Приложение № 4
к Общим условиям использования
электронных документов

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ[1]

I. При использовании Подсистемы «ИКБ»

1. Обмен Электронными документами

1.1. Для работы в Системе Пользователь Системы использует программно-технические средства, удовлетворяющие требованиям, приведенным в Списке технических и программных средств, необходимых для работы подсистемы «Клиент» (далее – Список).

1.2. В процессе работы Пользователь Системы выполняет в Системе следующие действия:

- Регистрация в Системе – формирование специального ЭД «регистрация», подписанного ЭП Клиента (далее – ЭПК). Работа в Системе возможна только после успешной проверки ЭПК сервером Системы.
- Работа с ЭД, исходящими от Клиента, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе и предусмотренных в Заявлении. Для каждого типа ЭД в Системе имеется соответствующая экранная форма. Для документов «Платежное поручение» возможен импорт в Систему файлов определенного Банком формата. Описание структуры файла импорта имеется на сервере Банка.
- Проставление для каждого ЭД одной или нескольких ЭПК. Количество ЭПК для каждого типа ЭД определено в Заявлении. После подписания ЭД всеми необходимыми ЭПК в соответствии с Заявлением происходит автоматическая пересылка ЭД в Банк для исполнения.
- Просмотр, печать, сохранение в файл поступивших из Банка ЭД.
- Выход из Системы.

1.3. Процедура обработки ЭД сервером Системы происходит следующим образом:

По окончании формирования ЭД Пользователи Системы проставляют ЭПК в количестве, определенном в Заявлении и отправляют ЭД в Банк.

Сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭПК.

Основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭПК в ЭД. При положительном результате проверки сервер Банка проставляет в документе отметку о времени приема ЭД и ЭП Банка (далее – ЭПБ), свидетельствующую о получении Банком ЭД, и сохраняет данный ЭД в Системе. При отрицательном результате проверки ЭПК ЭПБ в ЭД не проставляется, Клиент получает сообщение об ошибке средствами Системы. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов ключей размещаются на сервере системы https://www.bankline.ru. Сертификат Ключа проверки электронной подписи Банка подписывается только уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 5 лет.

[1] Настоящий Порядок определяет порядок взаимодействия Сторон при использовании Клиентом подсистемы «ИКБ» и подсистемы «Прямая интеграция».

1.4. Процедуры, описанные в п.1.3 настоящего Порядка, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть выполнены в другой последовательности и рассматриваться независимо друг от друга.

1.5. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл должен содержать ЭПК, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

1.6. Переданный Клиентом в Банк ЭД в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус ЭД изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк ЭД. Сервер Банка присваивает полученным от Клиента ЭД следующие статусы:

Рублевые платежные поручения:

- получен банком
- документ отправлен на исполнение
- Рассчитана комиссия за РКО хх.хх.
- Принято или «обработано с ошибкой» с указанием причины, по которой документ отвергнут
- Отправлен на валютный контроль
- Включен в рейс для РКЦ
- Исполнен

Остальные типы документов:

- получен банком
- документ отправлен на исполнение
- Принят к исполнению или «обработано с ошибкой» с указанием причины, по которой документ отвергнут
- Реестр к росписи
- Реестр расписан или частично расписан в случае частичной росписи
- Сообщение отправлено в филиал
- Документ получен сотрудником валютного контроля.

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «документ отправлен на исполнение», а при работе в Депозитарном модуле Системы - получение Клиентом документа типа «Статус обработки распоряжения/запроса», в котором указано, что статус обработки соответствующего ЭД Клиента «Принято к исполнению».

Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Системы.

Примечание: Перечень и описание статусов ЭД, присваиваемых сервером Банка в Депозитарном модуле Системы, приведены в руководстве пользователя Депозитарного модуля Системы.

1.7. При формировании ЭД для Клиента Банк проставляет в нем ЭПБ. ЭД считается переданным Банком Клиенту, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих ЭД Клиента на сервере Банка. Клиент может сохранить любой входящий

документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

1.8. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭПК и ЭПБ, и доставленных Клиенту ЭД, содержащих ЭПБ, и хранит их способом, обеспечивающим Клиенту доступ к данным ЭД на сервере Банка.

