УТВЕРЖДЕНЫ
Приказом «Запсибкомбанк» ОАО
от «09» декабря 2009г. №284

Правила
обслуживания Клиентов с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)
от «09» декабря 2009 г. №21/1045
(с изменениями и дополнениями №1 от «07» октября 2010г., изменениями и дополнениями № 2 от «20» апреля 2011г., с изменениями № 3 от «28» июня 2011г., с изменениями № 4 от «31» августа 2011 года, с изменениями № 5 от «29» декабря 2011 г., изменениями № 6 от «02» июля 2012 г., изменениями № 7 от «29» декабря 2012 г., изменениями № 8 от «13» августа 2013 г., с изменениями №9 от «31» декабря 2013г.)

1. Общие положения

1.1. «Правила обслуживания Клиентов с использованием Интернет-технологий (система ДБО «Интернет-Банк») (далее - Правила) определяют порядок обслуживания Клиентов с использованием Интернет-технологий (система ДБО «Интернет-Банк»).
1.2. Правила являются неотъемлемой частью Договора о дистанционном банковском обслуживании с использованием Интернет-технологий (система ДБО «Интернет-Банк») (далее – Договор ДБО).
1.3. Все Приложения к настоящим Правилам являются неотъемлемой их частью и обязательны для исполнения Банком и Клиентом.
1.4. Термины, применяемые в тексте настоящих Правил, используются в следующем значении:
Администратор Сертификационного Центра Банка – сотрудник Банка, в обязанности которого входит создание и выдача сертификатов ключей проверки электронной подписи.
Банк – Акционерный Западно-Сибирский коммерческий банк открытое акционерное общество («Запсибкомбанк» ОАО), его филиалы, дополнительные офисы, операционные офисы и иные внутренние структурные подразделения (участник Системы дистанционного банковского обслуживания «Интернет-Банк»).
Владелец сертификата ключа проверки электронной подписи – лицо, на имя которого Сертификационным Центром Банка выдан сертификат ключа проверки электронной подписи и которому принадлежат соответствующие ключи электронной подписи, позволяющие с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы электронной подписью).
Внеплановая смена ключа электронной подписи - смена ключа электронной подписи, вызванная его компрометацией, а также в случае, когда уполномоченное лицо Клиента меняет существующий ключевой носитель на Rutoken ЭЦП 64 Кб до момента истечения срока действия сертификата ключа проверки электронной подписи.
Доставка электронного документа – физический процесс перемещения электронного документа от отправителя к получателю.
Клиент (владелец сертификата ключа проверки электронной подписи) – юридическое лицо, индивидуальный предприниматель без образования юридического лица или физическое лицо, занимающееся (-ийся) в установленном законодательством Российской Федерации порядке частной практикой, заключившие (-ий) с Банком Договор банковского счета в рублях и/или иностранной валюте и Договор о дистанционном банковском обслуживании с использованием Интернет-технологий (система ДБО “Интернет-Банк»)(участник Системы ДБО) которому, как участнику Системы ДБО «Интернет-Банк», выдан сертификат ключа проверки электронной подписи.
Ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи – участнику Системы ДБО и предназначенная для создания электронной подписи и шифрования электронного документа с использованием средств электронной подписи.
Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи, доступная участникам Системы ДБО и

предназначенная для шифрования электронного документа и подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Ключевой носитель – информационный носитель, содержащий криптографические ключи.

Компрометация ключа электронной подписи – нарушение конфиденциальности, угроза доступа неуполномоченных лиц (лиц, не имеющих права первой и\или второй подписи банковских документов Клиента, не наделенных правом распоряжения денежными средствами, находящимися на счете, с использованием электронной подписи (аналога собственно ручной подписи)). К событиям, связанным с нарушением конфиденциальности, компрометацией ключа электронной подписи, относятся следующие события:

- утрата ключевых носителей;
- утрата ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения ключа электронной подписи;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате чьих-либо несанкционированных действий).

Корректная электронная подпись Клиента – электронная подпись электронного документа, проверка которой с использованием соответствующего ключа проверки электронной подписи дает положительный результат, которая соответственно обладает свойствами:

- уникальна для подписанного документа при использовании ключа электронной подписи;
- подлинность ее может быть удостоверена Банком и Клиентом;
- она неразрывно связана с конкретным документом и только с ним.

Криптографические ключи – общее название ключей проверки электронной подписи и ключей электронной подписи.

Личный кабинет – индивидуальный раздел клиента в Системе, доступ к которому осуществляется по защищенному соединению.

Отправитель электронного документа – физическое или юридическое лицо, индивидуальный предприниматель, которое (-ый) непосредственно направляет или от имени которого направляется электронный документ, за исключением лиц, действующих в качестве информационных посредников в отношении этого документа.

Перевод денежных средств - действия Банка в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Плановая смена ключа электронной подписи – смена ключа электронной подписи, вызванная окончанием срока действия сертификата ключа проверки электронной подписи, по истечению 1 (одного) года 3 (трех) месяцев с момента выдачи Банком сертификата ключа проверки электронной подписи.

Получатель электронного документа – физическое или юридическое лицо, индивидуальный предприниматель, которому электронный документ отправлен самим отправителем или от имени отправителя за исключением лиц, действующих в качестве информационных посредников в отношении этого документа.

Сертификат ключа проверки электронной подписи – документ на бумажном носителе с собственноручной подписью или электронный документ с электронной подписью администратора Сертификационного Центра Банка, который включает в себя ключ проверки электронной подписи и который выдается администратором Сертификационного Центра Банка уполномоченному лицу участника Системы ДБО для подтверждения принадлежности электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификационный Центр Банка – подразделение Департамента информационных технологий Банка, в обязанности которого входит создание и выдача сертификатов ключей проверки электронных подписей (удостоверяющий центр).

Система дистанционного банковского обслуживания «Интернет-Банк» (далее – Система ДБО) – автоматизированная компьютерная система, позволяющая Клиенту осуществлять передачу электронных документов в Банк по сети Интернет. При использовании данной системы

все электронные документы хранятся на сервере Системы ДБО. Система ДБО устанавливается на любое рабочее место или несколько рабочих мест, имеющих доступ к сети Интернет. Действия по подготовке электронных документов Клиент производит на сайте Банка, являющемся составной частью комплекса обслуживания Клиента с использованием Системы ДБО.
Система ДБО является информационной, коммуникационной и операционной, поскольку предоставляет Клиенту возможность совершать расходные операции по его счету путем оформления распоряжений о переводе денежных средств и направления их в Банк, а также получать выписки по счету, обмениваться официальными письмами с Банком и распечатывать платежные поручения, согласно которым Банком осуществляется зачисление средств на счет Клиента.
Средства криптографической защиты информации (далее по тексту - СКЗИ) – совокупность программно-технических средств, обеспечивающих применение электронной подписи и шифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.
Средства электронной подписи (далее по тексту - СЭП) – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждение с использованием сертификата ключа проверки электронной подписи подлинности электронной подписи в электронном документе, создание ключей проверки электронной подписи и ключей электронной подписи. СЭП могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.
Трансграничный перевод денежных средств - перевод денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.
Уполномоченные лица - лица, имеющие право первой и/или второй подписи банковских документов Клиента, наделенные правом распоряжения денежными средствами, находящимися на его счете, допущенные Клиентом к работе с Банком в Системе ДБО с использованием электронной подписи (аналога собственноручной подписи) в пределах срока полномочий лиц, указанных в карточке с образцами подписей и оттиска печати.
Формат электронного документа – перечень реквизитов (полей) документа и правил их заполнения.
Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного электронного документа.
Электронная подпись (далее - ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Усиленная неквалифицированная электронная подпись – электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с помощью средств электронной подписи.

В настоящих Правилах под электронной подписью понимается усиленная неквалифицированная электронная подпись.
Электронный документ (далее по тексту - ЭД) – информация, подписанная ЭП и представленная в электронно-цифровой форме, пригодной для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
Электронный документооборот – это система ведения документации, при которой весь массив создаваемых, передаваемых и хранимых документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сетевую структуру,

предусматривающую возможность формирования и ведения распределенной базы данных, в которой ЭД признается приоритетным над бумажным документом, создается, корректируется и хранится в компьютере. Обмен электронными документами включает в себя:

- формирование ЭД в формате, установленном для данного ЭД;
- регистрацию ЭД;
- проверку ЭД на соответствие установленному формату, а также на предмет подлинности всех электронных подписей ЭД;
- подтверждение получения ЭД;
- отзыв ЭД;
- учет электронных документов (регистрацию входящих и исходящих электронных документов);
- хранение электронных документов (ведение архивов электронных документов);
- создание дополнительных экземпляров ЭД;
- создание бумажных копий ЭД.

Rutoken ЭЦП 64 Кб – физический носитель, предназначенный для хранения ключа электронной подписи и ключа проверки электронной подписи, являющийся персональным средством аутентификации уполномоченного лица Клиента и обеспечивающий доступ к распоряжению счетом и обмену электронными документами по Системе ДБО.

2. Общие положения об обеспечении Клиентам доступа к Системе ДБО

2.1. Порядок ввода Системы ДБО в эксплуатацию

2.1.1. Основанием ввода Системы ДБО в эксплуатацию является заключенный между Банком и Клиентом Договор ДБО при условии предварительного оформления Заявления о регистрации в Реестре пользователей Сертификационного Центра Банка (Приложение 1 к настоящим Правилам).
2.1.2. В согласованные с Клиентом сроки, но не позднее 1 (одного) месяца с момента оформления и передачи в Банк Заявления о регистрации в Реестре пользователей Сертификационного Центра Банка, Банк предоставляет Клиенту:

– программное обеспечение для защиты передаваемой информации по каналам связи - InterPRO Client;

– необходимые пароли и идентификаторы для доступа к Системе ДБО - пароль для входа в Систему ДБО, код пользователя Системы ДБО;

– ключевой носитель Rutoken ЭЦП 64 Кб в необходимом количестве;

– драйвер Rutoken ЭЦП 64 Кб, а также программное обеспечение для генерации ключей ЭП на Rutoken ЭЦП 64 Кб - AdminPKI.

