюте, юридическим лицам (кроме кредитных организаций), индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством РФ порядке частной практикой;

- ТАРИФЫ БАНКА «НЕЙВА» ООО на услуги, оказываемые в рублях юридическим лицам, индивидуальным предпринимателям, в отношении которых введена процедура банкротства, применяемая в деле о банкротстве;

- ТАРИФЫ БАНКА «НЕЙВА» ООО на услуги, оказываемые в рублях , платежным агентам, банковским платежным агентам и поставщикам услуг.

Уведомления через корпоративную ИС — сообщение, направляемое Банком посредством корпоративной ИС, и содержащее в себе информацию об операции, совершаемой по счету Клиента.

Усиленная электронная подпись - электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

- позволяет определить лицо, подписавшее ЭД;

- позволяет обнаружить факт внесения изменений в ЭД после момента его подписания;

- создается с использованием средств электронной подписи.

Участник корпоративной ИС – для целей настоящего Регламента следующие лица:

– Корпоративный клиент, заключивший с Банком Договор «Об обмене электронными документами с использованием электронной цифровой подписи» (до 30.11.2011г. включительно) либо Договор «Об обмене электронными документами с использованием электронной подписи» (начиная с 01.12.2011г.) (далее – Договор);

– физическое лицо - уполномоченный представитель Корпоративного клиента, владелец ключа ЭП, заключивший с Банком Соглашение о присоединении к «Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО» по форме Приложения N2 к настоящему Регламенту (далее – Соглашение).

Электронный документ (ЭД) – документ в электронной форме, подтвержденный электронной подписью, обеспечивающий юридически значимый обмен информацией между Банком и Клиентом, в том числе являющийся основанием для совершения Банком операций по банковскому счету по поручению Клиента.

Электронная подпись (далее — ЭП) - реквизит ЭД, информация в электронной форме, которая присоединена к подписываемому ЭД (или иным образом связана с ЭД), и используется для определения лица, подписывающего ЭД.

В соответствии с Федеральным законом от 06.04.2011 N63-ФЗ «Об электронной подписи» (далее – Федеральный закон N63-ФЗ) и настоящим Регламентом для подтверждения ЭД в корпоративной ИС применяются простая электронная подпись и усиленная электронная подпись.

E-mail-уведомление - электронное сообщение, направляемое Банком на адрес электронной почты Клиента в сети Интернет, и содержащее в себе информацию об операции, совершаемой по Счету Клиента.

SMS-уведомление - сообщение, направляемое Банком через оператора сотовой связи на номер мобильного телефона, указанный Клиентом и содержащее в себе информацию об операции, совершаемой по счету, информацию о паролях для доступа в Корпоративную ИС или информацию о кодах, паролях и иных средствах подтверждения, необходимых для формирования простой электронной подписи в электронном документе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1.Настоящий Регламент разработан в соответствии с действующим законодательством Российской Федерации.

2.2. Настоящий Регламент определяет правила взаимодействия участников корпоративной ИС с владельцем корпоративной ИС, включая их права, обязанности и ответственность, основные организационно-технические мероприятия, направленные на осуществление обмена электронными документами между владельцем и участниками корпоративной ИС.

2.3. Для Клиентов, заключивших до даты введения в действие настоящего Регламента «Договор об обмене электронными документами с использованием электронной подписи», Договор «Об обмене электронными документами с использованием электронной цифровой подписи» настоящий Регламент является новой редакцией Регламента взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО.

2.4. Настоящий Регламент является общедоступным и размещается в форме электронного документа на информационном web-сайте Банка в сети Интернет по адресу: www.neyvabank.ru (далее – информационный сайт Банка).

2.5. Присоединение участника корпоративной ИС к настоящему Регламенту осуществляется в соответствии со статьей 428 Гражданского кодекса Российской Федерации путем:

- заключения Договора «Об обмене электронными документами с использованием электронной подписи» между Банком и Клиентом

- заключения Соглашения о присоединении к «Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО» по форме Приложения №2 к настоящему Регламенту между Банком и физическим лицом, уполномоченным представителем Корпоративного клиента — участника корпоративной ИС.

2.6. Присоединение участника корпоративной ИС к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент заключения соответствующего договора/соглашения, а также дальнейших изменений (дополнений), вносимых в Регламент в соответствии с условиями настоящего Регламента.

2.7. Деятельность Банка по управлению единой инфраструктурой ключей проверки электронной подписи с целью обеспечения юридической значимости электронных документов и контроля целостности информации, защищённой усиленной электронной подписью осуществляется на основании Лицензий ФСБ России в соответствии с действующим законодательством Российской Федерации и настоящим Регламентом.

2.8. Сертификационный центр Банка реализован на базе программно-аппаратного комплекса обеспечения «Notary-PRO v2.7» разработки ЗАО «Сигнал-КОМ» г. Москва (сертификат ФСБ России СФ/128-2560 от 06.11.2014).

2.9. В сертификационном центре применяется средства криптографической защиты информации (СКЗИ) «Крипто-КОМ v 3.3». Заключение ФСБ России № 149/3/2/2-1269 от 21.07.2014 г. Разработчик ЗАО «Сигнал-КОМ» г.Москва.

2.10. Владелец корпоративной ИС устанавливает типы устройств хранения электронной подписи, порядок использования видов электронной подписи при обмене ЭД в корпоративной ИС, в том числе путем установления ограничений на использование конкретных видов электронной подписи участниками корпоративной ИС или для подтверждения определенной категории ЭД/определенного вида операций, а также путем установления соответствующих лимитов на совершение операций на основании ЭД Клиента. Лимиты на совершение операций, подтвержденных простой электронной подписью, устанавливаются в одностороннем порядке владельцем корпоративной ИС и публикуются на информационном сайте Банка.

2.11. Участник корпоративной ИС при обмене ЭД вправе использовать как усиленную, так и простую электронную подпись для подтверждения ЭД с учетом установленных владельцем корпоративной ИС ограничений для отдельных категорий ЭД.

Участник корпоративной ИС – уполномоченный представитель Корпоративного клиента вправе подключить простую электронную подпись для подтверждения ЭД только при наличии у него сгенерированных ключей усиленной электронной подписи.

2.12. Владелец и участники корпоративной ИС признают достаточной для защиты от несанкционированного доступа и подтверждения авторства и подлинности ЭД используемую ими при взаимодействии в рамках корпоративной ИС систему защиты информации, обеспечивающую аутентификацию участника корпоративной ИС, установление подлинности ЭД, а также контроль целостности ЭД в случае использования усиленной электронной подписи.

2.13. Участники корпоративной ИС признают юридическую силу ЭД, подписанных электронной подписью, в том числе простой электронной подписью, при положительном результате аутентификации, равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями законодательства РФ.

2.14. Физическое лицо - участник корпоративной ИС может являться владельцем только одного действительного сертификата ключа проверки ЭП для работы в корпоративной ИС.

2.15. Физическое лицо - владелец сертификата ключа проверки ЭП может одновременно являться клиентом Банка в рамках «Договора комплексного банковского обслуживания физических лиц» и уполномоченным представителем неограниченного круга Корпоративных Клиентов Банка в соответствии с предоставленными ему полномочиями.

2.16. В случае, если на момент присоединения физического лица — уполномоченного представителя Корпоративного клиента к настоящему Регламенту на основании заключенного им Соглашения, указанное физическое лицо уже является владельцем сертификата, выданного в соответствии с Договором комплексного банковского обслуживания физических лиц, изготовление нового сертификата ключа проверки ЭП в соответствии с настоящим Регламентом не осуществляется, обмен электронными документами в рамках Договора и Соглашения осуществляется с использованием ранее полученной усиленной электронной подписи.