1.9. Клиент с помощью программы проверки ЭП CryptoManager.exe, установленной на Персональном компьютере, имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива. Вышеуказанная программа проверки ЭП позволяет выполнять проверку типов ЭП (раздел 3 настоящего Порядка), разрешенных для использования в Системе.

1.10. Программу проверки ЭП CryptoManager.exe можно получить у фирмы-разработчика Системы – ЗАО «ИНИСТ» (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 115035, г. Москва, Космодамианская наб., д.40-42, стр.3.

2. Порядок получения, замены и хранения ключей

2.1. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Клиентами, относящимися к корпоративному сегменту:

2.1.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах с использованием своих технических средств.

2.1.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.

2.1.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, являющегося единоличным исполнительным органом Клиента и направленного в Банк с использованием Системы. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя, в том числе являющимся единоличным исполнительным органом.

2.1.4. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. По заявлению Клиента, направленному в Банк в произвольной форме средствами Системы до окончания срока действия Комплекта ключей, его действие может быть продлено на срок не более 3 месяцев. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.

2.1.5. Оформленные со стороны Банка Сертификаты ключей Клиента вручаются УПК либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.

2.1.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификата ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.

2.1.7. В случае информирования Банком Клиента в Системе о необходимости осуществить замену USB-токена соответствующего типа, Клиент обязан осуществить замену USB-токена. С момента информирования Банком Клиента в Системе о необходимости осуществить замену USB-токена, генерация Комплектов ключей с помощью USB-токена, подлежащего замене, не осуществляется.

2.2. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Клиентами, относящимися к сегменту предпринимателей:

2.2.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.

2.2.3. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.

2.2.4. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, и направленного в Банк с использованием Системы. Указанный запрос также может быть подписан простой электронной подписью Пользователя Системы, сформированной на основании предъявленного клиентом SMS-кода, ранее направленного Банком на номер телефона данного Пользователя Системы, указанный в Заявлении и/или предоставленный Банку Пользователем Системы в процессе обслуживания в Системе. Пользователь Системы должен обладать полномочиями на направление в Банк соответствующего электронного запроса. При использовании Клиентом Системы при наличии открытого расчетного счета подпись такого Пользователя должна быть включена в карточку с образцами подписей и оттиска печатей, действующей к счету Клиента, обслуживаемому в рамках Договора, в случае ее оформления. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя по направлению в Банк электронного запроса на выдачу Сертификата ключа.

2.2.5. Срок действия Комплекта ключей определяется Банком и указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае, если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока действия Комплекта ключей Клиент обязан инициировать процедуру смены Комплектов ключей. При этом, до окончания срока действия Комплекта ключей Клиент может продлить его действие на срок не более 3 (трех) месяцев, направив в Банк заявление посредством Системы. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Банком, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.

2.2.6. Оформленные со стороны Банка Сертификаты ключей Клиента на бумажных носителях вручаются уполномоченному представителю Клиента либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.

2.2.7. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификата ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.

2.2.8. В случае информирования Банком Клиента в Системе о прекращении действия имеющегося у Клиента USB-токена соответствующего типа, Клиент должен осуществить процедуру смены Комплектов ключей своих Пользователей Системы:

- путем генерирования Комплектов ключей своих Пользователей Системы на иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств, либо
- путем осуществления замены USB-токена, посредством обращения в подразделение Банка.

2.3. Для Комплекта ключей, сгенерированного посредством Мобильного приложения:

2.3.1. Пользователь вправе генерировать Комплект ключей для Мобильного приложения с помощью программных средств, предоставленных Банком, при наличии действующего Комплекта ключей, сгенерированного для работы на Персональном компьютере.

2.3.2. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей, сгенерированного посредством Мобильного приложения, не может превышать срок действия Комплекта ключей Пользователя, сгенерированного для работы на Персональном компьютере. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.

2.3.3. Статус ЭП Пользователя Системы, сгенерированной посредством Комплекта ключей для Мобильного приложения, соответствует Статусу ЭП Пользователя Системы, указанному в Заявлении, при генерации Комплекта ключей на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.).

