Порядок организации электронных расчетов посредством Системы дистанционного банковского обслуживания BS-Client v.3

1. **Основные используемые понятия:**

1.1. **Акт признания ключа проверки электронной подписи** (**Акт признания ключа**) – документ, содержащий распечатку ключа проверки электронной подписи Клиента в шестнадцатеричной системе счисления, сведения о Клиенте – юридическом лице, сведения об Уполномоченном лице Клиента, обладающем правом использования ЭП, подписанный Клиентом и заверенный оттиском печати Клиента (Приложение № 3 к Правилам).

1.2. **Зарегистрированный ключ** - ключ проверки электронной подписи, размещенный в каталоге ключей, ключ проверки электронной подписи ЦУКС Банка.

1.3. **Зарегистрированный Клиент** - пользователь Системы ДБО, ключи проверки электронной подписи Уполномоченных лиц которого размещены в каталоге ключей проверки электронной подписи ЦУКС Банка.

1.4. **Запрос на выдачу Карточки регистрации Ключа проверки электронной подписи Уполномоченного лица Клиента** (**запрос на выдачу Карточки регистрации**) – электронный документ, подписанный действующим ключом ЭП Уполномоченного лица, который включает в себя новый ключ проверки электронной подписи Клиента. Запрос на выдачу Карточки регистрации создается средствами ЭП автоматически в процессе генерации новой пары ключей ЭП Уполномоченного лица.

1.5. **Интернет Клиент-Банк –** подсистема Системы ДБО. Подключение данной подсистемы позволяет организовать дистанционное банковское обслуживание наиболее простым способом с возможностью использования на мобильном или стационарном компьютере.

1.6. **Каталог ключей проверки электронной подписи** - совокупность действующих ключей проверки электронной подписи, наименований Клиентов и иной служебной информации.

1.7. **Плановая смена ключа ЭП –** процедура замены криптографического ключа Уполномоченного лица, проводимая по инициативе Клиента по истечении 12 (двенадцати) месяцев с момента выпуска соответствующей Карточки регистрации, не связанная с компрометацией ключа.

1.8. **Центр управления ключевыми системами (ЦУКС) Банка** – организационная структура Банка, выполняющая функции регистрации и ведения базы ключей проверки электронной подписи Клиентов.

2. **Общие положения.**

2.1. Настоящий документ устанавливает порядок организации и проведения обмена электронными документами, в частности электронных расчетов, между Банком и Клиентом.

2.2. Абонентский пункт Клиента состоит из персонального компьютера, общесистемного программного обеспечения и программного обеспечения Системы ДБО в составе и в соответствии с требованиями, указанными в Приложении № 2 к Соглашению.

2.3. Абонентский пункт Банка принимает документы, передаваемые Клиентом по Системе ДБО, а также размещает всю необходимую информацию для Клиента в Системе ДБО в автоматическом режиме.

2.4. Для обслуживания Системы ДБО Банк организует работу службы поддержки клиентов, в обязанности которой входит:

- обеспечение бесперебойной работы Системы ДБО;
- помощь при установке и настройке Клиентом программного обеспечения Системы ДБО;
- консультационная поддержка персонала Клиента;
- поддержка ключевого управления в Системе ДБО.

3. **Процедуры создания, обновления, регистрации и действия при компрометации ключей криптографической защиты.**

3.1. Процедуры регистрации и проверки ключей системы защиты информации происходят на базе ЦУКС Банка по адресу: 123100, Москва, Краснопресненская наб., д. 14.

3.2. Акты признания ключей оформляются отдельно на каждый ключ ЭП.