2.1.3. Рабочее место Клиента, с которого осуществляется работа в Системе ДБО должно соответствовать требованиям, изложенным в пп. 6.2. настоящих Правил и Приложении 2 к настоящим Правилам.
2.1.4. При открытии Клиенту нового счета (расчетного, текущего\транзитного валютного счета) обслуживание Клиента с использованием Системы ДБО по вновь открытому счету осуществляется на основании Заявления (Приложение 3 к настоящим Правилам). Оформленное Клиентом Заявление передается в Банк на бумажном носителе либо в виде ЭД, заверенного ЭП уполномоченного лица Клиента и отправленного в Банк с использованием Системы ДБО.

2.2. Порядок предоставления Банком Rutoken ЭЦП 64 Кб

2.2.1. В качестве ключевого носителя Клиент в обязательном порядке использует Rutoken ЭЦП 64 Кб. Допускается хранение ключей ЭП на прочих отчуждаемых носителях (дискетах, флэш-картах) для Клиентов Банка, заключивших Договор ДБО до «01» июля 2011 года, до момента плановой или внеплановой смены ключа ЭП. При плановой или внеплановой смене ключа ЭП начиная с «01» июля 2011 года Клиенты Банка в обязательном порядке используют в качестве ключевого носителя Rutoken ЭЦП 64 Кб.
2.2.2. Для получения Rutoken ЭЦП 64 Кб уполномоченное лицо Клиента предварительно оформляет Заявление о регистрации в Реестре пользователей Сертификационного Центра Банка (Приложение 1 к настоящим Правилам) и передает его в Банк.

Клиенты, впервые заключающие Договор ДБО и оформившие Заявление о регистрации в Реестре пользователей Сертификационного Центра Банка (Приложение 1 к настоящим Правилам)

в соответствии с п. 2.1.1. настоящих Правил, повторно указанное Заявление (Приложение 1 к настоящим Правилам) в Банк не предоставляют.

2.2.3. Банк передает Клиенту Rutoken ЭЦП 64 Кб после проверки работоспособности ключевого носителя (выполняется сотрудником Банка) и подписания Акта приема-передачи обеими сторонами (Приложение 4 к настоящим Правилам).

Акт приема-передачи оформляется в двух экземплярах. Один экземпляр Акта приема-передачи остается у Клиента, второй экземпляр хранится в Банке и прилагается к Договору ДБО.

2.2.4. Передача Rutoken ЭЦП 64 Кб осуществляется Банком руководителю Клиента. Передача Rutoken ЭЦП 64 Кб прочим лицам осуществляется на основании доверенности, оформленной по форме Приложения 5 к настоящим Правилам.

2.2.5. Использование в качестве ключевых носителей Rutoken ЭЦП 64 Кб, полученных Клиентом не в Банке, запрещается.

2.2.6. Одному Клиенту может быть выдано несколько Rutoken ЭЦП 64 Кб в соответствии с Тарифами Банка.

2.3. Порядок подключения сервисов безопасности Системы ДБО

2.3.1. К сервисам безопасности Системы ДБО относятся:

– дополнительный уровень авторизации пользователей Системы ДБО путем ввода одноразового пароля для входа в Систему ДБО, который направляется Банком Клиенту посредством SMS на сотовый телефон.

– сервис по информированию пользователей с помощью SMS на сотовый телефон об успешном подключении к Системе ДБО.

2.3.2. Для подключения сервисов безопасности Системы ДБО Клиенту необходимо оформить Заявление по форме Банка (Приложение 6 к настоящим Правилам).

2.3.3. Использование сервиса по дополнительному уровню авторизации пользователей Системы ДБО через одноразовый пароль, направляемый Банком посредством SMS на сотовый телефон, носит рекомендательный, а не императивный, характер для всех Клиентов Банка.

2.3.4. Клиенты, впервые после «01» сентября 2011 года заключающие Договор ДБО, подключают сервис по информированию пользователей с помощью SMS на сотовый телефон об успешном подключении к Системе ДБО в обязательном порядке.

Для Клиентов, заключивших Договор ДБО до «01» сентября 2011 года, использование сервиса по информированию пользователей с помощью SMS на сотовый телефон об успешном подключении к Системе ДБО носит рекомендательный характер, за исключением Клиентов, имеющих по состоянию на «01» сентября 2011 года действующий Договор об оказании клиенту услуг по предоставлению информации о состоянии счета (счетов) посредством SMS-сообщений с использованием программно-аппаратного комплекса GSM SMS (услуга «GSM-Банк») (далее по тексту – «Договор GSM-Банк»). Такие Клиенты подключаются Банком к сервису по информированию пользователей с помощью SMS об успешном подключении к Системе ДБО автоматически после предварительного уведомления посредством Системы ДБО о внедрении данного сервиса. При этом Заявление о подключении сервисов безопасности Системы ДБО (Приложение 6 к настоящим Правилам) Клиентом в Банк не предоставляется, если SMS об успешном подключении к Системе ДБО Банку необходимо направлять только на сотовый телефон, указанный в Договоре GSM-Банк.

Если на момент внедрения сервиса по информированию пользователей с помощью SMS на сотовый телефон об успешном подключении к Системе ДБО у Клиента сменился номер сотового телефона, на который Банку необходимо направлять SMS в рамках Договора GSM-Банк, или Клиенту необходимо получать SMS на прочие номера сотовых телефонов, не указанные в Договоре GSM-Банк, Клиент оформляет соответствующее Заявление о подключении дополнительных сервисов безопасности Системы ДБО по форме Банка (Приложение 6 к настоящим Правилам).

В срок не позднее 5 (пяти) календарных дней с момента уведомления Банком Клиентов, заключивших Договор ДБО до «01» сентября 2011 года и имеющих по состоянию на «01» сентября 2011 года действующий Договор GSM-Банк, о внедрении сервиса по информированию пользователей с помощью SMS об успешном подключении к Системе ДБО Клиент в праве предоставить заявление об отказе в подключении к сервису по информированию пользователей с помощью SMS об успешном подключении к Системе ДБО в свободной форме, подписать ЭП и

направить данное заявление в Банка посредством Системы ДБО. В этом случае сервис по информированию пользователей с помощью SMS об успешном подключении к Системе ДБО Банком не предоставляется.
2.3.6. В случае отказа Клиентов от подключения сервисов безопасности систем ДБО в соответствии с п. 2.3.1. настоящих Правил, Клиенту необходимо оформить Заявление по форме Банка (Приложение 11 к настоящим Правилам – для Клиентов, заключивших Договор ДБО до «01» сентября 2011 года; Приложение 12 к настоящим Правилам – для Клиентов, заключивших Договор ДБО после «01» сентября 2011 года).

2.4. Порядок формирования ключа ЭП и получения сертификата ключа проверки ЭП, а также порядок смены ключей ЭП и их аннулирования (отзыва)

2.4.1. Изготовление уполномоченным лицом Клиента ключа ЭП и получение сертификата ключа проверки ЭП

2.4.1.1. После передачи Банком Клиенту:

- программного обеспечения для защиты передаваемой информации по каналам связи - InterPRO Client (в случае ввода Системы ДБО в эксплуатацию);
- необходимых паролей и идентификаторов для доступа к Системе ДБО - пароль для входа в Систему ДБО, код пользователя Системы ДБО (в случае ввода Системы ДБО в эксплуатацию);
- ключевого носителя Rutoken ЭЦП 64 Кб в необходимом количестве (в случае ввода Системы ДБО в эксплуатацию, а также при плановой и внеплановой смене ключа ЭП);
- драйвера Rutoken ЭЦП 64 Кб, а также программного обеспечения для генерации ключей ЭП на Rutoken ЭЦП 64 Кб – AdminPKI (в случае ввода Системы ДБО в эксплуатацию, а также при плановой и внеплановой смене ЭП)

уполномоченное лицо Клиента самостоятельно, либо с привлечением сотрудника Банка, генерирует ключи ЭП на Rutoken ЭЦП 64 Кб. В результате генерации ключей ЭП создается ключ ЭП и ключ проверки ЭП. Ключ проверки ЭП создается в форме запроса на изготовление сертификата ключа проверки ЭП.
2.4.1.2. Запрос на изготовление сертификата ключа проверки ЭП направляется уполномоченным лицом Клиента электронно в Банк.
2.4.1.3. Сертификационный Центр Банка имеет право отказать уполномоченному лицу Клиента в выпуске сертификата ключа проверки ЭП, если информация, указанная в запросе на выпуск сертификата ключа проверки ЭП, отличается от информации, указанной в Заявлении на регистрацию в Реестре пользователей Сертификационного Центра Банка (Приложение 1 к настоящим Правилам). В этом случае Сертификационный Центр Банка должен уведомить уполномоченное лицо Клиента об отказе в выпуске сертификата ключа проверки ЭП с указанием причин любым удобным способом не позднее рабочего дня поступления запроса на выпуск сертификата ключа проверки подписи.
2.4.1.4. Если причин для отказа в выпуске сертификата ключа проверки ЭП не выявлено, администратор Сертификационного Центра Банка подписывает запрос на изготовление сертификата ключа проверки ЭП своей ЭП и направляет электронно сертификат ключа проверки ЭП уполномоченному лицу Клиента не позднее дня получения вышеуказанного запроса.
2.4.1.5. Уполномоченное лицо Клиента, получив сертификат ключа проверки ЭП, на своих технических средствах с помощью программной среды, предоставляемой Системой ДБО, производит регистрацию сертификата ключа проверки ЭП согласно инструкции, предоставленной Банком.
2.4.1.6. После регистрации сертификата ключа проверки ЭП уполномоченное лицо Клиента обязано распечатать 3 (три) экземпляра Сертификата ключа проверки электронной подписи на бумажном носителе. Сертификат ключа проверки ЭП заверяется:

- собственноручной подписью уполномоченного лица Клиента, проходящего процедуру регистрации;
- собственноручной подписью руководителя и печатью Клиента-пользователя Системы ДБО;
- собственноручной подписью администратора Сертификационного Центра Банка и печатью Сертификационного Центра Банка, либо сотрудником филиала Банка, уполномоченным на

основании доверенности заверять собственноручной подписью и специально предусмотренной для этих целей печатью.