2.3.4. Обязательная замена Комплекта ключей проводится в следующих случаях:

- истек срок действия Комплекта ключей;
- произошла Компрометация ключей.

2.4. В случае лишения Клиентом Пользователя Системы права подписывать ЭП ЭД соответствующие Комплекты ключей выводятся из действия на основании письменного заявления Клиента или ЭД свободного формата, направленного в Банк посредством Системы и подписанного уполномоченным лицом Клиента.

2.5. Банк вправе аннулировать Сертификат ключа в следующих случаях:

не подтверждено, что владелец Сертификата ключа владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

установлено, что содержащийся в Сертификате ключ проверки ЭП уже содержится в ином ранее созданном Сертификате ключа;

вступило в силу решение суда, которым, в частности, установлено, что Сертификат ключа содержит недостоверную информацию.

Информация о прекращении действия Сертификата ключа вносится Банком в соответствующий реестр сертификатов в срок, установленный действующим законодательством Российской Федерации.

3. Обеспечение безопасности процедуры обмена документами

3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

3.1.1. Для Персонального компьютера:

Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.» (вариант исполнения 2), разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3535 от 12.12.2018 г.). Клиент, относящийся к сегменту предпринимателей, имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (оптические диски, флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов.

Использованием СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных ЗАО «Алладин Р.Д.» (сертификат соответствия ФСБ России № СФ/124 – 3956 от 17.11.2020 г.). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к Ключу электронной подписи осуществляется с использованием пароля. Клиент, относящийся к сегменту предпринимателей, имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов.

Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 4.0 и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246 и выше[2]).

Удостоверения принадлежности сервера Системы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО «КРИПТО-ПРО».

3.1.2. Для Мобильного приложения:

Средства криптографической защиты информации с использованием алгоритма RSA для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v.1.2, RFC 2246), применяются криптографические международные алгоритмы шифрования RSA (3072 bit), обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с SHA 512.

[2] Рекомендуется использовать версию TLS v.1.2.

Симметричное шифрование AES с длиной ключа 256 bit., генерация и хранение Ключа электронной подписи, а также подписание ЭД производится во внутренней защищенной памяти Мобильного устройства. Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации, предназначенных для генерации и хранения ключа ЭП, за исключением USB-токенов.

3.2. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

3.2.1. Для работы на Персональном компьютере:

Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком;

Генерацию и хранение ключевой информации, а также подписание документов производить с использованием USB-токенов JaCarta -2 ГОСТ;

В случае генерации Клиентом, относящимся к сегменту предпринимателей, Ключей электронной подписи своих Пользователей на носители, отличные от USB-токенов, осуществлять эксплуатацию рабочего места и обеспечение его безопасности организационными и техническими мерами в соответствии с требованиями эксплуатационной документацией для СКЗИ «Бикрипт 5.0» для класса КС1: «Средство криптографической защиты информации «Бикрипт 5.0». Правила пользования» (ИНФК.11485466.4012.027.31). Данный документ размещен на официальном сайте Банка в сети Интернет по адресу https://www.rosbank.ru.

Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов;

Проверять, что установлено защищенное TLS-соединение с официальным ресурсом сервиса https://www.bankline.ru.

Средствами подсистемы «Клиент» закрепить за Пользователями Системы IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка;

Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление;

Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников;

Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

Исключить использование средств удаленного администрирования;

Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана;

Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

Контролировать соблюдение требований безопасности.

3.2.2. Для работы с Мобильным устройством:

Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

Исключить использование средств удаленного администрирования;

Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты);

Контролировать соблюдение требований безопасности;

Обеспечить наличие антивирусного программного обеспечения.

3.3. Пользователи Системы, уполномоченные использовать Систему Клиентами, относящимися к сегменту предпринимателей, должны в Системе ввести номер телефона сотовой связи для получения на указанный номер информационных сообщений в соответствии с Договором.