3. УСЛУГИ, ПРЕДОСТАВЛЯЕМЫЕ БАНКОМ В РАМКАХ НАСТОЯЩЕГО РЕГЛАМЕНТА

3.1.Банк предоставляет следующие услуги в рамках обмена ЭД, подтверждаемыми простой электронной подписью:

3.1.1. присвоение уникального идентификатора (логина) — участнику корпоративной ИС, согласно порядка предоставления ключа простой ЭП; предоставление средства подтверждения ЭД - ключа простой электронной подписи (логин и статический пароль, динамический пароль);

3.1.2. временное ограничение прав доступа, временное блокирование доступа к ресурсам корпоративной ИС;

3.1.3. отмена временного ограничения прав доступа, отмена временного блокирования доступа к ресурсам корпоративной ИС;

3.1.4. признание средств подтверждения ЭД недействительными;

3.1.5. ведение электронного журнала реестра уникальных идентификаторов участников корпоративной ИС, соответствующих им средств подтверждения, обеспечение его актуальности;

3.1.6.осуществление по обращениям участников корпоративной ИС подтверждения подлинности электронной подписи в ЭД в отношении зарегистрированных в корпоративной ИС уникальных идентификаторов и соответствующих средств подтверждения.

3.1.7. совершение операций по банковскому счету на основании распоряжений участника корпоративной ИС, направляемых с использованием корпоративной ИС;

3.1.8. обмен электронными документами между Банком и Клиентом с помощью корпоративной ИС в рамках заключенных договоров и соглашений.

3.2. Банк предоставляет следующие услуги в рамках обмена ЭД, подтверждаемыми усиленной электронной подписью:

3.2.1. изготовление сертификатов ключей проверки ЭП;

3.2.2. временное ограничение прав доступа, временное блокирование доступа к ресурсам корпоративной ИС;

3.2.3. отмена временного ограничения прав доступа, отмена временного блокирования доступа к ресурсам корпоративной ИС;

3.2.4. отзыв сертификатов ключей проверки ЭП;

3.2.5. ведение реестра сертификатов ключей проверки ЭП и обеспечение его актуальности;

3.2.6. проверка уникальности ключей проверки электронной подписи в реестре сертификатов ключей проверки ЭП и архиве сертификационного центра;

3.2.7. выдача сертификатов ключей проверки ЭП в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

3.2.8.осуществление по обращениям участников корпоративной ИС подтверждения подлинности электронной подписи в электронных документах в отношении выданных им сертификатов ключей проверки ЭП.

3.2.9. совершение операций по банковскому счету на основании распоряжений участника корпоративной ИС, направляемых с использованием корпоративной ИС;

3.2.10. обмен электронными документами между Банком и участником корпоративной ИС с помощью корпоративной ИС в рамках заключенных договоров и соглашений.

4. ПОРЯДОК РЕГИСТРАЦИИ УЧАСТНИКА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

4.1.Для регистрации в корпоративной ИС Банка Корпоративного клиента, уполномоченный представитель Корпоративного клиента должен:

4.1.1.обратиться в офис Банка с документами, подтверждающими полномочия и удостоверяющими личность;

4.1.2.ознакомиться с Тарифами Банка;

4.1.3.ознакомиться с настоящим Регламентом, включая указанные в разделе 16 настоящего Регламента условия использования, ограничения способов и мест использования корпоративной ИС Банка, а также случаи повышенного риска использования корпоративной ИС Банка, и присоединиться к нему путем заключения с Банком Договора «Об обмене электронными документами с использованием электронной подписи»;

4.1.4.предоставить «Список уполномоченных лиц для осуществления обмена ЭД» в порядке, приведенном в Договоре.

4.2. Для регистрации в корпоративной ИС Банка участника корпоративной ИС - уполномоченного на обмен ЭД представителя Корпоративного клиента, представитель Корпоративного клиента должен:

4.2.1.обратиться в офис Банка с документами, удостоверяющими личность;

4.2.2.ознакомиться с настоящим Регламентом, включая условия использования, ограничения способов и мест использования корпоративной ИС Банка, а также случаи повышенного риска использования корпоративной ИС Банка и присоединиться к нему путем заключения с Банком Соглашения о присоединении к «Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА»;

4.2.3.оформить запрос на выпуск сертификата ключа проверки ЭП в соответствии с разделом 6 настоящего Регламента.

4.3.Банк осуществляет регистрацию участника в корпоративной ИС Банка не позднее 1 (одного) рабочего дня с даты заключения соответствующего договора/соглашения.

5. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ КЛЮЧА ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Подтверждение ЭД электронной подписью Клиента осуществляется с помощью средств подтверждения, перечень и порядок использования которых для различных способов аутентификации, устанавливается Банком.

5.2. В качестве средства подтверждения ЭД простой электронной подписью используется логин и статический пароль, а также динамический пароль.

5.2.1. Участник корпоративной ИС — уполномоченный представитель корпоративного клиента - для использования простой электронной подписи самостоятельно создает логин и статический пароль в Корпоративной ИС, а также указывает номер мобильного телефона, на который Банком будет направляться динамический пароль для подтверждения операций в Корпоративной ИС.

5.2.2. Статический пароль имеет срок действия, который Корпоративный Клиент устанавливает самостоятельно при создании статического пароля в Корпоративной ИС.

5.2.3.Динамический пароль автоматически генерируется корпоративной ИС, в т.ч в целях дополнительной аутентификации участника корпоративной ИС (уполномоченного представителя Корпоративного клиента) при предоставлении ему доступа в корпоративную ИС и/или подтверждения ЭД, и направляется корпоративному Клиенту на указанный Клиентом номер мобильного телефона в настройках корпоративной ИС. Участник корпоративной ИС должен ввести полученный динамический пароль для прохождения процедуры аутентификации/ или подтверждения ЭД. Участник корпоративной ИС может самостоятельно изменить номер мобильного телефона средствами корпоративной ИС для изменения канала получения динамического пароля.

5.2.4.Банк вправе без уведомления участника корпоративной ИС временно заблокировать доступ к ресурсам корпоративной ИС с тем или иным средством подтверждения ЭД (ключом электронной подписи) при наличии у Банка оснований полагать, что произошла компрометация ключей и возможна попытка несанкционированного доступа в корпоративную ИС от имени Клиента. Возобновление доступа участнику корпоративной ИС, в данном случае, осуществляется Банком только после замены Клиентом средств подтверждения ЭД.

6. ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

6.1. Для получения сертификата ключа проверки ЭП для осуществления обмена ЭД, подтвержденными усиленной электронной подписью, участник корпоративной ИС должен:

6.1.1. обратиться в офис Банка с документами, удостоверяющими личность;

6.1.2. создать собственноручно с помощью инструментальных средств корпоративной ИС запрос на выпуск сертификата ключа проверки ЭП в электронном виде, а также предоставить в Банк данный запрос на бумажном носителе, заверенный собственноручной подписью. При выполнении регистрации участник корпоративной ИС сообщает Банку секретную комбинацию «вопрос — ответ», которая в дальнейшем может быть использована участником корпоративной ИС для блокирования доступа к ресурсам корпоративной ИС.

6.2. При поступлении в Банк запроса на выпуск сертификата ключа проверки ЭП в электронном виде, Банк сверяет данные, содержащиеся в указанном запросе в электронном виде с данными, указанными в запросе, представленном на бумажном носителе. При обнаружении каких-либо несоответствий- процедура выпуска сертификата не производится.

При отсутствии - Банк обрабатывает поступивший запрос и осуществляет выпуск сертификата ключа проверки ЭП. Выпущенный сертификат размещается в корпоративной ИС.

6.3. Изготовление сертификатов ключей проверки ЭП осуществляется на основании запроса физического лица - участника корпоративной ИС, который содержит сведения, необходимые для идентификации владельца сертификата ключа проверки ЭП и передачи ему сообщений. Запрос на выпуск сертификата формируется физическим лицом — участником корпоративной ИС самостоятельно с помощью программного обеспечения, входящего в состав корпоративной ИС, и представляет собой следующий набор информации:

6.3.1. запрашиваемые ФИО физического лица - участника корпоративной ИС;

6.3.2. запрашиваемый номер Соглашения с уполномоченным представителем Корпоративного клиента и, в случае, если участник корпоративной ИС на момент формирования запроса на выпуск сертификата является стороной действующего договора комплексного банковского обслуживания физических лиц с Банком, № такого договора;

6.3.3. проверочный код запроса;

6.3.4. информация о ключе проверки электронной подписи, включающая идентификатор алгоритма и собственно ключ проверки электронной подписи.