3.3. Дата и время ввода ключа в действие совпадает с датой и временем изготовления Банком соответствующей Карточки регистрации. Дата и время вывода ключей из действия определяется моментом вывода ключей Банком из действия в соответствии с Заявлениями Клиента, моментом завершения срока действия Карточки регистрации, либо датой и временем расторжения Соглашения. Вывод ключа из действия осуществляется:

- в случае изменения режима подписи Уполномоченного лица вывод из действия ключа со старым режимом подписи производится при обработке Заявления Клиента в ЦУКС Банка. Вывод из действия ключа со старым режимом подписи производится не позднее 18:00 в день размещения Карточки регистрации Уполномоченного лица с новым режимом подписи в Системе ДБО. После вывода ключа из действия все ЭПД, подписанные данным ключом, отбраковываются Системой ДБО;
- в случае плановой либо досрочной смены ключа Уполномоченного лица, а также в случае замены одного Уполномоченного лица другим вывод из действия старого ключа производится после успешного завершения Клиентом процедуры приема Карточки регистрации нового Ключа проверки электронной подписи. Банк выводит из действия старый ключ не позднее 18:00 московского времени рабочего дня, следующего за днём приёма Клиентом Карточки регистрации нового Ключа проверки электронной подписи;
- в случае отзыва прав Уполномоченного лица вывод из действия ключа производится не позднее рабочего дня, следующего за днём поступления Заявления Клиента в Банк. Использование выведенного из действия ключа в Системе ДБО невозможно.

3.4. При необходимости экстренного отзыва прав Уполномоченного лица Клиент оформляет Заявление о компрометации ключей системы защиты информации по форме Приложения № 7 к Соглашению. В указанном случае вывод ключа из действия осуществляется в максимально сжатые сроки.

Этапы работы	Исполнитель
Подключение Клиента. Выбор услуг ДБО.	
1. Подписание и передача в Банк Заявления на конфигурирование АРМ Системы ДБО. 2. Предоставление документов на Уполномоченных лиц.	Клиент
3. Изготовление копии Заявления Клиента, регистрация Заявления, предоставление Клиенту копии заявления с регистрационной информацией. 4. Заведение Клиента в системе ДБО, подготовка установочного комплекта для передачи Клиенту не позднее 5 рабочих дней с момента поступления Заявления в Банк. 5. Передача Клиенту установочного комплекта, согласно выбранному в Заявлении способом. Установочный комплект передается в соответствии с Приложением №4.	Банк
6. Установка необходимого для работы ПО. Перечень необходимого ПО и оборудования указан в Приложении № 2 данных правил. 7. Предоставление в Банк 2 (двух) экземпляров Акта приема-передачи, подписанного со стороны Клиента. 8. Генерация пары рабочих ключей ЭП (Ключа электронной подписи и Ключа проверки электронной подписи), формирование запроса на выдачу Карточки регистрации, передача запроса на выдачу Карточки регистрации в Банк по Системе ДБО. 9. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого ключа. Передача 3 (трех) экземпляров Акта в Банк. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента. 10. Печать, заполнение и подписание 2 (двух) экземпляров Акта о начале использования Системы ДБО. 11. Передача в Банк Актов признания каждого ключа и Актов о начале использования Системы ДБО.	Клиент
12. Сравнение Акта признания и запроса на выдачу Карточки регистрации. При положительном результате сравнения производится выдача Карточек регистрации и брелоков для генерации одноразовых паролей. 13. Подключение указанного Клиентом способа защиты Клиент-Банка, согласно п. 5 Заявления. Размещение Карточки регистрации в Системе ДБО для получения Клиентом. С данного момента Клиент считается Зарегистрированным и функционал системы ДБО доступен ему в полном объеме. 14. Подписание Актов приема-передачи со стороны Банка. 15. Подписание Акта о начале использования со стороны Банка.	Банк
Плановая смена рабочих ключей Клиента в процессе использования Системы ДБО.	