3.4. Клиент обязан:

Исключить появление на Персональном компьютере или Мобильном устройстве подсистемы «Клиент» вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;

Исключить возможность несанкционированных Банком изменений в технических и программных средствах Клиента, определенных в Списке;

Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.

3.5. Стороны обязаны:

обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия;

уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

3.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Системы в случае появления обоснованных подозрений в наличии на Персональном компьютере и/или Мобильном устройстве Пользователя Системы вирусов или других программ деструктивного действия. Блокировка Ключа электронной подписи. Пользователя Системы снимается Банком по факту получения от Клиента подтверждения об удалении с Персонального компьютера и/или Мобильного устройства Пользователя Системы вирусов или других программ деструктивного действия.

3.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

Если произошла Компрометация ключей любого Пользователя Клиента, последний обязан:

В случае доступности Комплекта ключей (подозрение на несанкционированное копирование) немедленно послать в Банк ЭД «Блокировка ключа». При этом Система автоматически заблокирует возможность использования данного Комплекта ключей Пользователя Системы;

В случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны на сайте www.bankline.ru, а также в Заявлении, используя для авторизации кодовую фразу, приведенную в Сертификате ключа, о факте Компрометации ключей;

В случае утраты Пользователем Системы кодовой фразы Администратор Системы вправе произвести дополнительные действия по авторизации Пользователя Системы (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае предоставления необъективной информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Системе;

В случае компрометации (утраты, разглашения) SMS-кода незамедлительно проинформировать Банк по любому каналу связи;

В срок не более трех рабочих дней после сообщения по телефону о факте Компрометации ключей направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены Комплекта ключей;

В случае принятия решения о замене Комплекта ключей, сгенерированного для Персонального компьютера, сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации. В случае принятия решения о замене Комплекта ключей, сгенерированного посредством Мобильного приложения, сгенерировать новый Комплект ключей самостоятельно в соответствии с Порядком.

Если произошла Компрометация ключей Банка, последний обязан:

Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Системы и смене Комплекта ключей Банка посредством Системы с указанием даты и точного времени смены вышеуказанного Комплекта ключей;

Произвести внеплановую смену Комплекта ключей Банка, опубликовать новый Ключ проверки электронной подписи и копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы.

3.8. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного по кодовой фразе Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде.

Дальнейшее использование Системы Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.

II. При использовании Подсистемы «Прямая интеграция»

4. Общие правила обмена электронными документами

4.1 Клиент самостоятельно определяет способ интеграции учетной системы и Банка. Банк поддерживает следующие варианты интеграции (каждому из вариант интеграции соответствует свой набор электронных документов):

- через сервис «1С:ДиректБанк»;
- через протокол «SOAP» / «FTPs»;
- через сервис «Транзит НРД» (транзит документов Клиентов через систему электронного документооборота Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (ИНН 7702165310);

- через сеть «CyberFT» (транзит документов Клиентов через систему электронного документооборота Общества с ограниченной ответственностью «КИБЕРПЛАТ» (ИНН 7731220815).

4.2 Для работы в Подсистеме «Прямая интеграция» Клиент самостоятельно производит настройки учетной системы и выполняет необходимые доработки своей системы в зависимости от выбранного способа интеграции с Банком.

4.3 Для подключения к Банку по выбранному каналу прямого обмена Клиент использует:

- web-сервис «1С:ДиректБанк», опубликованный Банком по адресу https://www.bankline.ru/h2h/db1c;
- SOAP-сервер, опубликованный Банком по адресу https://www.bankline.ru/h2h/iso/H2HService;
- FTPs-ресурс, предоставленный Банком персонально каждому клиенту;
- интеграционный сервис «Транзит 2.0», предоставляемый НКО АО НРД;
- интеграционный сервис «CyberFT», предоставляемый ООО «КИБЕРПЛАТ».