6.4. Данная информация подписывается ключом подписи владельца сертификата ключа проверки ЭП, при этом запрос является самоподписанным, т.е. подписанным ключом электронной подписи, парным ключу проверки электронной подписи, включённому в запрос.

Содержащиеся в запросе сведения подтверждаются предъявлением соответствующих документов.

6.5. За услуги по выдаче сертификатов ключей проверки ЭП, зарегистрированных сертификационным центром, одновременно с информацией об их действии в форме электронных документов отдельная плата не взимается.

6.6. Банк формирует сертификат ключа проверки ЭП путём заверения электронной подписью собственного сертификационного центра набора данных, включающих следующую информацию:

6.6.1. серийный номер сертификата;

6.6.2. номер соглашения о присоединении к настоящему Регламенту и, в случае, если участник корпоративной ИС на момент формирования запроса на выпуск сертификата является стороной действующего договора комплексного банковского обслуживания физических лиц, номер такого договора;

6.6.3. идентификатор алгоритма, используемого для подписи;

6.6.4. параметры сертификата издателя;

6.6.5. период действия сертификата, состоящий из двух дат: начала и конца периода;

6.6.6. ФИО владельца сертификата ключа проверки ЭП;

6.6.7. информацию о ключе проверки электронной подписи: идентификатор алгоритма и собственно ключ проверки электронной подписи.

6.7. При формировании сертификатов применяется криптографический алгоритм ГОСТ Р 34.10-2001.

6.8. Сертификаты ключа проверки ЭП формируются на основе знания ключей проверки электронной подписи владельцев сертификата ключа проверки ЭП. Ключи проверки электронной подписи предоставляются Банку в виде запросов на выпуск сертификатов.

6.9. Ключи проверки электронной подписи сертификационного центра Банка выпускаются каждый год со сроком действия сертификата ключа проверки электронной подписи 3 (три) года. После выпуска ключа сертификационного центра Банка все запросы физических лиц - участников корпоративной ИС подписываются новым ключом электронной подписи.

6.10. Ключ усиленной электронной подписи имеет ограниченный срок действия (1 год), однако любой сертификат ключа проверки ЭП может быть отозван до истечения этого периода в случае:

6.10.1. компрометации ключа электронной подписи владельца сертификата ключа проверки ЭП соответствующего данному сертификату;

6.10.2. выбывания владельца сертификата из числа участников корпоративной ИС в результате расторжения им Соглашения, если он не является стороной действующего договора комплексного банковского обслуживания физических лиц;

6.10.3. получения владельцем сертификата ключа проверки ЭП нового сертификата;

6.10.4. компрометации ключа электронной подписи сертификационного центра Банка использованного при формировании сертификата ключа проверки ЭП.

6.11. По окончании процедуры выпуска сертификата, участник корпоративной ИС получает возможность, используя программные средства корпоративной ИС, удалённо завершить процедуру формирования ключа электронной подписи и приступить к его эксплуатации.

6.12. Сроки выпуска сертификатов ключа проверки ЭП определены в Договоре.

7. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВРЕМЕННОГО ПРИОСТАНОВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ (в т. ч. блокировки, ограничения прав доступа к ресурсам корпоративной информационной системы)

7.1.Участник корпоративной ИС самостоятельно устанавливает факт компрометации ключа (угрозы компрометации) и/или использования ключа электронной подписи без его согласия. В случае компрометации или при подозрении на компрометацию ключа электронной подписи, а также использования ключа электронной подписи без согласия участника корпоративной ИС требуется незамедлительно направить соответствующее сообщение Банку, после чего осуществляется блокирование прав доступа участнику корпоративной ИС к ресурсам корпоративной ИС с указанным ключом электронной подписи.

7.2.Для сообщения Банку о компрометации или подозрении на компрометацию ключа электронной подписи а также использования ключа электронной подписи без согласия участника корпоративной ИС:

7.2.1. Физическому лицу — уполномоченному представителю Корпоративного клиента (владельцу ключа ЭП) необходимо обратиться в контакт-центр Банка по телефонам, указанным в разделе 17 настоящего Регламента, при этом блокирование доступа к корпоративной ИС для данного участника корпоративной ИС - физического лица осуществляется в данном случае после его успешной аутентификации по комбинации секретный «вопрос — ответ», либо в любой офис Банка с соответствующим заявлением и документом, удостоверяющим личность;

7.2.2. Участнику корпоративной ИС – Корпоративному клиенту — обратиться непосредственно в любой офис Банка с соответствующим заявлением о блокировании доступа к корпоративной ИС уполномоченному представителю Корпоративного клиента (владельцу ключа ЭП) и документами, удостоверяющими личность и подтверждающими его полномочия.

7.3. Моментом получения Банком сообщения Клиента о факте компрометации или ее угрозе и/или использования ключа электронной подписи без согласия участника корпоративной ИС является:

7.3.1. При обращении участника корпоративной ИС по телефону в контакт-центр Банка - дата и время фиксации сообщения сотрудниками контакт-центра.

7.3.2. При предоставлении заявления в офис Банка - дата и время приема заявления сотрудником Банка.

7.4. Банк вправе без уведомления участника корпоративной ИС временно заблокировать доступ к ресурсам корпоративной ИС при наличии у Банка подозрений о факте компрометации ключей электронной подписи для предотвращения попыток несанкционированного доступа неуполномоченных лиц в корпоративную ИС от имени Клиента, несоблюдении участником корпоративной ИС требований к обмену ЭД и обеспечению информационной безопасности при обмене ЭД, предусмотренных законодательством РФ, условиями Регламента и Договора, указанного в п. 2.5. Регламента.

7.5.При отсутствии более 3-х месяцев операций по банковскому счету участника корпоративной ИС — Корпоративного клиента, Банк вправе временно ограничить доступ к ресурсам корпоративной ИС. При наличии у Клиента нескольких счетов в Банке ограничение доступа к ресурсам корпоративной ИС возможно только при отсутствии операций в течение указанного времени по всем счетам. Ограничение прав доступа к ресурсам корпоративной ИС предоставляет уполномоченным представителям Клиента право осуществлять только функции просмотра выписок по счету и сообщений, направленных Банком, просмотра и создания ЭД без права их подписания ЭП.

7.6. В случае непредставления или представления недостоверных сведений и документов, запрашиваемых Банком в целях выполнения требований законодательства Российской Федерации, нормативных актов Банка России, Банк вправе временно ограничить доступ к корпоративной ИС с сохранением функций, указанных в п. 7.5. настоящего Регламента. Возобновление доступа осуществляется Банком только после получения соответствующих сведений и документов.

7.7. Банк вправе отказать Клиенту в совершении операций с использованием системы удаленного управления счетом в случае выявления факта отсутствия по своему местонахождению Корпоративного клиента, его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени Корпоративного клиента без доверенности.

7.8. Банк вправе полностью или частично ограничить доступ Клиента к корпоративной ИС при наличии непогашенной в течение 15 календарных дней задолженности Клиента по оплате услуг Банка.

7.9. В целях недопустимости несанкционированного доступа в корпоративную ИС от имени Корпоративного клиента Банк вправе без уведомления участника корпоративной ИС временно заблокировать доступ к ресурсам корпоративной ИС участнику корпоративной ИС при неурегулированности вопроса о правах лиц по распоряжению счетом или при наличии сомнения Банка относительно прав лиц на распоряжение счетом, в том числе, когда о правах на распоряжение счетом заявляют несколько лиц (корпоративный конфликт). Возобновление доступа участнику корпоративной ИС, в данном случае, осуществляется Банком только после предоставления документов, которые Банк сочтет достаточными для разрешения всех противоречий и сомнений.