1. Генерация пары (ключ электронной подписи и ключ проверки электронной подписи) новых ключей ЭП, формирование запроса на выдачу Карточки регистрации, передача подписанного на действующем ключе ЭП запроса на выдачу Карточки регистрации в Банк по Системе ДБО. Предоставления Заявления на конфигурирование Системы ДБО не требуется. 2. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого ключа. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента. 3. Передача документов в Банк.	Клиент
4. Сравнение Акта признания и запроса* на выдачу Карточки регистрации. При положительном результате сравнения выдача Карточки регистрации. Размещение Карточки регистрации в Системе ДБО для получения Клиентом. ** Запрос Клиента на выдачу Карточки регистрации хранится в Банке в течение 180 (ста восьмидесяти) дней, после чего аннулируется.*	Банк
Внеплановая смена рабочих ключей Клиента в процессе использования Системы ДБО.	
1. Подписание и передача в Банк Заявления на конфигурирование АРМ Системы ДБО. Заявление должно содержать требование одновременного внесения следующих изменений перечня Уполномоченных лиц, режимов подписи: • вывести из действия (отключить) используемые ключи; • изготовить новые (подключить) профили. 2. После передачи в Банк Заявления на конфигурирование АРМ Системы ДБО необходимо действовать в порядке: • установленном для начального подключения, в случае заказа восстановления начальных настроек; • установленном для плановой смены рабочих ключей Клиента в процессе использования Системы ДБО, в остальных случаях.	Клиент
Компрометация ключа Уполномоченного лица Клиента.	
1. Клиент оформляет Заявление о компрометации ключей системы защиты информации и передает в Банк по факсу, электронной почте или нарочным в офис Банка.	Клиент
2. Банк производит временное блокирование ключей Клиента.	Банк
3. Клиент передаёт оригинал Заявления о компрометации ключей системы защиты информации в Банк.	Клиент
4. В случае если оригинал Заявления компрометации ключей не поступил в Банк до окончания рабочего дня, следующего за днём временного блокирования ключей, работа в Системе ДБО с использованием временно заблокированных ключей возобновляется. 5. При поступлении в Банк оригинала Заявления о компрометации ключей системы защиты информации Банк фиксирует факт компрометации ключей Клиента и блокирует дальнейшее использование скомпрометированных ключей. Дальнейшее использование скомпрометированного ключа возможно только в качестве технологического.	Банк
6. Клиент проводит обновление ключей, зарегистрированных в ЦУКС Банка, в порядке, установленном для внеплановой смены ключа.	Клиент
Добавление Уполномоченного лица, изменение режима подписи.	
1. Оформление и передача в Банк 1 (одного) экземпляра Заявления на конфигурирование АРМ Системы ДБО и необходимых документов на Уполномоченные лица.	Клиент
2. Генерация Профиля Ключа Клиента для каждого Уполномоченного лица.	Банк
3. Генерация пары (ключ электронной подписи и ключ проверки электронной подписи) рабочих ключей ЭП, формирование запроса на выдачу Карточки регистрации, передача запроса на выдачу Карточки регистрации в Банк по Системе ДБО. 4. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого	Клиент

ключа. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента. 5. Передача 3 (трех) экземпляров Акта признания ключа в Банк.	
6. Проверка Акта признания, Заявления на внесение изменений в Систему ДБО и запроса на выдачу Карточки регистрации. При положительном результате проверки производится выдача Карточки регистрации. 7. Размещение Карточки регистрации в Системе ДБО для получения Клиентом. С данного момента ключ Клиента считается Зарегистрированным и функционал системы ДБО доступен ему в полном объеме.	Банк
Расторжение Соглашения.	
1. Исключение ключей Клиента из каталога ключей ключа проверки электронной подписи Банка. 2. Блокирование работы Клиента в Системе ДБО.	Банк

4. **Безопасное использование систем дистанционного банковского обслуживания.**

4.1. Клиент должен самостоятельно генерировать криптографические ключи.

4.2. Закрытые криптографические ключи должны храниться на съемных носителях информации в недоступном неуполномоченным лицам месте. Ключевые носители должны извлекаться из хранилища только на время непосредственного использования. Ключевые носители не должны быть доступны для посторонних лиц от момента генерации до момента уничтожения ключей. Ответственность за организацию надлежащего хранения закрытых ключей Клиента несет Клиент.