4.4 Банк поддерживает следующие типы электронных документов в зависимости от выбранного варианта интеграции:

- «1С:ДиректБанк»:
  - документы от Клиента:
    - платежные поручения в рублях РФ;
    - платежные поручения в валюте;
    - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
  - документы от Банка:
    - статус исполнения платежного поручения;
    - подтверждение зачисления денежных средств на счета сотрудников;
    - выписки по рублевым и валютным счетам.
- протокол «SOAP» / «FTPS»:
  - документы от Клиента:
    - платежные поручения в рублях РФ и валюте;
    - заявления на покупку/продажу валюты;
    - заявления об обязательной продаже валюты;
    - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
    - документы валютного контроля;
    - заявления о размещении денежных средств;
    - документы свободного формата;
    - запросы на отзыв документа.
  - документы от Банка:
    - статус исполнения платежного поручения;
    - подтверждение зачисления денежных средств на счета сотрудников;
    - выписки;
    - статус отзыва документа.
- через «Транзит НРД»/сеть «CyberFT»:
  - документы от Клиента:
    - платежные поручения в рублях РФ и валюте;

- заявления на покупку/продажу валюты;
- заявления об обязательной продаже валюты;
- зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
- документы валютного контроля;
- заявления о размещении денежных средств;
- документы свободного формата;

o документы от Банка:
- статус исполнения платежного поручения;
- подтверждение зачисления денежных средств на счета сотрудников;
- выписки.

4.5 Банк поддерживает следующие форматы электронных документов в зависимости от выбранного варианта интеграции:

- «1С:ДиректБанк»: XML-формат технологи DirectBank (ДиректБанк) фирмы 1С. Описание приведено на сайте компании по адресу https://v8.1c.ru/its/services/1c-direktbank/.
- «SOAP» / «FTPS»: XML-формат стандарта ISO 20022:
  - o для платежей в рублях РФ на базе формата pain.001.001.03 (06)
  - o для статусов исполнения платежей на базе формата pain.002.001.03 (06)
  - o для выписок по окончанию операционного дня на базе формата camt.053.001.02
  - o для промежуточных выписок по запросу на базе формата camt.052.001.02
  - o для платежей в валюте и конверсии на базе формата pain.001.001.03 (06)
  - o для отзывов поручений клиента на базе формата camt.055.001.06
  - o для постановки на учет кредитного договора/контракта на базе формата auth.018.001.01
  - o для внесения изменений в ВБК на базе формата auth.021.001.01
  - o для снятия с учета контракта на базе формата auth.020.001.01
  - o для сведений о валютных операциях на базе формата auth.024.001.01
  - o для справки о подтверждающих документах на базе формата auth.025.001.01
  - o для статусов по документам Валютного контроля на базе формата auth.027.001.01
  - o для возврата ранее размещенных денежных средств на базе формата trea.325.001.01.RU
  - o для подтверждения о размещении депозита на базе формата trea.320.001.01.RU
  - o для писем свободного формата из/в банк auth.026.001.01

  Детальное описание форматов предоставляется Банком в Правилах Имплементации (TIG).
- «Транзит НРД»/сеть «CyberFT»: XML-формат стандарта ISO 20022:
  - o для платежей на базе формата pain.001.001.03 (06)
  - o для статусов исполнения платежей на базе формата pain.002.001.03 (06)
  - o для выписок по окончанию операционного дня на базе формата camt.053.001.02

4.6 Для начала работы в Системе Пользователь Системы должен быть зарегистрирован в Системе, иметь действующий Сертификат и соответствующий ему Закрытый ключ.

4.7 Работа с ЭД в Системе происходит с ЭД, подписанными ЭП Клиента с помощью действующего Сертификата. Банк исполняет ЭД, полученные от Клиента, только после успешной проверки ЭП Клиента сервером Системы. ЭП Клиента под пакетом документов приравнивается к ЭП Клиента под каждым документом внутри пакета.

4.8 Клиент может создать неограниченное количество Сертификатов для работы в Системе. При этом количество единовременно используемых Сертификатов для подписания ЭД ЭП Клиента:

- для технологии «1С:ДиректБанк» - не более 4 (четырех) Сертификатов;
- для технологий на базе протокола «SOAP» / «FTPS» /«Транзит НРД»/сети «CyberFT» – не ограничено.