7.10. Окончание срока действия сертификата ключа проверки ЭП не влечет прекращения возможности обмена электронными документами с использованием простой ЭП в случае если владельцем сертификата ранее была подключена возможность использования простой ЭП. При этом изменение существующих настроек работы с простой ЭП возможно лишь при использовании усиленной электронной подписи. Прекращение использования простой ЭП не влечет прекращения возможности обмена ЭД с использованием усиленной ЭП.

8. ПОРЯДОК ОТМЕНЫ ОГРАНИЧЕНИЯ ПРАВ ДОСТУПА, ВРЕМЕННОЙ БЛОКИРОВКИ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ

8.1.Для отмены ограничения прав доступа или блокирования доступа к ресурсам корпоративной ИС участник корпоративной ИС должен обратиться непосредственно в один из офисов Банка с соответствующим заявлением и документом, удостоверяющим личность.

8.2.Банк отменяет ограничение прав доступа, снимает блокировку доступа к ресурсам корпоративной ИС для данного участника корпоративной ИС, при наличии у лица соответствующих прав на осуществление доступа к корпоративной ИС.

8.3.Банк отменяет ограничение прав доступа к ресурсам корпоративной ИС участника корпоративной ИС — Корпоративного клиента при предоставлении в Банк

заявления на бумажном носителе, подписанного уполномоченным представителем Корпоративного клиента (владельцем сертификата ключа проверки ЭП) и скрепленного печатью организации.

8.4. По окончании процедуры отмены блокировки доступа, участник корпоративной ИС сообщает Банку новую секретную комбинацию «вопрос-ответ».

8.5. Возобновление доступа к корпоративной ИС после блокирования по инициативе Банка в случае выявления факта компрометации ключей электронной подписи осуществляется по согласованию с Клиентом после замены соответствующих средств подтверждения ЭД, в т.ч. перевыпуска сертификата ключа проверки ЭП.

9. ПОРЯДОК ОТЗЫВА СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

9.1. При компрометации ключа усиленной электронной подписи и/или использования ключа усиленной электронной подписи без согласия участника корпоративной ИС участник корпоративной ИС - должен незамедлительно выполнить действия по блокированию доступа к ресурсам корпоративной ИС в соответствии с разделом 7 настоящего Регламента и/или отзыву сертификата ключа проверки ЭП.

9.2. Для осуществления отзыва сертификата ключа проверки ЭП владелец сертификата ключа проверки ЭП должен обратиться непосредственно в один из офисов Банка с заявлением на отзыв сертификата ключа проверки ЭП и документом, удостоверяющим личность.

9.3. После проведения идентификации личности участника корпоративной ИС - владельца сертификата ключа проверки ЭП Банк изменяет статус данного сертификата на «недействительный».

10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАНОВОГО ПЕРЕВЫПУСКА СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКОВ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

10.1.Плановая смена ключей инициируется участником корпоративной ИС - владельцем сертификата ключа проверки ЭП и проводится не ранее, чем за 30 календарных дней до даты окончания срока ключа электронной подписи, и не позднее двух рабочих дней до окончания срока его действия.

10.2.Физическое лицо - участник корпоративной ИС самостоятельно генерирует свой ключ электронной подписи и электронный запрос на изготовление нового сертификата ключа проверки ЭП. Идентификационные данные запроса на сертификат должны соответствовать ранее зарегистрированным в Банке идентификационным данным участника корпоративной ИС, запрос должен быть подписан действующим ключом электронной подписи данного участника корпоративной ИС.

10.3.Созданный запрос на выпуск нового ключа посредством инструментальных средств корпоративной ИС передается в Банк.

10.4.В Банке полученный запрос на выпуск сертификата ключа проверки ЭП обрабатывается и выпускается новый сертификат. Выпущенный сертификат ключа проверки ЭП размещается в корпоративной ИС для прохождения владельцем сертификата ключа проверки ЭП процедуры завершения формирования ключа электронной подписи.

10.5.По окончании процедуры выпуска сертификата ключа проверки ЭП, участник корпоративной ИС - владелец сертификата ключа проверки ЭП получает возможность,

используя программные средства корпоративной ИС, удалённо завершить процедуру формирования ключа электронной подписи и приступить к его эксплуатации.

11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНЕПЛАНОВОЙ ЗАМЕНЫ СЕРТИФИКАТОВ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКОВ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

11.1. Внеплановая смена ключей электронной подписи владельцев сертификата ключа проверки ЭП осуществляется:

11.1.1. при возникновении компрометации либо подозрении на компрометацию ключа и/или использования ключа электронной подписи без согласия владельца сертификата ключа проверки ЭП;

11.1.2. в случае возникновения компрометации ключа сертификационного центра банка;

11.1.3. в случае если владелец сертификата ключа проверки ЭП по каким-либо причинам не смог осуществить плановую смену ключей электронной подписи в установленные для этой процедуры сроки;

11.1.4. в случае изменения регистрационных данных физического лица — участника корпоративной ИС;

11.1.5. в иных необходимых случаях.

11.2. При появлении у владельца сертификата ключа проверки ЭП необходимости во внеплановой смене сертификата ключа проверки ЭП, данное физическое лицо — участник корпоративной ИС должно обратиться в офис Банка с соответствующим заявлением и документом, удостоверяющим личность.

11.3. После проведения идентификации личности участника корпоративной ИС - владельца сертификата ключа проверки ЭП и подтверждения его полномочий на обмен ЭД, Банк осуществляет выпуск нового сертификата ключа проверки ЭП данному участнику корпоративной ИС.

11.4. По окончании процедуры выпуска сертификата ключа проверки ЭП, владелец сертификата ключа проверки ЭП получает возможность, используя программные средства корпоративной ИС, удалённо завершить процедуру формирования ключа электронной подписи и приступить к его эксплуатации.

12. ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТА О СОВЕРШЕНИИ ОПЕРАЦИЙ ПО БАНКОВСКОМУ СЧЕТУ

12.1. Банк информирует Клиента о совершении каждой операции по банковскому счету, в том числе о совершении операции по распоряжению Клиента, переданному Банку в электронном виде с использованием корпоративной ИС, путем направления уведомления через корпоративную ИС.

12.2. Дополнительно Клиент вправе получать сообщения о совершении операций по банковскому счету по иным каналам связи, указанным Клиентом, (посредством SMS-уведомлений, e-mail - уведомлений).

Выбор дополнительного канала связи осуществляется Клиентом самостоятельно путем настройки соответствующей опции и введения информации о номере телефона и/или адресе электронной почты в корпоративной ИС либо путем подачи в Банк соответствующего заявления.

12.3. Сообщение Банка о совершении операции по банковскому счету содержит номер, код или иной идентификатор корпоративной ИС, вид операции, дату совершения

операции, сумму операции, идентификатор устройства при его применении для осуществления операций по банковскому счету с использованием корпоративной ИС.

Сообщение Банка о совершении операции по банковскому счету, направленное посредством SMS-уведомлений, e-mail-уведомлений содержит также наименование Банка.

Банк информирует Клиента о взимании комиссионного вознаграждения за совершение операции по банковскому счету путем указания суммы комиссионного вознаграждения в сообщении о совершении операции по банковскому счету либо путем направления отдельного сообщения с указанием общей суммы комиссионного вознаграждения за совершение операций по банковскому счету в расчетном периоде в соответствии с Тарифами Банка.

12.4. Клиент обязан в течение операционного дня отслеживать получение сообщений, указанных в п. 12.1. настоящего Регламента.

12.5. Обязанность Банка информировать Клиента о совершении операции по банковскому счету считается исполненной в случае направления Банком сообщения о совершении такой операции не позднее дня, следующего за днем ее совершения, любым из указанных в пп.. 12.1., 12.2. настоящего Регламента способов, а также в случаях предоставления Клиенту в указанный срок выписок об операциях по банковскому счету или бумажных копий расчетных ЭД.