Два экземпляра Сертификата ключа проверки ЭП уполномоченного лица Клиента хранятся в Банке. Третий экземпляр находится у Клиента.

До момента предоставления двух экземпляров Сертификата ключа проверки ЭП уполномоченного лица Клиента в Банк Система ДБО для Клиента заблокирована.

2.4.2. Порядок смены ключей ЭП уполномоченным лицом Клиента

2.4.2.1. При плановой и внеплановой смене ключа ЭП осуществляется изготовление новых ключей и сертификата ключа проверки ЭП. Формирование ключей подписи и сертификата ключа проверки ЭП уполномоченного лица Клиента осуществляется аналогично процедуре, описанной в пп. 2.4.1. настоящих Правил.

2.4.3. Аннулирование (отзыв) сертификата ключа проверки ЭП Клиента

2.4.3.1. Уполномоченное лицо Клиента, указанное в сертификате ключа проверки электронной подписи, обязано обратиться в Банк с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи в случае компрометации ключа (Приложение 7 к настоящим Правилам) незамедлительно, но не позднее чем в течение одного рабочего дня со дня получения соответствующей информации о компрометации ключа. С момента подачи заявления на аннулирование (отзыв) сертификата ключа проверки ЭП ключ ЭП не используется.

2.4.3.2. После подачи заявления на аннулирование (отзыв) сертификата его рассмотрение и исполнение Сертификационным Центром Банка осуществляется в течение одного рабочего дня.

2.4.3.3. Временем аннулирования (отзыва) сертификата ключа проверки подписи признается время исключения Сертификационным Центром сертификата ключа проверки ЭП из списка зарегистрированных.

2.4.3.4. До внесения информации об аннулировании (отзыве) сертификатов ключа проверки электронной подписи администратор Сертификационного Центра Банка уведомляет владельца сертификата ключа проверки электронной подписи об аннулировании (отзыве) сертификатов ключа проверки электронной подписи путем направления электронного документа.

2.5. Сертификаты ключей электронной цифровой подписи, выданным Клиентам до 01.07.2012 г., приравниваются к Сертификатам ключей проверки электронной подписи.

Закрытые (секретные) ключи электронной цифровой подписи, сгенерированные Клиентами до 01.07.2012 г., приравниваются к ключам электронной подписи.

Открытые ключи электронной цифровой подписи, сгенерированные Клиентами до 01.07.2012 г., приравниваются к ключам проверки электронной подписи.

3. Требования, предъявляемые к ЭД Системы ДБО

3.1. ЭД, сформированный в Системе ДБО, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия.

3.2. ЭД, используемый в Системе ДБО, считается надлежащим образом оформленным при условии его соответствия законодательству Российской Федерации, соответствующим нормативным документам Банка, а также договорам, заключаемым между Клиентом и Банком.

3.3. Использование ЭП и шифрования в электронном документообороте.

3.3.1. ЭД считается подписанным уполномоченным лицом, если он подписан тем ключом ЭП, для которого Сертификационный Центр Банка изготовил сертификат ключа проверки ЭП для уполномоченного лица Клиента.

3.3.2. Замена ключей ЭП не влияет на юридическую силу ЭД, если он был подписан действующим на момент подписания ключом ЭП.

3.3.3. У каждого участника Системы ДБО имеются индивидуальные ключи ЭП, при помощи которых они подписывают ЭД своей ЭП.

3.3.4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью.

3.3.5. Все электронные документы подлежат шифрованию.

3.3.6. При получении зашифрованного ЭД, он расшифровывается в соответствии с применяемой технологией, затем проверяется ЭП ЭД.
3.3.7. Предусмотренные для данного документа правовые последствия могут наступить, только если получен положительный результат проверки ЭП и реквизитов ЭД.
3.3.8. Порядок проверки ЭП:

ЭД считается подписанным уполномоченным лицом, если он подписан тем ключом ЭП, для которого Сертификационный Центр Банка изготовил Сертификат ключа проверки электронной подписи для уполномоченного лица Клиента.

Электронный документ, подписанный неквалифицированной ЭП, признается равнозначным документом на бумажном носителе, в следующих случаях:

- Сертификат ключа проверки электронной подписи не утратил силу (действующий), информации о прекращении действия или аннулировании сертификата ключа проверки электронной подписи в момент подписания электронного документа и/или на момент проверки и принятия электронного документа не поступало в Сертификационный Центр Банка.
- Электронная подпись Клиента является корректной, подтверждена подлинность электронной подписи в электронном документе.
- Электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.
- Фактов внесения изменений в электронный документ после момента его подписания при осуществлении проверки в момент принятия электронного документа не обнаружено.

3.3.9. С целью уменьшения объемов передаваемой информации при транспортировке электронных документов могут использоваться специальные алгоритмы сжатия информации. В случае необходимости, может выполняться подпись и шифрование сжатого ЭД.
3.4. ЭД вступает в силу с момента его регистрации в Системе ДБО. Внесение каких-либо изменений в ЭД, зарегистрированный в Системе ДБО, не допускается.
3.5. Все экземпляры ЭД являются подлинниками данного ЭД. ЭД не может иметь копий в электронном виде.
3.6. Копии ЭД могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Банком или участником Системы ДБО, являющимся отправителем или получателем ЭД. ЭД и его копии на бумажном носителе должны быть идентичными.
3.7. Программные средства, осуществляющие преобразование ЭД для изготовления (распечатки) в виде бумажного документа, являются составной частью программного обеспечения, используемого в подсистемах Системы ДБО.

4. Порядок совершения операций по Системе ДБО

4.1. Моментом регистрации ЭД в Системе ДБО является момент полного помещения содержимого ЭД на жесткий магнитный диск компьютера принимающей стороны.
Формирование электронного документа осуществляется в следующем порядке:

- формирование электронного сообщения в формате, установленном для данного электронного документа;
- в процессе формирования электронного документа Система ДБО проверяет правильность заполнения отдельных реквизитов документа;
- подписание сформированного электронного сообщения электронной подписью.

Регистрация электронного документа в Системе ДБО происходит автоматически после завершения его формирования.

Проверка электронного документа включает:

- проверку электронного документа на соответствие установленному для него формату;
- проверку подлинности всех электронных подписей электронного документа;
- внесение каких-либо изменений в электронный документ, зарегистрированный в ДБО, не допускается.

При получении электронного документа, подписанного скомпрометированным ключом электронной подписи, данный ЭД отклоняется Системой ДБО.

Форматы электронных документов, принимаемых Банком от Клиента, представлены в Приложении 10 к Правилам.

4.2. Электронные документы, зарегистрированные в Системе ДБО в течение операционного времени Банка, принимаются к исполнению текущим днем. Электронные документы, зарегистрированные в послеоперационное время Банка, принимаются к исполнению следующим банковским днем.

Списание средств со счета Клиента на основании зарегистрированного ЭД осуществляется программным способом при достаточности средств на счете в соответствии со значениями цифровых реквизитов плательщика и получателя в ЭД. Указанные операции осуществляются независимо от значения текстовых реквизитов ЭД.

Операционное время Банка размещено на стендах в операционных залах Банка в местах, доступных для всеобщего обозрения и на официальном сайте Банка - www.zapsibkombank.ru. Контрольным временем - является время системных часов аппаратных средств Банка.

Прием электронного документа Клиента к исполнению подтверждается Банком присвоением статуса ЭД в Системе ДБО в Списке транзакций «Выполненные транзакции», в случае отказа от исполнения ЭД Банк уведомляет Клиента посредством присвоения статуса ЭД в Списке транзакций «Непринятые транзакции» с указанием причины отказа.

В случае помещения документа в Картотеку 2 документу Банк уведомляет Клиента посредством присвоения статуса ЭД в Списке транзакций «Непринятые транзакции» с указанием причины отказа «Документ помещен в картотеку». Исполнение документов, переведенных на «Картотеку 2», контролируется Клиентом по выписке.

4.3. Участник Системы ДБО может отозвать созданный ЭД путем удаления его из списка необработанных Банком транзакций. ЭД со статусом «Выполнен» не может быть отозван пользователем. Все электронные документы, зарегистрированные в Системе ДБО, хранятся в электронных архивах.

При хранении электронных документов должна быть обеспечена привязка (синхронизация) электронных документов и соответствующих сертификатов ключей проверки ЭП для проведения процедуры разрешения конфликтных ситуаций.

4.4. При невозможности передачи информации в Банк с использованием Системы ДБО документы могут поступить от Клиента в виде подлинника на бумажном носителе. При этом Банком взимается комиссия за обработку документов на бумажном носителе в соответствии с Тарифами.

4.5. Банк вправе отклонять поступившие от Клиента неправильно оформленные электронные документы.

4.6. Банк информирует Клиента о совершении каждой операции с использованием Системы ДБО путем направления клиенту соответствующего уведомления в порядке, установленном настоящими Правилами, содержащего все необходимые реквизиты, предусмотренные пунктом 4.9 Главы 4 «Положения о правилах осуществления перевода денежных средств» (утв. Банком России 19.06.2012 N 383-П).