4.9 Для технологии на базе протокола «SOAP» / «FTPS» /«Транзит НРД»/сети «CyberFT» Клиент может установить дополнительные требования к подписанию ЭД по сумме, заполнив соответствующий раздел Заявления о настройке пользователей системы и перечне электронных документов для подсистемы «Прямая интеграция» при наличии открытого расчетного счета (Приложение 1.2 к Условиям). В этом случае ЭД, получаемый Банком, должен быть сформирован таким образом, чтобы удовлетворять требованиям сочетания ЭП Клиента как для верификации на сервере Подсистемы «Прямая интеграция», так и для дополнительной проверки подписей на базе Заявления о дополнительной настройке подписей по типам электронных документов. В случае, если Клиент уже имеет действующее соглашение для работы в подсистеме «ИКБ» и требования к подписанию ЭД, настроенные в подсистеме «ИКБ», то данные требования будут применяться к ЭД, полученным по Подсистеме «Прямая интеграция» до отмены такого требования.

4.10 Процедура обработки ЭД сервером Подсистемы «Прямая интеграция» происходит следующим образом:

- сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭП.
- основанием для принятия Банком ЭД, переданного Клиентом по Подсистеме «Прямая интеграция», является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭП Клиента под ЭД. При положительном результате проверки сервер Банка проставляет в ЭД отметку о времени и ЭП Банка, свидетельствующую о получении пакета Банком, и сохраняет данный документ в Подсистеме «Прямая интеграция». При отрицательном результате проверки ЭП Клиента ЭП Банка в документе не проставляется, Клиент получает сообщение об ошибке средствами Подсистемы «Прямая интеграция». Сертификат ключа ЭП Банка выпускается уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 1 (один) год.

4.11 Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. При наличии действующего договора для работы в подсистеме «ИКБ» все входящие документы будут отображаться в «Исходящих документах» Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл содержит ЭП Клиента, отметку о времени приема документа Банком и ЭП Банка. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

4.12 Переданный Клиентом в Банк документ в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус документа изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк документа. Сервер Банка присваивает полученным от Клиента документам следующие статусы:

- для технологии «1С:ДиректБанк»:
  - Платежные поручения в рублях РФ, платежные поручения в валюте:
    - «Принят» – электронный документ прошел первичный контроль и поступил в обработку;
    - «Исполнен» – платежный документ исполнен Банком;

- «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;
- «Приостановлен» – платежный документ отложен Банком по причине недостатка средств на счете Клиента;
- «Аннулирован» – Электронный документ был отозван Клиентом с одобрения Банка;
- «Не подтвержден» – Платежный документ ожидает подтверждения по SMS или личном кабинете Клиента;

o Зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке:

- «Принят» – электронный документ прошел первичный контроль и поступил в обработку;
- «Исполнен» – электронный документ исполнен Банком;
- «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «Принят». Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Подсистемы «Прямая интеграция».

- для технологии «SOAP» / «FTPS» /«Транзит НРД»/сети «CyberFT» используются следующие статусы:

  «RCVD» - получено Банком;

  «RJCT» - отклонено;

  «ACTC» - принято, проверены подлинность и формат;

  «ACCP» - принято, документ отправлен на исполнение;

  «ACSP» - конечный успешный для внешних платежей;

  «ACSC» - конечный успешный для внутренних платежей.

4.13 При формировании ЭД для Клиента Банк проставляет в нем ЭП Банка. Документ считается переданным Банком Клиенту, если он подписан ЭП Банка и помещен во входящие документы Клиента на сервере Банка. При наличии действующего договора для работы в Подсистеме «ИКБ», исходящие документы от Банка будут присутствовать в списке «Входящие документы» Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

4.14 Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭП Клиента и ЭП Банка, и доставленных Клиенту ЭД, содержащих ЭП Банка, и хранит их.

5. Порядок получения, замены и хранения ключей

5.1. Клиент может запросить генерацию Сертификатов своих Пользователей Подсистемы «Прямая интеграция» согласно Заявлению о настройке пользователей системы (Приложение 1.2, Приложение 1.3 к Условиям) в соответствии с Руководством по генерации сертификатов электронной подписи пользователя для Подсистемы «Прямая интеграция», опубликованном на сайте Банка. В рамках Договора Клиент может использовать сертификаты ЭП, выпущенные Банком для Пользователей Клиента в рамках заключенного договора об использовании электронных документов.