12.6. Информация о совершенных операциях по банковскому счету считается доведенной до сведения Клиента независимо от фактического восприятия такой информации Клиентом (его уполномоченным представителем).

12.7. Обязанность Банка информировать Клиента о совершении операции по банковскому счету считается исполненной в момент отправки сообщения о совершении операции в соответствии с имеющейся у Банка информацией для связи с Клиентом.

Банк не несет ответственности в случае неполучения или получения Клиентом указанного сообщения с задержкой по времени или с искажением информации вследствие обстоятельств, независящих от Банка, в том числе:

12.7.1. по вине Клиента, провайдеров и других лиц в случаях аварий и сбоев в работе сети Интернет, перерывов в обслуживании Клиента посредством сети Интернет, связанных с нарушением в работе оборудования, систем подачи электроэнергии и/или линий связи и сетей, приостановления/прекращения предоставления услуг доступа в сеть Интернет, ухудшения работы сети Интернет, в результате чего возникли ошибки, пропуски, удаление файлов, дефекты и задержки в работе при передаче данных с использованием сети Интернет, неработоспособности или некачественного функционирования программного обеспечения, используемого Клиентом;

12.7.2. по вине Клиента, операторов мобильной связи и других лиц в случаях аварий и сбоев в работе систем мобильной связи, перерывов в обслуживании Клиента посредством мобильной связи, отключением услуги SMS-сообщений оператором мобильной связи, недоставкой сообщений оператором мобильной связи;

12.7.3. отключения мобильного телефона, нахождения его вне зоны действия сети, блокировке номера мобильного телефона, утери мобильного телефона (SIM-карты), возникновения технических проблем с мобильным телефоном, прекращения использования Клиентом SIM-карты или адреса электронной почты, несвоевременного оповещения Банка об изменении номера мобильного телефона или адреса электронной почты, отрицательном балансе на лицевом счете Клиента у оператора мобильной связи, прекращения приема сообщений в связи переполнением памяти мобильного телефона.

12.8. Банк не несет ответственности за невозможность получения Клиентом уведомлений Банка в случаях утраты Клиентом возможности получения таких уведомлений через Корпоративную ИС и непредоставлении Клиентом информации для направления уведомлений по иным каналам связи, предусмотренным в Регламенте, вследствие

приостановления обмена ЭД по причинам несоблюдения владельцем сертификата ключа ЭП требований к обмену ЭД и обеспечению информационной безопасности при обмене ЭД, истечения срока действия сертификата ключа проверки ЭП или его отзыва, компрометации ключа и/или использования ключа электронной подписи без согласия участника корпоративной ИС, возникновения корпоративного конфликта, не позволяющего достоверно установить полномочия лиц по распоряжению счетом, замене карточки с образцами подписей и оттиска печати по банковскому счету Клиента с исключением из нее всех ранее уполномоченных на обмен ЭД лиц, ограничения доступа Клиента к корпоративной ИС при наличии непогашенной в течение 15 календарных дней задолженности Клиента по оплате услуг Банка.

13. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПРОЦЕДУРЫ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ БАНКА

13.1. Процедура проверки подлинности ЭД, в случае возникновения конфликтных ситуаций при обмене ЭД, приведена в Приложении №1 к настоящему Регламенту.

14. ОБЯЗАННОСТИ ВЛАДЕЛЬЦА И УЧАСТНИКОВ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

14.1. Банк обязуется:

14.1.1. обеспечивать регистрацию участников корпоративной ИС в соответствии с настоящим Регламентом;

14.1.2. своевременно рассматривать технологические запросы физических лиц - участников корпоративной ИС;

14.1.3. предоставлять участникам корпоративной ИС средства подтверждения ЭД;

14.1.4. предоставлять участникам корпоративной ИС сертификаты ключа проверки ЭП сертификационного центра Банка;

14.1.5. использовать для изготовления ключа электронной подписи сертификационного центра и формирования электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации (средства электронной подписи);

14.1.6. использовать ключ электронной подписи сертификационного центра только для подписи издаваемых им сертификатов ключа проверки ЭП - участников корпоративной ИС;

14.1.7. принимать меры по защите ключа электронной подписи сертификационного центра от несанкционированного доступа;

14.1.8. обеспечивать присвоение уникального идентификатора участнику корпоративной ИС — уполномоченному лицу Корпоративного клиента, гарантировать его уникальность для обеспечения идентификации данного участника корпоративной ИС; осуществлять ведение реестра уникальных идентификаторов;

14.1.9. обеспечивать занесение регистрационной информации владельца сертификата ключа проверки ЭП в реестр и гарантировать уникальность регистрационной информации участников корпоративной ИС, используемой для идентификации владельцев сертификатов ключей проверки ЭП;

14.1.10. обеспечивать уникальность номеров изготавливаемых сертификатов ключа проверки ЭП и уникальность значений ключей проверки электронной подписи в изготовленных сертификатах ключа проверки ЭП их владельцев;

14.1.11. аннулировать (отзывать) сертификат ключа проверки ЭП по соответствующему заявлению участника корпоративной системы - владельца сертификата ключа проверки ЭП об аннулировании (отзыве), в соответствии с настоящим Регламентом;

14.1.12. аннулировать (отзывать) сертификаты ключей проверки ЭП владельцев сертификата ключа проверки ЭП в случае компрометации ключа сертификационного центра, с использованием которого были изданы сертификаты ключей проверки ЭП;

14.1.13. своевременно блокировать доступ и осуществлять отмену временной блокировки доступа к ресурсам корпоративной ИС в порядке, установленном настоящим Регламентом;

14.1.14. информировать Клиента о совершении операции по банковскому счету, не позднее дня, следующего за днем ее совершения, в порядке, предусмотренном гл. 12 настоящего Регламента;

14.1.15. обеспечить возможность информирования Банка Участником корпоративной ИС о случаях компрометации ключа и/или использования ключа электронной подписи без его согласия в порядке, установленном настоящим Регламентом;

14.1.16. фиксировать направленные Клиенту сообщения о совершении операций по банковскому счету с использованием корпоративной ИС, а также полученные от Участника корпоративной ИС сообщения о компрометации (подозрении на компрометацию) ключа электронной подписи уполномоченного лица Клиента и/или использования ключа электронной подписи без его согласия, а также хранить соответствующую информацию не менее трех лет.

14.2.Участник корпоративной ИС — физическое лицо — уполномоченный представитель Клиента обязан:

14.2.1.хранить в тайне информацию об уникальном идентификаторе и средствах подтверждения ЭД;

14.2.2.принимать все возможные меры для предотвращения раскрытия данной информации и ее несанкционированного использования;

14.2.3.незамедлительно обращаться в Банк с заявлением на блокирование доступа к ресурсам корпоративной ИС в случае обнаружения факта либо при подозрении на компрометацию ключа и/или использования ключа электронной подписи без согласия Участника корпоративной ИС;

14.2.4.осуществлять регулярные сеансы связи с корпоративной ИС для своевременного получения сообщений Банка, в том числе уведомлений через корпоративную ИС, контролировать получение уведомлений Банка, направленных с использованием иных средств связи;

14.2.5.предоставлять достоверную информацию для связи с участником корпоративной ИС, в том числе информацию о номере телефона и адресе электронной почты для получении SMS – уведомлений и e-mail - уведомлений Банка, а в случае изменения информации для связи с участником корпоративной ИС своевременно предоставлять актуальную информацию.

14.2.6. принимать необходимые и достаточные организационные и технические меры безопасности для предотвращения несанкционированного доступа неуполномоченных лиц, в том числе посредством сети Интернет, к собственным средствам вычислительной техники, ключам электронной подписи, ключевым носителям.