4.3. Для резервных копий ключевых носителей необходимо соблюдение тех же правил обращения с ними, которые установлены для основных носителей.

4.4. После выведения закрытых криптографических ключей из действия такие ключи должны уничтожаться.

4.5. При возникновении подозрения на компрометацию пароля входа в Систему ДБО или криптографических ключей такой пароль или ключи должны быть немедленно заменены. Криптографические ключи должны меняться ежегодно в плановом порядке.

4.6. Использование для работы в Системе ДБО гостевых рабочих мест (интернет-кафе и т.п.) не рекомендуется по причине повышенного риска кражи криптографических ключей и паролей доступа.

4.7. При невозможности установления связи с серверами ДБО Банка Клиенту следует обратиться в Единый Центр сопровождения ДБО Банка.

4.8. Необходимо строго соблюдать требования по организационному обеспечению эксплуатации СКЗИ, требования по размещению СКЗИ и режиму охраны, требования по обеспечению безопасности ключевой информации, содержащиеся в документации на СКЗИ.

4.9. Необходимо обеспечить защиту от рисков, связанных с распространением вредоносного программного обеспечения. Меры по защите рабочего места Системы ДБО должны включать:

- использование только лицензионного программного обеспечения, получаемого из надежных источников;
- своевременную установку обновлений безопасности используемого программного обеспечения (операционная система, веб браузер, офисное программное обеспечение и т.п.);
- использование только необходимого для работы программного обеспечения;
- использование регулярно обновляемого антивирусного программного обеспечения;
- использование средств сетевой защиты (межсетевого экрана) и средств обнаружения вторжений (IDS/IPS);
- ограничение использования публичных сетей, файлового обмена и сообщений электронной почты;
- контроль целостности исполняемых файлов и файлов конфигураций;
- использование многофакторной авторизации, согласованных с Банком идентификационных признаков компьютера Клиента (фильтрация по IP и MAC адресам, одноразовых паролей на брелоках eToken PASS) и иных дополнительных средств обеспечения безопасности, предоставляемых Банком;
- проведение плановой перегенерации ключей ЭП не реже одного раза в 15 (пятнадцать) месяцев;
- установку пароля на контейнер ЭП в СКЗИ;
- своевременное обновление клиентского программного обеспечения системы ДБО до рекомендованной Банком в информационных письмах версии;
- использование безопасного входа в подсистему «Интернет-Клиент» ДБО через виртуальную клавиатуру;

- осуществление смены пароля Клиента на вход в Систему ДБО и контейнер СКЗИ не реже 1 (одного) раза в квартал;
- недопущение установки ранее использованных, коротких и простых (менее 3 (трех) групп символов) паролей;
- незамедлительное информирование Банка о хищении или компрометации средств идентификации, ключей ЭП Клиента в Системе ДБО;
- другие меры, признанные целесообразными.

4.10. Необходимо обеспечить защиту от несанкционированного доступа к оборудованию и программному обеспечению СКЗИ третьих лиц.

4.11. Размещение, специальное оборудование, охрана и организация режима в помещениях, в которых установлены СКЗИ или хранятся криптографические ключи, должны обеспечивать сохранность СКЗИ и криптографических ключей. Такие помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие (для юридических лиц - в том числе в нерабочее время). Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в такие помещения посторонних лиц, необходимо оборудовать металлическими решетками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению.

5. Порядок передачи и приема документов по Системе ДБО.

5.1. Инициатором проведения всех расчетных операций, получения информации по Системе ДБО, смены ключей Клиента является Клиент, для чего он формирует соответствующие запросы, в ответ на которые Банк предоставляет затребованную либо принимает переданную информацию.

5.2. Информация, размещенная Банком в Системе ДБО, становится доступной для Клиента с момента размещения при условии установления Клиентом авторизованного сеанса связи с Банком по Системе ДБО.

5.3. После идентификации и аутентификации Клиент получает доступ к Системе ДБО и начинает работу с ней.