4.7. В качестве надлежащего уведомления Клиента о совершении каждой операции с использованием Системы ДБО применяются следующие способы:

4.7.1. Предоставление информации в рамках оказания услуги «GSM-Банк» посредством направления Клиенту по каждой совершенной операции SMS-сообщения на указанный им номер мобильного телефона в порядке, установленном Договором «GSM-Банк» и Правилами обслуживания Клиентов с использованием программно-аппаратного комплекса «GSM SMS» (услуга «GSM-Банк») (далее – Правила «GSM-Банк»), являющихся неотъемлемой часть Договора «GSM-Банк» и размещенных на официальном сайте Банка.

4.7.2. Предоставление ежедневной выписки по счету в офисе Банка. Выписки предоставляются Клиентам уполномоченными сотрудниками Банка на бумажном носителе не позднее следующего рабочего дня после исполнения распоряжений о переводе денежных средств. Если Клиент своевременно не обратился в офис Банка за получением выписки на бумажном носителе, в этом случае Клиент принимает на себя все риски совершения операций, совершенных с использованием системы ДБО без его согласия и Банк не несет ответственности за последствия исполнения таких операций.

4.8. Дополнительными способами получения информации о совершении каждой операции с использованием Системы ДБО, либо неуспешности прохождения операции для Клиента является:

4.8.1. сервисные сообщения, отображаемые Клиенту в системе ДБО по факту совершения операции;
4.8.2. электронная выписка, содержащая информацию обо всех движениях по счету и сформированная Клиентом самостоятельно с использованием системы ДБО.
4.9. Моментом исполнения Банком обязанности уведомления Клиентов с использованием дополнительных способов уведомлений, указанных в п. 4.8. настоящих Правил, является момент непосредственного отображения информации Клиенту в системе ДБО.
4.10. Банк обязан предоставлять Клиенту документы и информацию, которые связаны с использованием Клиентом системы ДБО по письменному запросу Клиента, в срок не более 20 рабочих дней с момента получения запроса.

5. Оплата за услуги Банка по обслуживанию Клиентов с использованием Системы ДБО
5.1. Услуги Банка по обслуживанию Клиентов с использованием Системы ДБО оплачиваются согласно Тарифам, утвержденным Банком, если иной размер не установлен соглашением сторон. Клиент заранее дает Банку акцепт (согласие) на списание платы за услуги Банка по Договору ДБО со счета Клиента, указанного в разделе 4 Договора ДБО, либо с иного счета Клиента, открытого в Банке и указанного в письменном уведомлении Клиента, без дополнительных распоряжений для списания денежных средств на основании платежного требования либо иного документа, установленного законодательными актами и нормативными документами Банка России.
5.2. Банк в одностороннем порядке устанавливает (в том числе вводит новые), изменяет, дополняет Тарифы, порядок и условия оплаты за услуги по обслуживанию Клиентов с использованием Системы ДБО. Обо всех изменениях, дополнениях, нововведениях Тарифов, порядка и условий оплаты за услуги Банк не позднее, чем за 5 (пять) календарных дней до вступления в силу соответствующих изменений, дополнений, нововведений извещает Клиентов путем размещения соответствующей информации на официальном сайте Банка - www.zapsibkombank.ru, в операционных залах Банка в местах, доступных для всеобщего обозрения, а также путем направления информационного письма по Системе ДБО.

Если после установления, изменения, дополнения, нововведения Тарифов, а также порядка и условий оплаты за услуги Клиент продолжает пользоваться услугами, считается, что Клиент согласен с указанными изменениями. Оплата услуг Банка по обслуживанию Клиентов с использованием Системы ДБО осуществляется в соответствии с Тарифами, действующими на дату предоставления услуг.

6. Порядок эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части Системы ДБО

В целях обеспечения безопасности работы с Системой ДБО Клиенту необходимо строго и точно соблюдать нижеперечисленные требования.

6.1.Организационные меры информационной безопасности Системы ДБО
6.1.1. Клиенту необходимо ежедневно контролировать состояние счета любым из способов, перечисленных в пунктах 4.7. и 4.8. настоящих Правил. При обнаружении подозрительных операций, а также в случае утраты электронного средства платежа и (или) его использования без согласия клиента незамедлительно обратиться в Банк для информирования о несанкционированном доступе к Системе ДБО и объявления ключей ЭП скомпрометированными.
6.1.2. На рабочей станции, на которой установлена Система ДБО, не открывать и не исполнять файлы, полученные из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них вирусов и вредоносных программ.
6.1.3. Двери помещения во время осуществления действий доступа и других манипуляций в Системе ДБО должны быть закрыты, присутствие посторонних лиц, не имеющих доступа к ключевой информации, должно быть исключено.
6.1.4. Все оборудование, входящее в состав рабочего места, с которого осуществляется работа в Системе ДБО, должно быть технически исправным.
6.1.5. При эксплуатации Системы ДБО запрещается:

- вносить изменения в исполняемые и конфигурационные файлы программного и информационного обеспечения Системы ДБО;
- вносить изменения или удалять контрольные архивы, создаваемые Системой ДБО;

- вносить изменения или удалять программное обеспечение, используемое для работы с Rutoken ЭЦП 64 Кб в Системе ДБО.

6.1.6. В случае возникновения технических неисправностей Системы ДБО и ее элементов, а также в случае неисправности работы Rutoken ЭЦП 64 Кб, Банк должен быть незамедлительно проинформирован о невозможности использования Системы ДБО и/или Rutoken ЭЦП 64 Кб в Системе ДБО по телефону, указанному в Приложении 8 к настоящим Правилам.

6.1.7. В случае утраты электронного средства платежа и (или) его использования без согласия клиента, а также в случае возникновения подозрений в нарушении безопасности Системы ДБО, выявления признаков или фактов, возможности таких нарушений, а также в случаях компрометации ключа ЭП, передача платежных поручений должна быть приостановлена, а Банк незамедлительно уведомлен Клиентом об этом по телефону, указанному в Приложении 8 к настоящим Правилам (при этом Банк записывает и хранит сообщение в течение 5 лет). Уполномоченный сотрудник Банка перезванивает Клиенту для его идентификации (посредством запроса ФИО, паспортных данных сотрудника Клиента, обратившегося по вопросу приостановления работы Системы ДБО, проверки наличия права обратившегося сотрудника распоряжаться счетом организации) перед приостановлением работы Системы ДБО не позднее 30 минут с момента обращения Клиента. Удостоверившись в личности Клиента и получив подтверждение приостановления работы Системы ДБО Сотрудник Банка блокирует Систему ДБО.

После уведомления Банка о приостановлении использования Системы ДБО посредством телефонной связи, Клиент в течение пяти рабочих дней обязан направить в Банк письменное подтверждение с подробным описанием произошедшего случая. Система ДБО блокируется Банком с момента подтверждения Клиентом приостановления работы Системы ДБО при его идентификации посредством телефонной связи до устранения признаков небезопасной работы с Системой ДБО, при этом Клиент считается уведомленным о приостановлении работы системы ДБО с момента его идентификации.

6.2. Меры по обеспечению безопасности персонального компьютера, с которого осуществляется работа с Системой ДБО

6.2.1. Строго соблюдать регламент ограниченного доступа к Системе ДБО. К работе с Системой ДБО допускаются только уполномоченные сотрудники Клиента, имеющие ЭП для работы с Системой ДБО.

6.2.2. На компьютере должно быть установлено только лицензионное программное обеспечение (операционные системы, офисные пакеты, антивирусные программы и пр.) с учетом последних всевозможных обновлений.

6.2.3. На компьютере не должны быть установлены развлекательные и игровые программы.

6.2.4. Осуществлять проверку компьютера на наличие вирусов перед началом работы с Системой ДБО, а также в следующих случаях:

- при увольнении штатного системного администратора, осуществляющего обслуживание компьютера, с которого ведется работа с Системой ДБО;
- после доступа к компьютеру внештатных системных администраторов или любых других сотрудников, выполнивших работу по установке, обновлению и поддержке различных бухгалтерских, правовых, информационных и других программ.

Заражение компьютера троянскими вирусами представляет собой серьезный риск для безопасности, так как позволяет отслеживать нажатия клавиш и похищать конфиденциальную банковскую информацию (например, номера счетов, пароли).

6.2.5. Незамедлительно удалять обнаруженное вредоносное программное обеспечение (вирусы, шпионское программное обеспечение и т.п.). Клиент должен незамедлительно проинформировать Банк (по телефону, указанному в Приложении 8 к настоящим Правилам, либо путем направления по Системе ДБО письма в свободной форме) об обнаруженном и удаленном вредоносном программном обеспечении для дальнейшего осуществления действий по внеплановой смене ключа ЭП.