14.3.Дополнительно владелец сертификата обязан:

14.3.1.собственноручно генерировать личный ключ электронной подписи;

14.3.2.применять для хранения личного ключа электронной подписи ключевой носитель, поддерживаемый средством электронной подписи корпоративной ИС Банка;

14.3.3. хранить в тайне личный ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования;

14.3.4. применять для формирования электронной подписи в ЭД только действующий личный ключ электронной подписи;

14.3.5. не применять личный ключ электронной подписи, если стало известно о факте его компрометации;

14.3.6. не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки ЭП, заявление на аннулирование (отзыв) которого подано в Банк;

14.3.7.незамедлительно обращаться в Банк с заявлением на блокирование доступа к ресурсам корпоративной ИС и/или отзыв сертификата ключа проверки ЭП в случае обнаружения факта либо при подозрении на компрометацию ключа и/или использования ключа электронной подписи без согласия Владельца сертификата ключа проверки ЭП;

14.4.Участник корпоративной ИС — Корпоративный клиент обязан:

14.4.1 незамедлительно обращаться в Банк с заявлением на блокирование доступа к ресурсам корпоративной ИС и отзыв сертификата ключа проверки ЭП и/или блокирования средства подтверждения простой ЭП в случае обнаружения факта либо при подозрении на компрометацию ключа и/или его использования без согласия Участника корпоративной ИС;

14.4.2. осуществлять регулярные сеансы связи с корпоративной ИС для своевременного получения уведомлений через корпоративную ИС, контролировать получение уведомлений Банка, направленных с использованием иных средств связи;

14.4.3. предоставлять достоверную информацию для связи с Участником корпоративной ИС, в том числе информацию о номере телефона и адресе электронной почты для получении SMS – уведомлений и e-mail - уведомлений Банка, а в случае изменения информации для связи с Участником корпоративной ИС своевременно предоставлять актуальную информацию.

14.4.4. оплачивать услуги Банка в размере и в сроки, установленные Тарифами.

15. ПРАВА ВЛАДЕЛЬЦА И УЧАСТНИКОВ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

15.1.Банк имеет право:

15.1.1.отказывать участникам корпоративной ИС в создании, аннулировании (отзыве) сертификата ключа проверки ЭП, блокировании доступа к ресурсам корпоративной ИС в случае ненадлежащего оформления соответствующего заявления.

15.1.2.отказывать участникам корпоративной ИС в аннулировании (отзыве) сертификата ключа проверки ЭП, блокировании и отмене временной блокировки доступа к ресурсам корпоративной ИС в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификата ключа проверки ЭП;

15.1.3.в одностороннем порядке ограничивать права доступа либо блокировать доступ к ресурсам корпоративной ИС, приостанавливать действие сертификата ключа проверки ЭП с обязательным уведомлением Клиента/владельца сертификата ключа проверки ЭП, действие которого приостановлено, и указанием обоснованных причин;

15.1.4. вносить изменения и/или дополнения в настоящий Регламент, о чем уведомляет участников корпоративной ИС не позднее чем за 10 (десять) календарных дней до вступления в силу соответствующих изменений/дополнений, любым из способов, в том числе путем размещения соответствующей информации на информационном web-сайте Банка, информационных стендах в дополнительных офисах и других структурных подразделениях Банка, осуществляющих обслуживание Клиентов, иными способами,

позволяющими участникам корпоративной ИС получить информацию и определить, что она исходит от Банка.

В случае несогласия участника корпоративной ИС с внесенными в настоящий Регламент изменениями и/или дополнениями, участник корпоративной ИС вправе расторгнуть соответствующий договор/соглашение, путем заключением которого Клиент присоединился к настоящему Регламенту, направив Банку соответствующее уведомление не позднее, чем за 3 (три) дня до даты вступления в силу изменений.

В случае если участник корпоративной ИС в установленный срок не заявил о расторжении Соглашения о присоединении к настоящему Регламенту либо вышеуказанного Договора, изменения Регламента (новый Регламент) считаются принятыми участником корпоративной ИС и он обязуется их соблюдать.

15.2.Участник корпоративной ИС имеет право:

15.2.1.обращаться в Банк с заявлением об изготовлении сертификата ключа проверки ЭП;

15.2.2.применять сертификат ключа проверки ЭП для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки ЭП;

15.2.3.обращаться в Банк с заявлением о блокировании доступа к ресурсам корпоративной ИС, об аннулировании (отзыве) сертификата ключа проверки ЭП и/или средства подтверждения простой ЭП, владельцем которой он является.

15.2.4.обращаться в Банк с заявлением об отмене блокирования доступа к ресурсам корпоративной ИС;

15.2.5.обращаться в Банк за получением информации о статусе сертификата ключа проверки ЭП, изданного сертификационным центром Банка, на определённый момент времени;

15.2.6.обращаться в Банк за подтверждением подлинности электронной подписи в ЭД, сформированной с использованием средств подтверждения ЭД, в т.ч. сертификата ключа проверки ЭП, изданного сертификационным центром Банка.

16. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ И МЕРЫ ПРЕДОТВРАЩЕНИЯ РИСКОВ ПРИ ИСПОЛЬЗОВАНИИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В целях исключения рисков при использовании корпоративной ИС участник корпоративной ИС:

16.1. самостоятельно обеспечивает наличие необходимых и достаточных аппаратных, системных, сетевых, программных и телекоммуникационных средств для организации обмена ЭД, согласно техническим требованиям Банка, изложенным в Приложении №1 указанного в п.2.4. Договора;

16.2. принимает необходимые и достаточные организационные и технические меры безопасности для предотвращения несанкционированного доступа неуполномоченных лиц, в том числе посредством сети Интернет, к собственным средствам вычислительной техники, ключам электронной подписи и ключевым носителям, мобильному телефону, SIM-карте с абонентским номером, который используется для направления динамического пароля посредством SMS-уведомлений;

16.3. хранит в тайне личный ключ ЭП, принимает все возможные меры для предотвращения его компрометации;

16.4. не применяет личный ключ ЭП, если стало известно о его компрометации;

16.5. использует полученные программно-технические средства только для целей осуществления электронного документооборота в соответствии с настоящим Регламентом, не передает без письменного согласия Банка данные средства третьим лицам;

16.6. устанавливает критические обновления системы, антивирусную защиту и обеспечивает регулярное обновление антивирусных баз;

16.7. при использовании корпоративной ИС применяет лицензионное программное обеспечение;

16.8. осуществляет своевременную замену сертификатов ключей проверки ЭП;

16.9. Клиент - участник корпоративной ИС своевременно доводит до Банка информацию об исключении сотрудника из числа уполномоченных на обмен ЭД лиц в связи с его увольнением, переводом на другой участок работы и т.п. путем оформления нового «Списка уполномоченных лиц для осуществления обмена ЭД»;

16.10. незамедлительно производит действия по приостановлению обмена ЭД (блокирует доступ владельцу ключа ЭП к ресурсам корпоративной ИС) при компрометации (подозрении на компрометацию) ключа подписи Клиента /уполномоченного лица Клиента и/или использования ключа электронной подписи без согласия Клиента, сообщив об этом в контакт-центр Банка по телефонам, указанным в разделе 17 настоящего Регламента, либо путем обращения в Банк с соответствующим заявлением о блокировании доступа и документами, удостоверяющими личность в случаях, установленных в настоящем Регламенте;

16.11. не использует личный ключ в системах, в которых отсутствуют программно-технические средства, обеспечивающие должный уровень антивирусной защиты;

16.12. не производит декомпиляцию, модификацию программных средств, не совершает относительно указанных программно-технических средств других действий, нарушающих действующее законодательство РФ; не совершает действий, направленных или способных привести к нарушению целостности системы электронного документооборота;

16.13. незамедлительно сообщает Банку о ставших известными попытках третьих лиц совершить действия, способные привести к нарушению целостности системы электронного документооборота;

16.14. признает право Банка по своему усмотрению совершить телефонный звонок Клиенту на указанный при открытии счета телефонный номер для дополнительного подтверждения того, что созданный ЭД от имени Клиента составлен и подписан (подтвержден) именно Клиентом/уполномоченным лицом Клиента. В случае если в результате такого звонка Банку не удается связаться с Клиентом, либо на такой звонок отвечает лицо, которое не может быть идентифицировано Банком в качестве уполномоченного лица Клиента, а также в случае если Клиент/уполномоченное лицо Клиента не подтверждает составление и/или подписание (подтверждение) созданного ЭД, Банк вправе отказать в приеме и исполнении такого ЭД.