5.4. Клиент запрашивает и получает выписки, служебные сообщения, а также иную информацию, адресованную ему Банком.

5.5. Клиент запрашивает информацию и заполняет формы электронных документов и справочников, а Банк, осуществляет проверку правильности их заполнения и либо выдает служебные сообщения об ошибках, либо сохраняет переданные документы, записи справочников.

5.6. Уполномоченные лица Клиента подписывают электронные документы электронной подписью. Электронная подпись подтверждает авторство отправленного по Системе ДБО документа и гарантирует его целостность, т.к. любое изменение в документе после его подписания делает электронную подпись некорректной.

5.7. Основанием для принятия к исполнению Банком переданного Клиентом по Системе ДБО платежного документа является наличие подтверждения на исполнение ЭПД в виде необходимого количества корректных ЭП данного ЭД, а также соответствие ЭПД требованиям к оформлению платежных документов.

5.8. Проверка корректности ЭД осуществляется Банком в следующем порядке:

- ЭД Клиента, поступивший в ЦАП, автоматически расшифровывается и проходит автоматическую проверку на наличие и подлинность (корректность) зарегистрированных ЭП Клиента;
- при положительном результате расшифрования ЭД и проверки ЭП электронный документ передается в Систему ДБО для дальнейшей обработки;
- при передаче ЭПД в Систему ДБО происходит автоматическая проверка его реквизитов и, если Система ДБО не фиксирует ошибки, ЭПД передается в автоматизированную банковскую систему (АБС) Банка для исполнения.

При отрицательном результате одной из проверок Банк не принимает ЭД и формирует для Клиента соответствующее сообщение об ошибке.

5.9. Принятый к исполнению Банком ЭПД подлежит исполнению в порядке проведения расчетных операций, предусмотренных соответствующим Договором банковского счета / иным договором.

5.10. В случае отрицательного результата какой-либо проверки Клиент получает об этом служебное электронное сообщение. Система ДБО автоматически отражает сведения о текущем состоянии документов Клиента в Банке (получении, приеме к исполнению и исполнении или неисполнении документа) посредством изменения статусов электронных документов.

5.11. Информация по электронным документам, оформленным с нарушением требований, размещается Банком в Системе ДБО с указанием причины, по которой не принят документ.

5.12. По отдельным платежным документам Банк вправе запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе ДБО, либо иным образом в день получения платежного документа. В этом случае платежный документ принимается к исполнению после получения требуемого подтверждения.

5.13. Электронный документ валютного контроля передается и принимается в соответствии с требованиями валютного законодательства Российской Федерации в области валютного регулирования и валютного контроля.
Датой принятия/отправления электронного документа валютного контроля является дата его получения/направления Банком, зафиксированная Системой ДБО.

Отказ в принятии электронного документа валютного контроля по причине несоответствия направленных документов требованиям валютного законодательства направляется Клиенту в сроки, установленные нормативными актами органов валютного контроля.

5.14. Информирование Клиента о совершенных с использованием Системы ДБО операциях осуществляется путем автоматического направления Банком уведомлений по Системе ДБО об изменениях статуса каждого платежного документа.

6. **Порядок разрешения споров и рассмотрения претензий.**

6.1. **Порядок разрешения споров относительно подлинности электронных документов.**

6.1.1. Разрешение споров относительно подлинности ЭД осуществляется на основании результатов проверки ЭП Клиента под электронным документом. Электронный документ Клиента считается подлинным, если он надлежащим образом оформлен, снабжен необходимым количеством корректных ЭП и размещен Клиентом в Системе ДБО.

6.1.2. Оспаривающий подлинность электронного документа Клиент направляет в Банк обоснованную претензию в письменном виде,

6.1.3. По результатам рассмотрения претензии Банк предоставляет Клиенту ответ в письменном виде в течение 15 (пятнадцати) рабочих дней со дня получения претензии.