6.3. Меры по обеспечению информационной безопасности ключей ЭП

6.3.1. В качестве места хранения ключевой информации использовать только Rutoken ЭЦП 64 Кб. Допускается хранение ключей ЭП на прочих отчуждаемых носителях (дискетах, флэш-картах) для Клиентов Банка, заключивших Договор ДБО до «01» июля 2011 года, до момента плановой или

внеплановой смены ключа ЭП. Запрещается хранить ключи ЭП на жестких/сетевых дисках компьютера.
6.3.2. Использовать носители с ключами ЭП только для доступа к Системе ДБО. Запрещается использовать ключевой носитель для любой другой цели, например, для переноса документов или фотографий с одного компьютера на другой.
6.3.3. Ключевой носитель должен быть подключен к компьютеру только во время работы с Системой ДБО. В остальное время ключевой носитель информации должен храниться в месте, где доступ посторонних лиц к нему исключен (сейф, металлический шкаф и т.д.).
6.3.4. Не подвергать носители электронных ключей воздействию сильных магнитных полей и высокого напряжения.
6.3.5. Не копировать ЭП на другой носитель без разрешения руководителя Клиента.
6.3.6. Генерацию ЭП осуществлять только в присутствии уполномоченного лица Клиента, на имя которого изготавливается ЭП.
6.3.7. Не принимать от кого-либо, включая сотрудников Банка, ЭП, сгенерированную без присутствия уполномоченного лица Клиента, на имя которого изготавливается ЭП.
6.3.8. Ни под каким предлогом не передавать носитель ЭП другому лицу, включая системных администраторов или сотрудников Банка, даже для проверки работы Системы ДБО, настроек взаимодействия с Банком и т.п. При необходимости таких проверок, владелец ЭП обязан лично подключать носитель с ключами ЭП к компьютеру и производить необходимые настройки/проверки самостоятельно под наблюдением системных администраторов или сотрудников Банка.
6.3.9. Незамедлительно осуществлять перегенерацию ключей ЭП в следующих случаях:
- при возникновении любых подозрений на компрометацию (копирование) ключей ЭП;
- при проведении ремонтных работ, устранения технических сбоев и т.п. на компьютере, с которого осуществляется работа с Системой ДБО;
- в случае обнаружения каких-либо вредоносных программ на компьютере, используемом для работы в Системе ДБО.

6.4. Меры по обеспечению безопасности средств доступа, используемых в Системе ДБО
6.4.1. Не допускается использование простых паролей, например, 123456, qwerty. Необходимо использовать различные сложные комбинации из букв (желательно сочетание заглавных и строчных букв) и цифр, не расположенных подряд на клавиатуре, в количестве не менее 8 символов.
6.4.2. Осуществлять регулярно (минимум – 1 раз в месяц) смену паролей, используемых в Системе ДБО.
6.4.3. Пароли, используемые в Системе ДБО, желательно запоминать. Запрещается записывать и хранить пароли в местах, доступных посторонним лицам.
6.4.4. Не сообщать пароли, используемые в Системе ДБО, кому-либо, в том числе системным администраторам или сотрудникам Банка для проверки работы Системы ДБО, настроек взаимодействия с Банком и пр. При необходимости таких проверок владелец средств доступа обязан сам лично вводить свои пароли в Системе ДБО.
6.4.5. Не назначать пароль, используемый в Системе ДБО, в любых других системах и сервисах.
6.4.6. Ни при каких обстоятельствах не вводить пароль доступа в Систему ДБО на сайтах в сети Интернет.

6.5. Первоочередные меры информационной безопасности при работе с Системой ДБО изложены в Приложении 8 к настоящим Правилам в форме уведомления-памятки, которая выдается Клиенту в момент заключения Договора ДБО или смены ключей ЭП.

7. Ответственность сторон

7.1. Совместная ответственность Банка и Клиента
7.1.1. За невыполнение или ненадлежащее исполнение обязательств по Договору ДБО стороны несут ответственность в соответствии с законодательством Российской Федерации.
7.1.2. Банк и Клиент несут ответственность за сохранность, обеспечивают конфиденциальность своих ключей ЭП и отвечают за действия своего персонала.

7.1.3. Банк и Клиент несут ответственность за несвоевременное информирование друг друга обо всех случаях компрометации ключей ЭП, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств подсистем обработки, хранения, защиты и передачи информации.
7.1.4. Банк и Клиент не несут ответственность за сбои в обмене информацией, возникшие в результате неисправности линий связи, отключения или перебоев в линиях электропитания, неисправности аппаратных средств.

7.2.Ответственность Клиента:
7.2.1. Клиенты в полном объеме несут ответственность за последствия, вызванные нарушением ими порядка эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части Системы, описанном в п. 6. настоящих Правил.
7.2.2. Клиент в полном объеме несет ответственность за последствия несанкционированного доступа к ключам ЭП.
7.2.3. Клиент в полном объеме несет ответственность за последствия, вызванные отправкой Банком сообщений на неактуальный (-ые) номер (-а) сотового (-ых) телефона (-ов) в рамках сервисов безопасности Системы ДБО, указанных в п. 2.3.1. настоящих Правил, в следующих случаях:
а) если Клиент сообщил ошибочный номер телефона (номер, не принадлежащий Клиенту);
б) своевременно не оформил Заявление о смене номеров телефонов в рамках сервисов безопасности Системы ДБО (Приложение 9 к настоящим Правилам). Заявление о смене номеров телефонов в рамках дополнительных сервисов безопасности Системы ДБО оформляется Клиентом не позднее дня смены номера (-ов) телефона (-ов), подписывается ЭП и предоставляется в Банк посредством Системы ДБО.
7.2.4. Клиент несет ответственность за содержание реквизитов ЭД.
7.2.5. Клиент в полном объеме несет ответственность за последствия совершения операций, о которых Банк не проинформировал Клиента способами, указанными в п. 4.7. настоящих Правил, в следующих случаях:
а) Клиент отказался от первичного подключения услуги «GSM-Банк» или от использования подключенной услуги «GSM-Банк», предоставив соответствующее заявление по форме и в порядке, установленное Правилами «GSM-Банк», размещенными на официальном сайте Банка;
б) Клиент не предоставил, несвоевременно предоставил или предоставил неактуальную информацию для подключения и эксплуатации услуги «GSM-Банк», предусмотренную Правилами «GSM-Банк», размещенными на официальном сайте Банка;
в) Клиент не обратился в офис Банка за получением выписки на бумажном носителе.

Клиент принимает на себя все риски совершения операций, совершенных с использованием системы ДБО без его согласия и Банк не несет ответственности за последствия исполнения таких операций.

7.3. Ответственность Банка
7.3.1. Банк после принятия ЭД от Клиента несет ответственность за его неизменность в процессе исполнения.
7.3.2. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по счету Клиента на основании надлежащим образом оформленных и своевременно доставленных электронных документов Клиента в соответствии с действующим законодательством Российской Федерации.
7.3.3. Банк несет ответственность за убытки Клиента:

- при использовании ключа ЭП и сертификата ключа проверки ЭП уполномоченного лица Клиента только в случае, если данные убытки возникли при компрометации ключа подписи администратора Сертификационного Центра Банка;
- при проведении операций, совершенных без согласия Клиента после получения уведомления Клиента в соответствии с п. 6.1.7. настоящих Правил;
- при проведении операции, о которой Клиент не был проинформирован способами, указанными в п. 4.7. настоящих Правил (за исключением случаев, описанных в п. 7.2.5. настоящих Правил), и которая была совершена без согласия Клиента;

7.3.4. Банк не несет ответственности за:

- последствия исполнения поручений, выданных неуполномоченными лицами, в тех случаях, когда с использованием процедур, предусмотренных настоящими Правилами и Договором ДБО, Банк не мог установить факта выдачи распоряжения неуполномоченными лицами или Клиент своими действиями или бездействием способствовал поступлению в Банк указанных распоряжений;
- за работоспособность Системы ДБО, если работа с Системой ДБО осуществлялась на компьютере, не соответствующем требованиям, указанным в Приложении 2 к настоящим Правилам;
- ущерб Клиента, возникший вследствие принятия к исполнению электронных документов с недействительной или скомпрометированной ЭП Клиента, поступившей до получения от Клиента информации о признании ее недействительной или о ее компрометации;
- ущерб Клиента, возникший вследствие:
  a) неправильного заполнения Клиентом реквизитов ЭД в Системе ДБО;
  b) нарушение Клиентом порядка эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части Системы, указанного в п. 6. настоящих Правил;
  c) несанкционированного доступа к Системе ДБО по причинам, указанным в пп. 7.2.2., 7.2.3. настоящих Правил;
  d) совершения операций без согласия Клиента - в случае, если Банк исполняет обязанность по информированию Клиента о совершенной операции в соответствии с п. 4.7. настоящих Правил и Клиент не направил Банку уведомление в соответствии с п. 6.1.7. настоящих Правил, Банк не обязан возмещать Клиенту сумму операции, совершенной без согласия Клиента;
  e) совершения операций без согласия Клиента, если Банк не информировал Клиента о совершенной операции в связи со случаями, указанными в п. 7.2.5. настоящих Правил, и Клиент не направил Банку уведомление в соответствии с п. 6.1.7. настоящих Правил. Банк не обязан возмещать Клиенту сумму операции, совершенной без согласия Клиента.

8. Порядок разрешения конфликтов между участниками Системы ДБО

8.1. Возникновение конфликтных ситуаций в Системе ДБО возможно в следующих случаях:

8.1.1. При осуществлении электронного документооборота, связанного с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах ЭП.

Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- неподтверждение подлинности электронных документов средствами ЭП принимающей стороны;
- оспаривание факта формирования ЭД;
- оспаривание факта идентификации владельца сертификата ключа проверки ЭП, подписавшего документ;
- заявление участника Системы ДБО об искажении ЭД;
- оспаривание факта отправления и/или доставки ЭД;
- оспаривание времени отправления и/или доставки ЭД;
- оспаривание аутентичности экземпляров ЭД и/или подлинника и копии ЭД на бумажном носителе;
- оспаривание факта отправки Банком уведомления о совершенной операции в соответствии с п. 4.7. настоящих Правил;

иные случаи возникновения конфликтных ситуаций, связанных с функционированием Системы ДБО.

8.1.2. При высказывании Банком недоверия к программному обеспечению, функционирующему на рабочем месте Клиента, с которого ведется работа с Системой ДБО.

8.2. Уведомление о конфликтной ситуации

8.2.1. В случае возникновения конфликтной ситуации участник Системы ДБО должен незамедлительно, в течение не более чем одного рабочего дня со дня получения информации о таком нарушении, направить заявление о конфликтной ситуации противоположной стороне.