17. СПРАВОЧНАЯ ИНФОРМАЦИЯ

17.1. По всем возникающим у Клиента вопросам можно обратиться в офис Банка или контакт-центр по телефонам:

в г.Екатеринбург (343) 222 11 00;
в г. Верхняя Пышма (34368) 4 94 94;
в г. Новоуральск (34370) 7 42 24;
в г .Челябинск (351) 729 83 82;
в г. Магнитогорск (3519) 49 67 00;
в г .НижнийТагил (3435) 47 54 57.

Приложение 1 к Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО

Порядок разрешения конфликтных ситуаций при обмене электронными документами

1 Общие положения

1.1.Процедура проверки подлинности ЭП инициируется при поступлении соответствующего письменного заявления от Клиента. Под процедурой проверки подлинности ЭП, при обмене ЭД между Банком и участником корпоративной ИС, связанной с обменом электронными документами, подписанными усиленной ЭП или простой ЭП понимается возникновение у участника корпоративной ИС сомнений, связанных с непризнанием авторства и (или) целостности ЭД, подписанного его ЭП (усиленной или простой), либо его уполномоченного представителя.

1.2.Стороны признают информацию, содержащуюся в системных журналах, достаточной для проверки подлинности простой ЭП в ЭД. Подтверждение подлинности простой ЭП в ЭД осуществляется путем сопоставления данных, указанных участником корпоративной ИС в настройках использования простой ЭП в Корпоративной ИС, и данных, присвоенных оспариваемому ЭД в Корпоративной ИС, а также информации в системных журналах в соответствии с базовой процедурой, приведенной в разделе 3 настоящего Порядка.

1.3.Подтверждение подлинности усиленной ЭП в ЭД — осуществляется путем проверки соответствующим средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в ЭД Клиенту (владельцу сертификата) и отсутствия искажений в подписанном данной электронной подписью ЭД в соответствии с базовой процедурой, приведенной в разделе 3 настоящего Порядка.

1.4. Процедура проверки подлинности ЭП, при обмене ЭД с клиентами Банка в случае применения усиленной электронной подписи основывается на математических свойствах алгоритма электронной подписи, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения усиленной электронной подписи любым лицом, не обладающим ключом электронной подписи. Итогом разрешения конфликтной ситуации является либо доказательство подлинности, целостности и авторства оспариваемого участником корпоративной ИС электронного документа, либо признание факта приема Банком к исполнению искаженного электронного документа.

1.5. На случай возникновения споров Банк обеспечивает хранение в течение установленных законодательством РФ сроков в специальной базе данных электронных документов участника корпоративной ИС в виде единиц хранения, каждая из которых включает данные ЭД, строки электронной подписи с параметрами усиленной электронной подписи, сертификат ключа проверки электронной подписи участника корпоративной ИС, использованный при формировании усиленной электронной подписи, историю настроек участника корпоративной ИС для использования простой подписи в системных журналах Банка, а так же данные средств подтверждения ЭД участника корпоративной ИС,

использованные при формировании простой ЭД в оспариваемом ЭД. Банк обеспечивает защиту данных от возможных искажений в процессе хранения. Также Банк обеспечивает хранение первичного запроса на сертификат ключа проверки ЭП в бумажной форме.

1.6. Процедура проверки подлинности ЭП, при обмене ЭД с клиентами Банка выполняется Согласительной комиссией, в состав которой входят представители обеих сторон (не более 3 (трех) человек от каждой стороны). По соглашению сторон в состав комиссии может быть введен независимый эксперт.

2. Порядок разрешения конфликтной ситуации

2.1. В случае возникновения необходимости в проведении процедуры проверки подлинности ЭП, при обмене ЭД с клиентами Банка участник корпоративной ИС представляет Банку заявление, содержащее существо претензии с указанием на документ, который он оспаривает.

2.2. Банк обязан в течение не более пяти рабочих дней от даты приема заявления участника корпоративной ИС создать Согласительную комиссию для рассмотрения заявления.

2.3. Согласительная комиссия должна закончить свою работу в течение 10 рабочих дней с момента ее создания.

2.4. Согласительная комиссия проверяет принадлежность усиленной ЭП или простой ЭП под оспариваемым ЭД участника корпоративной ИС на основании данных в системных журналах Банка, в случае применения усиленной ЭП под оспариваемым ЭД участника корпоративной ИС применяется базовая процедура проверки, описанная в пунктах 3.1. - 3.3 настоящего Порядка, в случае применения простой ЭП под оспариваемым ЭД участника корпоративной ИС применяется базовая процедура проверки, описанная в пункте 3.4. настоящего Порядка.

2.5. Решение комиссии принимается большинством голосов, оформляется актом и подписывается всеми членами комиссии.

2.6. Стороны исполняют решения согласительной комиссии в течение десяти рабочих дней с момента подписания акта о решении Согласительной комиссии.

2.7. Уклонение какой-либо из сторон от участия в создании или работе Согласительной комиссии, причиной чего возникла невозможность создания или работы Согласительной комиссии не исключает возможности урегулирования конфликта в судебном порядке. В случае, если стороны не пришли к взаимному соглашению или в случае отказа от добровольного исполнения решения комиссии, стороны решают конфликтную ситуацию в судебном порядке.

3. Базовая процедура работы согласительной комиссии

3.1. Для проверки принадлежности усиленной ЭП участнику корпоративной ИС и отсутствия искажений в ЭД из базы данных Банка извлекается файл сертификата ключа проверки ЭП участника корпоративной ИС - владельца сертификата ключа проверки ЭП, использованный при формировании усиленной ЭП под оспариваемым ЭД.

3.1.1 Устанавливается принадлежность ключа проверки электронной подписи, содержащегося в извлеченном файле, владельцу сертификата ключа проверки ЭП по следующей процедуре:

3.1.1.1 из базы данных сертификационного центра извлекается первичный сертификат ключа проверки ЭП участника корпоративной ИС - владельца сертификата ключа проверки ЭП. Устанавливается принадлежность ключа проверки электронной подписи владельцу сертификата путем сравнения с ключом проверки электронной подписи в запросе на сертификат в бумажном виде. Если соответствие не установлено, то принадлежность ключа

электронной подписи данному владельцу сертификата проверки ключа ЭП – Клиенту/уполномоченному представителю Клиента не подтверждается;

3.1.1.2 из базы данных сертификационного центра извлекается последующий запрос (при наличии такового) на сертификат данного участника корпоративной ИС - владельца сертификата ключа проверки ЭП и устанавливается факт его подписания первичным ключом по содержанию сертификата ключа проверки ЭП. В противном случае - принадлежность ключа данному уполномоченному представителю Клиента не подтверждается;

3.1.1.3 вышеуказанные действия последовательно повторяются вплоть до проверки запроса на сертификат ключа подписи данного владельца сертификата ключа проверки ЭП, использованного для формирования электронной подписи под оспариваемым ЭД. Если из содержания запроса на сертификат проверки ключа ЭП в базе данных сертификационного центра не следует, что запрос проверен предыдущим сертификатом данного участника корпоративной ИС - владельца сертификата проверки ключа ЭП, принадлежность ключа данному участнику корпоративной ИС не подтверждается. В противном случае - ключ признается принадлежащим данному уполномоченному представителю Клиента.

3.1.2 Устанавливается действительность сертификата ключа проверки ЭП участника корпоративной ИС - владельца сертификата ключа проверки ЭП, на момент получения Банком оспариваемого ЭД. Сертификат ключа проверки ЭП является недействительным на момент получения Банком оспариваемого ЭД, если:

- срок действия сертификата ключа проверки ЭП истек;

- данный сертификат был помещен в список отозванных сертификатов;

в противном случае, сертификат ключа проверки ЭП участника корпоративной ИС - владельца сертификата ключа проверки ЭП признается действительным.