6.1.4. В случае согласия Банка с полученной претензией, Стороны проводят переговоры по урегулированию разногласий.

6.1.5. В случае несогласия Банка с полученной претензией в отношении подлинности ЭД и письменного требования Клиента о создании Экспертной комиссии Банк письменно сообщает Клиенту контактную информацию своего представителя, уполномоченного представлять интересы Банка в Экспертной комиссии. Такая информация указывается в ответе на претензию либо направляется Клиенту в течение 3 (трех) рабочих дней с даты получения требования от Клиента о создании Экспертной комиссии.

6.1.6. Неполучение в установленный срок Клиентом ответа на претензию признается Сторонами как несогласие Банка с претензией.

6.1.7. Экспертная комиссия создается Сторонами в течение 3 (трех) рабочих дней со дня получения Клиентом информации о представителе, уполномоченного представлять интересы Банка в Экспертной комиссии. В указанный срок Клиент обязан уведомить Банк о назначении своего представителя, уполномоченного представлять интересы Клиента в Экспертной комиссии, предоставить в Банк его контактные данные и организовать участие в экспертизе представителя фирмы-изготовителя программного обеспечения средств ЭП - Председателя Экспертной комиссии. Оплата услуг производится Клиентом с последующим отнесением расходов на виновную сторону.

6.1.8. В случае если одна из Сторон не назначает представителя в Экспертную комиссию в установленный срок либо иначе уклоняется от участия в работе Экспертной комиссии, Экспертная комиссия создается при участии двух представителей фирмы-изготовителя программного обеспечения средств ЭП, причем участие одного из представителей фирмы-изготовителя программного обеспечения осуществляется за счет Стороны, уклоняющейся от участия в Экспертной комиссии независимо от результатов разрешения спора.

6.1.9. Стороны по требованию Экспертной комиссии предоставляют ей документы и сведения, необходимые последней для разрешения спора.

6.1.10. Экспертная комиссия осуществляет свою работу на территории Банка с использованием эталонной ПЭВМ (персональный компьютер, свободный от вирусов), эталонного программного обеспечения.

6.1.11. Эталонное оборудование и программное обеспечение предоставляется Банком. Эталонное программное обеспечение состоит из операционной системы, программного

обеспечения средств ЭП, применяемых в Системе ДБО, и программного обеспечения Системы ДБО. По требованию Клиента программное обеспечение средств ЭП и Системы ДБО может предоставляться разработчиками.

6.1.12. Представитель Банка предоставляет документы, являющиеся надлежащими доказательствами соответствующих фактов при рассмотрении споров:

- Акт о начале использования Системы ДБО;
- спорный ЭД в виде файла, экспортированного из базы данных входящих ЭД, а также протоколы работы Системы ДБО;
- электронные Карточки регистрации действующих Ключей проверки электронной подписи;
- Акт признания ключа проверки электронной подписи;
- Заявления на конфигурирование АРМ Системы ДБО;
- Заявления о компрометации ключей системы защиты информации;
- журналы работы Системы ДБО, в которых отражены моменты принятия Карточки регистрации Ключа проверки электронной подписи Уполномоченного лица Клиентом;
- полученную претензию Клиента и ответ Банка по результатам ее рассмотрения;
- иные документы при необходимости.

6.1.13. Представитель Клиента предоставляет следующие документы, являющиеся надлежащими доказательствами соответствующих фактов при рассмотрении споров:

- Заявления на конфигурирование АРМ Системы ДБО с отметками Банка о принятии;
- Заявления о компрометации ключей системы защиты информации с отметками Банка о принятии;
- документы, свидетельствующие о расторжении Соглашения;
- иные документы при необходимости.

В присутствии членов Экспертной комиссии представитель Банка инсталлирует эталонное программное обеспечение на эталонную ПЭВМ.

6.1.14. Экспертная комиссия убеждается в работоспособности компьютера и программного обеспечения и производит действия по разрешению спора, на основании которых принимает решение относительно подлинности электронных документов.