8.2.2. Заявление о предполагаемом наличии конфликтной ситуации оформляется в произвольной письменной форме, отправляется электронно, по почте или нарочно. Заявление должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. В заявлении должны быть перечислены основные реквизиты оспариваемого ЭД, фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.
8.2.3. Сторона, которой направлено заявление, обязана незамедлительно, но не позднее чем в течение следующего рабочего дня, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить заявителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.
8.2.4. Банк обязан рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы ДБО, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования Системы ДБО для осуществления трансграничного перевода денежных средств.

8.3. Разрешение конфликтной ситуации в рабочем порядке

8.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от противоположной стороны.
8.3.2. В случае если уведомитель не удовлетворен информацией, полученной от противоположной стороны, для рассмотрения конфликтной ситуации формируется техническая комиссия.

8.4. Формирование технической комиссии (далее по тексту – Комиссия), ее состав

8.4.1. Не позднее чем на следующий рабочий день после того, как принято решение о необходимости сформировать Комиссию, или не позднее, чем на 6 (шестой) рабочий день после получения уведомления о конфликтной ситуации, в случае, если конфликтная ситуация не была урегулирована в рабочем порядке, Комиссия должна быть сформирована.
8.4.2. Если участники Системы ДБО, являющиеся сторонами в конфликтной ситуации не договорятся об ином, в состав Комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон.
8.4.3. В состав Комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Лица, входящие в состав Комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.
8.4.4. Право представлять в Комиссии соответствующую сторону должно подтверждаться доверенностью, выданной каждому представителю на срок работы Комиссии.
8.4.5. По инициативе любой из сторон к работе Комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, соответствующие требованиям, указанным в пп.8.4.3. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

8.5. Компетенция и полномочия Комиссии

8.5.1. Сформированная Комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки ЭД, его подлинности, а также о подписании ЭД конкретной ЭП, аутентичности отправленного документа полученному.
8.5.2. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению Комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.
8.5.3. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.
8.5.4. Для проведения необходимых проверок и документирования данных, используемых при указанных проверках, может применяться специальное программное обеспечение.

8.6. Протокол работы Комиссии

8.6.1. Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Комиссией, заносятся в Протокол работы Комиссии. Протокол работы Комиссии должен содержать следующие данные:
– состав Комиссии с указанием сведений о квалификации каждого из членов Комиссии;
– краткое изложение обстоятельств возникшей конфликтной ситуации;
– мероприятия, проводимые Комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;
– выводы, к которым пришла Комиссия в результате проведенных мероприятий;
– подписи всех членов Комиссии.
8.6.2. В случае если мнение члена (или членов) Комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов Комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами Комиссии), чье особое мнение отражает соответствующая запись.
8.6.3. Протокол составляется в одном подлинном экземпляре на бумажном носителе, который находится в Банке. По требованию любой из сторон в конфликтной ситуации, или любого из членов Комиссии, им может быть выдана заверенная Банком копия Протокола.

8.7. Акт по итогам работы Комиссии
8.7.1. По итогам работы Комиссии составляется Акт, в котором содержится краткое изложение выводов Комиссии. Помимо изложения выводов о работе Комиссии Акт должен также содержать следующие данные:
– состав Комиссии;
– дату и место составления Акта;
– даты и время начала и окончания работы Комиссии;
– краткий перечень мероприятий, проведенных Комиссией;
– подписи членов Комиссии;
– указание на особое мнение члена (или членов Комиссии), в случае наличия такового.
8.7.2. Акт составляется в таком количестве экземпляров, чтобы каждая из сторон в конфликтной ситуации имели по одному подлинному экземпляру составленного Акта. По требованию члена Комиссии ему может быть выдана заверенная Банком копия Акта.
8.7.3. К Акту может прилагаться особое мнение члена (или членов Комиссии), не согласных с выводами Комиссии, указанными в Акте. Особое мнение составляется в произвольной форме в таком же количестве подлинных экземпляров, что и Акт, и составляет приложение к Акту.
8.7.4. Акт по итогам работы Комиссии направляется Банком сторонам, участвовавшим в разборе конфликтной ситуации, с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

8.8. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, стороны будут стремиться разрешить, используя механизмы согласительного урегулирования споров и разногласий.
8.9. Если по итогам проведения согласительной процедуры конфликтная ситуация остается полностью или частично неурегулированной, стороны вправе передать неурегулированный спор и разногласия в Арбитражный суд Тюменской области.

9. Порядок прекращения (приостановления) использования Системы ДБО
9.1. Любая из сторон вправе в одностороннем порядке расторгнуть Договор ДБО письменно предупредив об этом другую сторону за 10 (десять) календарных дней до предполагаемой даты расторжения Договора ДБО.
9.2. В случае расторжения Договора ДБО или прекращения его действия Банк закрывает доступ Клиенту в Системе ДБО, Клиент обязан удалить программный модуль с ключевого носителя.
9.3. Клиент вправе временно приостановить и возобновить действие Договора ДБО, письменно уведомив об этом Банк.
9.4. Банк имеет право в одностороннем порядке приостановить использование Системы ДБО в случае получения от Клиента сведений о нарушении безопасности Системы ДБО, выявления признаков, фактов или возможности таких нарушений, возникновения технических

неисправностей элементов Системы ДБО, до устранения обстоятельств, препятствующих использованию Системы ДБО, при нарушении Клиентом порядка использования системы ДБО.
9.5. Банк вправе отказать Клиенту в дистанционном доступе к счету, распоряжение по которому производится с использованием аналога собственноручной подписи в следующих случаях:

- совершения сомнительных операций, то есть операций, в отношении которых есть основания полагать, что они не имеют экономического смысла или очевидной законной цели;
- появления в Банке информации, выявленной при обновлении сведений в анкете клиента, в том числе при проверке сведений, поступивших из контролирующих органов, о том, что Клиент, его постоянно действующий орган управления, иной орган или лицо, которое имеют право действовать от имени юридического лица без доверенности, отсутствует по адресу регистрации и/или в Банке отсутствуют актуальные документы, устанавливающие изменения в адресе регистрации и/или наличие по фактическому местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности.

В этом случае Банк направляет Клиенту Уведомление о том, что дистанционный доступ к счету прекращен полностью до предоставления им в Банк запрашиваемой информации:

- документов, поясняющих экономический смысл или очевидную законную цель проводимых операций;
- документов, подтверждающих изменения адреса регистрации и/или наличие по фактическому местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности.

К документам, поясняющим экономический смысл или очевидную законную цель проводимых операций, включая, но не ограничиваясь, относятся: документы, касающиеся целей, характера сделки, документы, относящиеся к исполнению и/или подтверждающие факт исполнения сделки, а также документы о стороне по сделке. К документам, подтверждающим изменения адреса регистрации относятся: изменения в учредительные документы, документ о государственной регистрации (свидетельство) изменений, вносимых в учредительные документы, выписка из Единого государственного реестра юридических лиц, новый опросный лист Клиента, и прочие документы, установленные Правилами расчетно-кассового обслуживания Банка. К документам, подтверждающим наличие по фактическому местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности, относятся: копии договоров аренды, субаренды, свидетельства о праве собственности и др.

В условиях прекращения дистанционного доступа к счету и невозможности совершения Клиентом операций по счету с использованием Системы ДБО Клиент вправе в дальнейшем совершать операции при предоставлении в Банк надлежащим образом оформленных распоряжений о переводе денежных средств на бумажном носителе в соответствии с порядком, установленным законодательством и Правилами расчетно-кассового обслуживания Банка, оплачивая услуги Банка в соответствии с Тарифами, утвержденными уполномоченными лицами Банка, если иные Тарифы не предусмотрены соглашением сторон.

Распоряжения Клиента на выполнение операций, кроме перечисления переводов денежных средств в бюджетную систему РФ, на бумажном носителе не выполняются Банком в случае, если Клиентом не представлены в Банк документы, подтверждающие изменения адреса регистрации и/или наличие по фактическому местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности.

При передаче Клиентом Банку распоряжений на выполнение операций, не имеющих экономического смысла и очевидной законной цели, на бумажном носителе, Банк будет выполнять такие распоряжения только при условии одновременного предоставления Клиентом необходимых документов, касающихся целей, характера, относящихся к исполнению/подтверждающие факт исполнения сделки, а также документов о стороне по сделке, и подтверждающих экономический смысл и очевидную законную цель проводимой операции.

В случае, если запрашиваемые документы Клиентом не представлены в течение 30 (тридцати) дней со дня направления Банком указанного Уведомления Клиенту, Банк в одностороннем

порядке отказывается от исполнения полностью Договора ДБО, вышеуказанный Договор ДБО считается расторгнутым с даты направления Клиенту соответствующего сообщения.

Срок предоставления Клиентом документов, подтверждающих изменения адреса регистрации и/или наличие фактического местонахождения юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности, устанавливается в соответствии с п. 2.9. действующей редакции Правил расчетно-кассового обслуживания.

Банк в одностороннем порядке отказывается от исполнения полностью Договора ДБО, Договор ДБО считается расторгнутым с Клиентом с даты направления Клиенту соответствующего сообщения в случае, если запрашиваемые документы, представлены Клиентом в срок, но из них не следует, что:

- проводимая операция имеет экономический смысл или очевидную законную цель;
- изменения адреса регистрации и/или наличие фактического местонахождения юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности, подтверждаются.

Клиенту, предоставившему в установленный настоящим пунктом Правил срок все запрашиваемые Банком документы, восстанавливается дистанционный доступ к счету при условии, что из представленных документов следует, что совершенная операция имеет экономический смысл и очевидную законную цель, и изменения адреса регистрации и/или наличие фактического местонахождения юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности, подтверждаются.