3.1.3. Устанавливается факт блокирования доступа владельцу сертификата ключа проверки ЭП к ресурсам корпоративной ИС на момент получения Банком оспариваемого ЭД. В случае, если дата подачи заявления на блокирование доступа в корпоративную ИС ее участнику раньше даты получения Банком оспариваемого ЭД — ЭД признается недействительным. В противном случае либо при установлении отсутствия факта подачи соответствующего заявления участником корпоративной ИС - ЭД признается действительным.

3.2. На компьютер устанавливается специальное сертифицированное программное обеспечение, предназначенное для проверки усиленной электронной подписи под электронным документом.

3.3. Проверка электронной подписи оспариваемого документа производится программой ccom32_verify. По результатам проверки электронной подписи под ЭД признается принадлежащей уполномоченному лицу Клиента - владельцу сертификата, если в протоколе проверки, выдаваемом программой, сформирована запись о том, что подпись подтверждена (signature, correct), и не принадлежащей уполномоченному лицу Клиента - владельцу сертификата, в противном случае. Протокол проверки усиленной электронной подписи распечатывается и подписывается всеми членами комиссии.

3.4 Для проверки принадлежности простой подписи участнику корпоративной ИС и отсутствия искажений в ЭД, из системного журнала Банка извлекается информация оспариваемого ЭД, которая содержит:

- содержимое оспариваемого ЭД;

- информация о подписанте (ФИО, право подписи на момент подписания); идентификатор ключа;

- время подписания ЭД;

- IP адрес, с которого совершалась операция;

- средства подтверждения ЭД;

- номер телефона/ e-mail, на который был отправлен динамический пароль для подтверждения операции;

- динамический пароль, введенный для подтверждения операции, дата и время формирования сообщения.

3.4.1 Устанавливается соответствие информации оспариваемого ЭД, данных средства подтверждения ЭД для использования простой ЭП, указанных клиентом в настройках корпоративной ИС на момент подписания оспариваемого ЭД и информации оспариваемого ЭД, данных средства подтверждения в ЭД, указанных в распечатке ЭД, полученных из системных журналов Банка.

3.4.2.При совпадении информации оспариваемого ЭД, данных средства подтверждения для использования простой ЭП, указанных участником корпоративной ИС в настройках корпоративной ИС на момент подписания оспариваемого ЭД, и информации оспариваемого ЭД, данных средства подтверждения в ЭД, указанных в распечатке ЭД, полученных из системных журналов Банка, проверяется факт блокирования Участником корпоративной ИС доступа к ресурсам корпоративной ИС.

3.4.3.Устанавливается факт блокирования Клиентом доступа к ресурсам корпоративной ИС на момент получения Банком оспариваемого ЭД. В случае, если дата подачи заявления на блокирование доступа в корпоративную ИС ее участнику раньше даты получения Банком оспариваемого ЭД — ЭД признается недействительным. В противном случае либо при установлении отсутствия факта подачи соответствующего заявления участником корпоративной ИС - ЭД признается действительным.

4. Ответственность сторон

4.1. Банк несет ответственность перед Клиентом, если Согласительной комиссией установлен хотя бы один из ниже перечисленных фактов:

4.1.1. средство подтверждения ЭД не принадлежит данному участнику корпоративной ИС;

4.1.2 средство подтверждения, использованное при формировании электронной подписи, было недействительно на момент получения Банком оспариваемого ЭД;

4.1.3 электронная подпись в ЭД не принадлежит данному участнику корпоративной ИС;

4.1.4. установлен факт подачи заявления участником ИС о блокировании доступа в корпоративную ИС с использованием средства подтверждения ЭД, которым был подписан оспариваемый ЭД, датой раньше даты получения Банком оспариваемого ЭД.

4.1.5 Динамический пароль для подписания ЭД простой ЭП был отправлен на номер мобильного телефона, отличающийся от номера мобильного телефона, указанного в настройках корпоративной ИС на момент подписания оспариваемого ЭД.

4.2. Банк не несет ответственности по выполненным действиям согласно полученному документу при установлении Согласительной комиссией совокупности следующих фактов:

4.2.1 средство подтверждения ЭД принадлежит участнику корпоративной ИС;

4.2.2. средство подтверждения ЭД, используемое при формировании электронной подписи, являлось действительным на момент получения Банком ЭД;

4.2.3 электронная подпись в ЭД принадлежит участнику корпоративной ИС;

4.2.4 не установлен факт подачи заявления участником ИС о блокировании доступа в корпоративную ИС с использованием средства подтверждения ЭД, которым был подписан оспариваемый ЭД, либо дата подачи заявления на блокирование позже или равна дате получения Банком оспариваемого ЭД.

4.2.5 динамический пароль в случае использования простой ЭП для подписания ЭД был отправлен на номер мобильного телефона, указанный в настройках корпоративной ИС на момент подписания оспариваемого ЭД.

4.3. В случае если любая из сторон откажется от исполнения решения Согласительной комиссии все споры и разногласия подлежат разрешению в порядке, установленном действующим законодательством РФ.

Приложение 2 к Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО

Соглашение № _____
о присоединении к Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО

г. Екатеринбург «___» _____20___

Я,

_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта

_____
(кем и когда выдан)

В соответствии со статьей 428 Гражданского кодекса Российской Федерации настоящим полностью и безусловно присоединяюсь к Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО, условия которого определены БАНКОМ «НЕЙВА» ООО и опубликованы на сайте по адресу www.neyvabank.ru.

С Регламентом взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО и приложениями к нему ознакомлен, согласен и обязуюсь соблюдать все положения указанного документа.

Подтверждаю, что до подписания настоящего Соглашения надлежащим образом ознакомлен с указанными в разделе 16 Регламента условиями использования корпоративной информационной системы, ограничениями способов и мест использования корпоративной информационной системы, а также случаями повышенного риска использования корпоративной информационной системы.

Прошу выпустить сертификат ключа проверки ЭП для участия в корпоративной информационной системе БАНКА «НЕЙВА» ООО.

Банк: Клиент:

Приложение 3 к Регламенту взаимодействия участников корпоративной информационной системы БАНКА «НЕЙВА» ООО

Перечень электронных документов, используемых в корпоративной информационной системе БАНКА "НЕЙВА" ООО

1. Платежное поручение.*
2. Заявление на покупку иностранной валюты.*
3. Заявление на продажу иностранной валюты.*
4. Заявление на перевод иностранной валюты.
5. Распоряжение о списании валюты с транзитного счета.
6. Уведомление о поступлении иностранной валюты на транзитный валютный счет.*
7. Справка о валютных операциях.
8. Выписка по счету клиента.*
9. Кассовая заявка на получение денежной наличности.
10. Заявление на подключение тарифного пакета. Заявки/уведомления, направляемые в рамках генерального соглашения о привлечении денежных средств в депозит, включая заявку на размещение денежных средств, заявку на изменение условий депозитного договора, заявку на возврат денежных средств. Реестры, направляемые в рамках договора о предоставлении услуги «Зарплатный проект», включая реестр на открытие банковских счетов работникам Клиента, реестр перечислений денежных средств на банковские счета работников Клиента, реестр уволенных и/или прекративших получение денежных средств в рамках зарплатного проекта работников, реестр на перевыпуск банковских карт.
11. ЭД информационного характера свободного формата.*

* доступно при использовании простой ЭП

Банк:
620142, Свердловская область,
г. Екатеринбург, ул. Чапаева, д. 3а.
Корреспондентский счет:
30101810800000000774
в Уральском ГУ Банка России

ИНН: 6629001024
БИК: 046577774

Клиент:
Адрес регистрации:
Адрес для почтовых уведомлений:

КПП:
ИНН:

_____ (ФИО)
М.П.

_____ (ФИО)
М.П.