6.1.15. Экспертная комиссия оформляет свое решение в виде акта, который подписывается лично всеми членами комиссии и вручается под роспись уполномоченного лица Клиенту и Банку или направляется путем почтового сообщения с уведомлением о вручении.

6.1.16. Акт комиссии является окончательным и пересмотру не подлежит. Решение, содержащееся в акте, обязательно для исполнения обеими Сторонами. В случае уклонения какой-либо Стороны от исполнения решения, содержащегося в Акте, другая Сторона может потребовать исполнения такого решения через Арбитражный суд Российской Федерации.

6.2. Порядок разрешения споров, связанных с совершением расчетных операций с использованием Системы ДБО без согласия Клиента.

6.2.1. При оспаривании расчетной операции, совершенной с использованием Системы ДБО без согласия Клиента (неуполномоченным лицом), Клиент предоставляет в Банк Заявление об использовании ключей защиты информации без согласия Клиента по форме Приложения № 9 к Соглашению с приложением Справки по факту инцидента информационной безопасности в Системе ДБО (далее – Претензия).

6.2.2. При получении Претензии Банк:

- предпринимает предусмотренные законодательством меры по возврату денежных средств путем обращения в банк-получателя;
- проводит внутреннее расследование, в том числе производит идентификацию оспоренного электронного документа в Системе ДБО и проверяет его подлинность.

6.2.3. По результатам рассмотрения Претензии и предпринятых действий Банк предоставляет Клиенту ответ в письменном виде в течение 15 (пятнадцати) рабочих дней со дня получения Претензии.

7. Порядок проверки подлинности электронного документа.

7.1. Установление факта соответствия спорного ЭД, представленного Банком, предмету спора.
7.2. Установление круга лиц, уполномоченных Клиентом на подписание ЭП спорного ЭД на момент генерации ЭП спорного ЭД.
7.3. Проверка соответствия принадлежности ключей проверки электронной подписи Клиента, предоставленных Банком для проведения проверки, перечню Уполномоченных лиц.
7.4. Проверка действительности представленных Банком ключей проверки электронной подписи Клиента на момент выработки каждой ЭП.
7.5. Проверка корректности ЭП спорного ЭД.
7.6. Установление соответствия всех ЭП спорного ЭД их заявленному назначению (ЭП группы А, ЭП группы Б, единственная ЭП).
7.7. Установление соответствия шестнадцатеричных значений задействованных в проверке ключей проверки электронной подписи Клиента с соответствующими значениями, указанными в Актах признания.
7.8. Спорный электронный документ признается подлинным тогда и только тогда, когда одновременно выполнены все условия:

- Банком представлен ЭД, соответствующий предмету спора;
- ключи проверки электронной подписи Клиента, предоставленные Банком для проведения проверки, зарегистрированы за Уполномоченными лицами;
- ключи проверки электронной подписи действовали в момент генерации соответствующих ЭП, т.е. на момент исполнения спорного ЭД в Банк не поступало Заявлений о компрометации соответствующих ключей защиты информации;
- спорный ЭД содержит необходимое количество ЭП согласно их назначению;
- все ЭП спорного ЭД корректны;
- шестнадцатеричные значения задействованных ключей проверки электронной подписи Клиента соответствуют значениям, указанным в Актах признания.

8. Особенности функционирования подсистемы Системы ДБО.

8.1. Интернет Клиент-Банк
8.1.1. Клиент устанавливает программное обеспечение подсистемы «Интернет Клиент Банк», представляющее собой набор элементов ActiveX, а также средства криптографической защиты информации на своем компьютере. Все электронные документы совместно с ЭП хранятся в системе управления базами данных (СУБД) Банка. СУБД на стороне Клиента не устанавливается.
8.1.2. При подключении к подсистеме Клиенту предоставляется 1 (один) комплект криптографических ключей: с правом единственной подписи или с разделенными правами ЭП групп А и Б.
8.1.3. В целях обеспечения возможности одновременного использования подсистемы разными Уполномоченными лицами по заявке Клиента Банк предоставляет дополнительные рабочие места (логины).
8.1.4. При подключении к подсистеме Клиент должен соблюдать следующие способы обеспечения дополнительной безопасности:
- фильтрация подключений Клиента - Клиент указывает параметры подключения Клиента (IP, MAC адреса), подлежащие контролю со стороны Банка,
- использование дополнительных средств аутентификации по одноразовым паролям - Клиент получает по одному брелоку OTP на каждый используемый им криптографический ключ единственной подписи либо подписи группы А.