Клиент обязуется предоставлять Банку по первому требованию документы, подтверждающие экономический смысл или очевидную законную цель проводимых операций по счету, и документы, подтверждающие изменения адреса регистрации и/или документы, устанавливающие наличие по фактическому местонахождению юридического лица, его постоянно действующего органа управления, иного органа или лица, которое имеет право действовать от имени юридического лица без доверенности.

Указанные в настоящем пункте уведомления и сообщения направляются Клиенту по Системе ДБО.

9.6. Прекращение (приостановление) использования Системы ДБО не прекращает обязательств Клиента и Банка, возникших до момента прекращения (приостановления) использования Системы ДБО.

10. Внесение изменений в Правила

10.1. Настоящие Правила могут быть изменены (дополнены) Банком в одностороннем порядке. Любые изменения настоящих Правил размещаются Банком на официальном сайте Банка - www.zapsibkombank.ru, в операционных залах Банка в местах, доступных для всеобщего обозрения, а также рассылаются Клиентам по Системе ДБО. Если после изменений (дополнений) настоящих Правил Клиент продолжает пользоваться услугами, то считается, что Клиент уведомлен надлежащим образом об указанных изменениях (дополнениях) в Правила, согласен с ними, и считает их для себя обязательными.

Приложение 1
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

☐ Без права подписи

В «Запсибкомбанк» ОАО
(_____ филиал/ДО/ОО «Запсибкомбанк» ОАО)

ЗАЯВЛЕНИЕ О РЕГИСТРАЦИИ

Настоящим _____
(наименование организации)
расч. сч._____
юридический адрес: _____,
в лице _____
(должность, Ф.И.О. руководителя или доверенного лица)
действующего на основании _____ ,
просит зарегистрировать в Реестре пользователей Сертификационного Центра
информационной сети «Запсибкомбанк» ОАО _____
_____
(*наименование и местонахождение организации)*
в лице_____,
(*должность, Ф.И.О. уполномоченного лица)*
действующего на основании _____
и изготовить на это наименование сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными

O = Организация = _____ (наименование организации)
T = Должность = _____(должность)
OU = Подразделение = _____ (наименование подразделения)
L = Город = _____(наименование населен. пункта)
C = Страна/Регион = RU
E = Электронная почта = _____

Срок действия сертификата ключа проверки электронной подписи Клиента:

☐ Постоянно *(в рамках планового периода действия – 1 год 3 месяца)*

☐ Временно на срок _____ месяцев *(указывается срок, на который необходимо изготовить сертификат ключа проверки электронной подписи)*

Области использования сертификата, при которых электронный документ с электронной подписью уполномоченного лица будет иметь юридическое значение, ограничиваются рамками договоров на дистанционное банковское обслуживание между «Запсибкомбанк» ОАО и _____ с использованием системы «Банк-Клиент»/«Интернет-Банк» *(нужное подчеркнуть).*

Уполномоченное лицо _____ /_____ заверяю
(подпись) (*Ф.И.О.*)
Руководитель _____ /_____/_____
(подпись) (*Ф.И.О.*) МП

Контактный телефон:_____
«____» _____ _____г.

Заявление о регистрации принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*
«____» _____ _____г.

Приложение 2
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Требования к программно-техническим средствам для проведения расчетных операций в электронной форме

1. Компьютер с установленной лицензионной операционной системой MS Windows XP/2003/Vista/Win7;
2. Антивирусное программное обеспечение с актуальными базами;
3. Монитор поддерживающий разрешение экрана не менее 800x600 точек, параметры цветности не менее 16 бит;
4. Канал доступа в сеть Интернет со скоростью приема/передачи данных не ниже 128 кБит/с;
5. Открытый доступ к USB-порту;
6. Работоспособный принтер, подключенный к компьютеру автоматизированного рабочего места.

Приложение 3
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

В «Запсибкомбанк» ОАО
(_____филиал/ДО/ОО «Запсибкомбанк» ОАО)
от _____
_____
_____
(наименование организации)

ЗАЯВЛЕНИЕ

от «___» _____ _____ года

Прошу обслуживать счет № | | | | | | | | | | | | | | | | | | | | |

с использованием Интернет-технологий (система ДБО «**Интернет-Банк»**).
Уполномоченным лицом, указанным (или которое будет указано) в сертификате ключа проверки электронной подписи, является:

Ф.И.О._____
Должность_____
Паспортные данные: Серия_____№_____Дата выдачи_____
Место выдачи_____

Руководитель:_____ / _____ /_____
(должность) (подпись) (Ф.И.О.)

М.П.

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«____» _____ _____г.

Приложение 4

к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Акт приема-передачи
Rutoken ЭЦП 64 Кб

«____»_____ _____ год

Акционерный Западно-Сибирский коммерческий банк открытое акционерное общество («Запсибкомбанк» ОАО), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, при совместном упоминании именуемые «Стороны», заключили настоящий Акт о нижеследующем:

1. По настоящему Акту Банк передал, а Клиент принял для использования в Системе ДБО Rutoken ЭЦП 64Кб в следующем количестве:

№ п/п	Серийный номер Rutoken ЭЦП 64Кб	Данные об уполномоченном лице Клиента, которое будет хранить ключ ЭП на Rutoken ЭЦП 64 Кб
1	…	Фамилия, имя, отчество, должность
2	…	Фамилия, имя, отчество, должность

2. Клиент подтверждает, что корпус (-а) преданного (-ых) Rutoken ЭЦП 64 Кб не имеет (-ют) видимых признаков повреждения или взлома.
3. Клиент подтверждает, что проинформирован о размещении на сайте Банка:
   - Драйвера для Rutoken ЭЦП 64 Кб;
   - Программного обеспечение для генерации ключей ЭП на Rutoken ЭЦП 64 Кб (AdminPKI).
4. Клиентом подтверждается обязанность:

4.1. организовать инсталляцию необходимого драйвера для Rutoken ЭЦП 64 Кб, а также программного обеспечения для генерации ключей ЭП, на компьютере, на котором будет эксплуатироваться вышеуказанное устройство и Система ДБО «Интернет-Банк»;

4.2. обеспечить генерацию с помощью Rutoken ЭЦП 64 Кб ключей ЭП уполномоченным лицом Клиента – ключ ЭП и ключ проверки ЭП – и предоставление в Банк сертификата ключа проверки ЭП Клиента/уполномоченного лица Клиента.

5. Клиент гарантирует использование Rutoken ЭЦП 64 Кб только для работы в Системе ДБО, а также обязуется не передавать их (его) третьим лицам.

К настоящему Акту прилагается Приложение 1 «Правила и требования по работе с Rutoken ЭЦП 64 Кб».

Настоящий Акт и Приложение 1 к настоящему Акту составлены в 2 (Двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

Дата, время передачи Rutoken ЭЦП 64 Кб Клиенту: «____»_____ _____ год _____:_____
(час. : мин.)

От БАНКА передал	**От КЛИЕНТА получил**
_____ (должность)	_____ (должность)
_____ (подпись)	_____ (подпись)
_____ (Ф.И.О.) М.П.	_____ (Ф.И.О.) М.П.

Приложение 1
к Акту приема-передачи Rutoken ЭЦП 64 Кб
от «___»_____ _____ года

Правила и требования по работе с Rutoken ЭЦП 64 Кб

Общие сведения о Rutoken ЭЦП 64 Кб

Электронный идентификатор Rutoken ЭЦП 64 Кб - физический носитель, предназначенный для хранения ключа ЭП и ключа проверки ЭП, являющийся персональным средством аутентификации уполномоченного лица Клиента и обеспечивающий доступ к распоряжению счетом и обмену электронными документами по Системе ДБО.

Основные преимущества использования Rutoken ЭЦП 64 Кб для Клиентов Банка:

1. *Безопасность применения* – воспользоваться Rutoken ЭЦП 64 Кб может только его владелец, знающий PIN-код устройства.

Rutoken ЭЦП 64 Кб гарантирует Клиентам Банка сохранность ключей ЭП от копирования как наиболее распространенного способа хищения ключевой информации, так как при подписании электронного документа ключом ЭП, находящимся на Rutoken ЭЦП 64 Кб, такой ключ не извлекается из памяти устройства, и весь процесс визирования электронного документа происходит внутри Rutoken ЭЦП 64 Кб.

Таким образом, ключ ЭП генерируется внутри Rutoken ЭЦП 64 Кб, хранится в защищенной памяти Rutoken ЭЦП 64 Кб и не может быть из Rutoken ЭЦП 64 Кб считан. А неизвлекаемость ключа ЭП из памяти ключевого носителя – залог надежного обеспечения секретности ключа ЭП.

2. *Надежность хранения информации* – качественная микросхема и прочный герметичный корпус существенно уменьшают риск выхода устройства из строя.

3. *Мобильность* – минимальные требования к рабочему месту для обеспечения использования Rutoken ЭЦП 64 Кб в Системе ДБО.

Rutoken ЭЦП 64 Кб работает под управлением операционных систем MS Windows начиная с Windows XP.

Для того, чтобы Клиент мог воспользоваться USB-ключом в Системе ДБО, необходимо на рабочую станцию установить драйвер Rutoken ЭЦП 64 Кб, а также программное обеспечение для генерации ключей ЭП (AdminPKI). Драйвер и программное обеспечение для генерации ключей ЭП предоставляется Банком.

4. *Удобство работы* – Rutoken ЭЦП 64 Кб выполнен в виде брелка со световой индикацией, напрямую подключается к компьютеру через USB-порт.