5.2. Сертификат каждого Пользователя Подсистемы «Прямая интеграция» регистрируется Банком на основании подписанного Сторонами Акта о признании открытого ключа Подсистемы «Прямая интеграция» (размещен на веб-сайте https://www.bankline.ru), распечатанного и

подписанного в 2 (двух) экземплярах, по одному для каждой из Сторон. Заполненный Акт Система формирует автоматически.

5.3. Срок действия Комплекта ключей указывается в Сертификате и составляет 1 (Один) год. Срок действия Сертификата не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Подсистемы «Прямая интеграция», срок действия Комплекта ключей не может превышать 1 (Одного) года. Клиент несет ответственность за отслеживание срока действия сертификата и полномочий Пользователей Клиента.

5.4. До истечения установленного срока Клиент обязан инициировать процедуру генерации нового Сертификата. Продление срока действия Сертификата невозможно. На основании Заявления об отзыве (аннулировании) сертификата, составленном в свободном формате, Сертификат Пользователя Подсистемы «Прямая интеграция» аннулируется и не подлежит восстановлению. Каждый новый Акт о признании конкретного Пользователя, подписанный Сторонами, автоматически отменяет действие Сертификата данного Пользователя Подсистемы «Прямая интеграция», выпущенного ранее.

5.5. Оформленный со стороны Банка Акт о признании Клиента вручается лично представителю Клиента, курьеру Клиента, либо направляется Клиенту посредством почтовой связи. Акт о признании должен храниться у каждой из Сторон не менее 5 (Пяти) лет после окончания срока действия Комплекта ключей.

5.6. Обязательное аннулирование Сертификата проводится в случае Компрометации Ключей электронной подписи Клиента.

5.7. В случае лишения Клиентом Пользователя Подсистемы «Прямая интеграция» права подписывать ЭП Клиента ЭД, соответствующий Сертификат выводится из действия на основании письменного Заявления об отзыве (аннулировании) сертификатов пользователей Подсистемы «Прямая интеграция», составленного в свободном формате.

6. Обеспечение безопасности процедуры обмена документами

6.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

6.1.1 Использованием СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных ЗАО «Алладин Р.Д.» (сертификат соответствия № СФ/124-3956 от 17 ноября 2020 года). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к ключу электронной подписи осуществляется с использованием ПИН-кода доступа к токену;

6.1.2 СКЗИ КриптоПро CSP версии 4.x и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246), применяются криптографические алгоритмы шифрования в соответствии с ГОСТ 28147-89, обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с ГОСТ Р 34.11-94;

6.1.3 Удостоверения принадлежности сервера Подсистемы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО «КРИПТО-ПРО».

6.2. На основании дополнительных соглашений между Сторонами возможно применение других технических средств по защите информации.

6.3. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

6.3.1 Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

6.3.2 Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

6.3.3 Исключить использование средств удаленного администрирования;

6.3.4 Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана);

6.3.5 Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

6.3.6 Контролировать соблюдение требований безопасности.

6.4. Клиент обязан:

6.4.1 исключить появление в компьютере вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение Подсистемы «Прямая интеграция», скомпрометировать ключи Пользователя Подсистемы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;

6.4.2 исключить возможность Компрометации ключей в процессе их эксплуатации и хранения.

6.5. Стороны обязаны:

6.5.1 обеспечивать конфиденциальность Ключей электронной подписи, в частности не допускать использование принадлежащих им Ключей электронной подписи без их согласия;

6.5.2 уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении;

6.5.3 не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного Ключа нарушена.

6.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Подсистемы «Прямая интеграция» в случае появления обоснованных подозрений в наличии на компьютере Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия. Для возобновления работы Клиенту после удаления с компьютера Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия потребуется заново сгенерировать Сертификат и Ключ электронной подписи.