8.1.5. При контроле Банком параметров подключения Клиента (IP, MAC адреса) Банк разрешает только соединения, параметры которых соответствуют заявленным Клиентом в Приложении № 3 к Соглашению.
8.1.6. При использовании дополнительных средств аутентификации по одноразовым паролям (OTP) при отказе от ввода такого пароля Клиент получает доступ в подсистему с ограниченными правами – не разрешена генерация ЭП электронных документов. При этом в целях использования каждого зарегистрированного брелока OTP Банк предоставляет Клиенту отдельное рабочее место (логин).
8.1.7. Для создания ЭД Клиент устанавливает сеанс связи с Банком, аутентифицируется в Системе ДБО при помощи пароля и ключа подписи, производит действия по созданию,

получению ЭД, выработке ЭП созданных ЭД. Все сохраненные Клиентом ЭД, а также их ЭП сохраняются в базе данных Банка.

8.1.8. ЭД, снабженный необходимым количеством ЭП Клиента, поступает в обработку в Банке после выполнения Клиентом необходимых действий по его передаче к исполнению.

8.1.9. В случае указания в Заявлении на конфигурирование АРМ необходимости предоставления доступа к счёту в режиме «только просмотр» Банк блокирует возможность управления данным счётом через указанные в Заявлении подсистемы ДБО.

8.1.10. Банк принимает документы, передаваемые Клиентом через информационно-коммуникационную сеть Интернет, а также размещает всю необходимую информацию в персонализированном разделе веб сервера Системы ДБО в автоматическом режиме. Данный раздел доступен Клиенту после прохождения процедуры авторизации.

8.1.11. Банк обязан размещать всю информацию, предназначенную для получения Клиентом в подсистеме на персонализированной странице интернет-сервера Системы ДБО.

8.1.12. Информация по электронным документам, оформленным с нарушением требований, размещается Банком на интернет-сервере Системы ДБО в день получения переданного Клиентом на исполнение документа, с указанием причины, по которой документ не принят.

8.1.13. Поток всех передаваемых между Клиентом и Банком данных шифруется с помощью протокола SSL.

8.1.14. Установление соединения производится Клиентом. Адрес сервера Банка: https://dbo.bank-peresvet.ru.

8.1.15. Количество разрешенных одновременных соединений Клиента с сервером ДБО Банка определяется числом лицензий, запрошенных Клиентом в Заявке на подключение Системы ДБО.

8.1.16. Системой ДБО могут присваиваться следующие статусы ЭД Клиента:

Статус ЭД	**Описание статуса**
новый	вновь созданный или импортированный документ, успешно прошедший проверку всех контролей Системы ДБО
импортирован	статус присваивается импортированному из бухгалтерской системы (БС) документу, в котором были обнаружены ошибки
подписан	документ подписан всеми требуемыми подписями
подписан I	документ подписан ЭП группы А из двух требуемых
подписан II	документ подписан ЭП группы Б из двух требуемых
в обработке	документ принят Системой ДБО со стороны Банка, производится его передача в АБС
принят АБС	документ успешно прошел проверку всех контролей АБС и передан на исполнение операционисту
отказан АБС	документу, переданному в АБС, отказано в исполнении, обоснование отказа можно увидеть в поле «Сообщение банка» (Комментарий банка) при просмотре документа
исполнен	документ исполнен
не принят	документ был удален
удален	документ был удален