6.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

6.8. В случае Компрометации ключей любого Пользователя Клиента, Клиент обязан:

6.8.1 В случаях доступности Комплекта ключей (подозрение на несанкционированное копирование), а также в случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Подсистемы «Прямая интеграция» по телефону (телефон и электронный адрес Администратора Подсистемы «Прямая интеграция» указаны в Заявлении о настройке пользователей Подсистемы «Прямая интеграция») о факте Компрометации или угрозе Компрометации), используя для авторизации данные из Сертификата.

6.8.2 При этом, Администратор Подсистемы «Прямая интеграция» вправе произвести дополнительные действия по авторизации Пользователя Подсистемы «Прямая интеграция» (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае непредоставления информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Подсистеме «Прямая интеграция».

6.8.3 В срок не более 3 (Трех) рабочих дней после сообщения по телефону о факте Компрометации ключей, направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены ключей;

6.8.4 В случае принятия решения о замене Комплекта ключей – Клиент обязан сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации.

6.9. В случае Компрометации ключей Банка, последний обязан:

6.9.1 Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Подсистемы «Прямая интеграция» и смене Комплекта ключей Банка посредством Подсистемы «Прямая интеграция» с указанием даты и точного времени смены вышеуказанного Комплекта ключей;

6.9.2 Произвести внеплановую смену Комплекта ключей Банка и передать Сертификат ключа Банка Клиенту.

6.10. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного Клиента Банк немедленно приостанавливает использование Подсистемы «Прямая интеграция» данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде или с использованием иных, не связанных с Подсистемой «Прямая интеграция», средств дистанционного обслуживания.

6.11. Дальнейшее использование Подсистемы «Прямая интеграция» Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.

III. Порядок проверки ЭД и ЭП при разногласиях

7.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Клиента в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Клиента могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.

7.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.

7.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

7.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows8.1 и выше и программу криптографической проверки ЭП:

- для Подсистемы «ИКБ» - это предоставленная фирмой-разработчиком ЗАО «ИНИСТ» программа проверки ЭП, указанная в п.1.10 настоящего Порядка;
- для Подсистемы «Прямая интеграция» - это программа КриптоПро CSP версии 4.x и выше.

7.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД, действовавшие в момент создания спорного ЭД Сертификаты Стороны, подписавшей спорный ЭД, Банк обязан предоставить сами Сертификаты, записанные на съемном носителе в виде файлов в формате, применяемом Подсистемой «Прямая интеграция» (в случае если Клиент не предоставляет спорный ЭД, он предоставляется Банком).

7.4.2. Стороны обязаны предоставить все имеющиеся в их распоряжении Сертификаты, информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Подсистемы «Прямая интеграция», в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).

7.5. Средством подтверждения ЭП являются:

- для Подсистемы «ИКБ» Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими Ключами проверки электронной подписи;
- для Подсистемы «Прямая интеграция» Сертификаты ключей.

7.6. Члены Согласительной комиссии должны выполнить следующие действия:

7.6.1. Произвести с помощью программы криптографической проверки ЭП и средства подтверждения ЭП, использованного при подписании спорного ЭД, операцию проверки ЭП;

7.6.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, создаваемый Подсистемой «Прямая интеграция» в качестве результата проверки ЭП спорного ЭД (далее – Протокол). Протокол должен содержать распечатанные на бумажном носителе Сертификаты, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП спорного ЭД. Протокол должен быть подписан собственноручно всеми членами Согласительной комиссии;

7.6.3. Сравнить средства подтверждения ЭП с соответствующими средствами подтверждения ЭП, зафиксированными в Протоколе установления подлинности ЭП спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);

7.6.4. Установить, являлись ли средство подтверждения ЭП действующим на момент создания ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Сертификат признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Сертификата. В противном случае Сертификат признается недействующим на момент создания ЭП.

7.7. Согласительная комиссия признает Электронный документ подлинным, если одновременно выполнены условия:

7.7.1. Средства подтверждения ЭП совпадают с соответствующими средствами подтверждения ЭП, зафиксированными в Протоколе,

7.7.2. Все результаты проверки ЭП в Протоколе положительны,

7.7.3. Согласительная комиссия признала все средства подтверждения ЭП, содержащиеся в Протоколе, действующими на момент выработки ЭП.