Функциональные возможности Rutoken ЭЦП 64 Кб

Rutoken ЭЦП 64 Кб обеспечивает:

- генерацию ключевых пар ЭП;
- формирование и проверку ЭП по ГОСТ Р34.10-2001;
- генерацию ключей шифрования;
- шифрование информации по ГОСТ 28147-89;
- формирование и проверку имитовставки по ГОСТ 28147-89;
- вычисление хэш-функции по ГОСТ 34.11-97.

В Rutoken ЭЦП 64 Кб может храниться до 45 ключей ЭП.

В одном Rutoken ЭЦП 64 Кб допускается одновременно хранить ключи нескольких уполномоченных лиц Клиента.

Правила использования Rutoken ЭЦП 64 Кб

Rutoken ЭЦП 64 Кб необходимо оберегать от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.), воздействия высоких и низких температур. При резкой смене температуры (перемещение охлажденного ключевого носителя с мороза в теплое помещение) не рекомендуется использовать Rutoken ЭЦП 64 Кб в течение 3 часов во избежание повреждения ключевого носителя из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать Rutoken ЭЦП 64 Кб от попадания на него прямых солнечных лучей.

Недопустимо воздействие на Rutoken ЭЦП 64 Кб сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.

При засорении разъема Rutoken ЭЦП 64 Кб нужно применять меры для его очистки. Для очистки корпуса и разъема необходимо использовать сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.

В случае неисправности или неправильного функционирования Rutoken ЭЦП 64 Кб необходимо обращаться в Банк по следующим телефонам:

- 8 (3452) 798-990;
- 8 (3452) 522-000;
- 8-800-100-5005 (звонок бесплатный как с городского, так и с мобильного телефона).

Подготовка Rutoken ЭЦП 64 Кб к работе

Перед началом роботы с Rutoken ЭЦП 64 Кб на рабочее место пользователя Системы ДБО необходимо предварительно установить:

1. *Драйвер Rutoken ЭЦП 64 Кб*. Драйвер Rutoken ЭЦП 64 Кб необходимо установить до подключения устройства.
2. *Программное обеспечение для генерации ключей ЭП* - AdminPKI.

Во время установки драйвера и программного обеспечения для генерации ключей ЭП все приложения должны быть закрыты.

Важно!

Не передавайте Rutoken ЭЦП 64 Кб третьим лицам! Не сообщайте третьим лицам PIN-код доступа к ключу ЭП. В случае утери (хищения) Rutoken ЭЦП 64 Кб немедленно свяжитесь с Банком по следующим телефонам:

- 8 (3452) 798-990;
- 8 (3452) 522-000;
- 8-800-100-5005 (звонок бесплатный как с городского, так и с мобильного телефона).

Обращаем особое внимание!

Rutoken ЭЦП 64 Кб должен быть подключен к компьютеру только на время работы в системе ДБО. **Недопустимо** постоянное подключение Rutoken ЭЦП 64 Кб к компьютеру.

Приложение 5
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Доверенность оформляется на фирменном бланке организации и подписывается руководителем Клиента.

ДОВЕРЕННОСТЬ

Город _____ Дата выдачи: «____» _____ год

Настоящим _____, в лице_____
(наименование Клиента) (должность, фамилия, имя, отчество)
_____(далее по тексту – «Доверитель»),
действующего на основании_____
(название документа, на основании которого действует указанное лицо)

предоставляет право _____
(фамилия, имя, отчество)
паспорт серии_____ № _____ выдан_____
(серия паспорта) (номер паспорта) (кем выдан)
_____
совершать от имени Доверителя следующие действия:

1. Получать Rutoken ЭЦП 64 Кб в количестве _____ штук.
2. Подписывать Акт приема-передачи Rutoken ЭЦП 64 Кб.
3. Прочие действия, связанные с получением Rutoken ЭЦП 64 Кб.

Подпись _____ _____ удостоверяю
(фамилия, имя, отчество)

Доверенность выдана сроком на _____
(не более 3-х лет)

_____ _____ _____
(должность руководителя Клиента) (подпись) М.П. (фамилия, имя, отчество)

Приложение 6
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Заявление о подключении сервисов безопасности Системы ДБО

от «___»_____ _____ года

Прошу подключить следующие дополнительные сервисы безопасности Системы ДБО:

☐ ***дополнительный уровень авторизации пользователей через одноразовый пароль, направляемый Банком посредством SMS на следующий номер телефона:***

☐-☐☐☐-☐☐☐-☐☐-☐☐

☐ ***сервис по информированию пользователей с помощью SMS об успешном подключении к системе «Интернет-Банк, направляемые на следующие номера телефонов:***

основной номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона:……

С правилами пользования вышеуказанными дополнительными сервисами безопасности Системы ДБО ознакомлен и согласен.

Руководитель _____ / _____ / _____
(подпись) *(Ф.И.О.)* *М.П.*

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«___» _____ _____ г.

Приложение 7
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Вице-Президенту
«Запсибкомбанк» ОАО
Чеснову В.А.

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ

_____
(наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____
в связи с _____
(причина аннулирования (отзыва) сертификата: компрометация ключа, прекращение работы и т.д.)
просит аннулировать (отозвать) сертификат ключа проверки электронной подписи серийный номер _____, выданного на имя/клиенту_____
(фамилия, имя, отчество/наименование)
_____
(серия и номер паспорта, кем и когда выдан/местонахождение)

Владелец сертификата _____ /Фамилия И.О./Наименование организации

«____» _____ _____ г.

Должность и Фамилия И.О. уполномоченного лица организации
Подпись уполномоченного лица организации, дата подписания заявления
Печать организации

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа проверки _____ (Ф.И.О./наименование) получено, личность _____ (Ф.И.О.) идентифицирована, сведения, указанные в Заявлении проверены.

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«__» _____ _____ г.

Приложение 8
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Уведомление-памятка Клиентам «Запсибкомбанк» ОАО о мерах информационной безопасности при работе с системами дистанционного банковского обслуживания - «Банк-Клиент», «Интернет-Банк» (далее по тексту - ДБО)

1. В качестве места хранения ключевой информации использовать только **Rutoken ЭЦП 64 Кб**.
2. Rutoken ЭЦП 64 Кб должен быть подключен к компьютеру только **во время работы с системой ДБО**. В остальное время Rutoken ЭЦП 64 Кб **должен храниться в месте, где доступ посторонних лиц к нему исключен (сейф, металлический шкаф и т.д.)**.
3. **Исключить использование сети Internet в служебных или личных целях** на компьютере с установленной программой Банк-Клиент или Internet Banking, **кроме сайта http://10.1.5.150**, используемого для входа в систему «Интернет-Банк», и **ни при каких обстоятельствах не вводить логин и пароль доступа системы на других сайтах**, а также не устанавливать развлекательные и игровые программы.
4. Генерацию ЭП осуществлять только **в присутствии ответственного за эту ЭП**.
5. **Не принимать** от кого либо, включая сотрудников «Запсибкомбанк» ОАО, **ЭП, сгенерированные без присутствия ответственного за эту ЭП.**
6. **Ни под каким предлогом не передавать носитель с ЭП другому лицу**, включая системных администраторов или сотрудников «Запсибкомбанк» ОАО.
7. **Обеспечить соблюдение мер по защите компьютера**, с которого осуществляется работа в системе ДБО:
   - **не передавать в какой-либо ремонт или на обслуживание** за пределы организации рабочие станции с установленным программным обеспечением «Банк-Клиент» **без уведомления «Запсибкомбанк» ОАО**;
   - строго **соблюдать регламент ограниченного доступа к компьютеру, на котором ведется работа с системой**;
   - обязательно использовать **лицензионное** программное обеспечение для защиты информации – антивирусные программы (**рекомендуемая антивирусная программа компании «Лаборатория Касперского» - Kaspersky Internet Security 2011**);
   - постоянно обновлять, **не реже 1 раза в неделю, а лучше ежедневно**, установленные антивирусные программы.

При возникновении следующих ситуаций:

1. утерян или похищен Rutoken ЭЦП 64 Кб или компьютер, на котором была установлена система ДБО,
2. не работает система ДБО по неизвестным причинам,

незамедлительно обращаться в Банк.

Телефоны для контактов с «Запсибкомбанк» ОАО:
телефон для технической поддержки Клиентов ДБО: **8 (3452) 798-990;**
телефон для справок: **8 (3452) 522-000;**
8-800-100-5005 (звонок бесплатный как с городского, так и с мобильного телефона)

Соблюдение указанных мер и своевременное сообщение в Банк об угрозе потери конфиденциальности ключей ЭП, помогут существенно снизить угрозу мошенничества с денежными средствами с использованием систем ДБО.

---

1. Уведомление – памятку получил _____ / _____ /
   (подпись) (ФИО, должность, организация)
2. Инструктаж провел _____ / _____ /
   (подпись) (ФИО, должность сотрудника Банка)

Приложение 9
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

Заявление о дополнении\изменении номеров телефонов в рамках сервисов безопасности Системы ДБО

Прошу исключить из списка следующий (-ие) номер (-а) сотового (-ых) телефона (-ов):

☐***дополнительный уровень авторизации пользователей через одноразовый пароль, направляемый Банком посредством SMS на следующий номер телефона:***

☐-☐☐☐-☐☐☐-☐☐-☐☐

☐ ***сервис по информированию пользователей с помощью SMS об успешном подключении к системе «Интернет-Банк, направляемые на следующие номера телефонов:***

основной номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона:……

Прошу включить в список следующий (-ие) номер (-а) сотового (-ых) телефона (-ов):

☐***дополнительный уровень авторизации пользователей через одноразовый пароль, направляемый Банком посредством SMS на следующий номер телефона:***

☐-☐☐☐-☐☐☐-☐☐-☐☐

☐ ***сервис по информированию пользователей с помощью SMS об успешном подключении к системе «Интернет-Банк, направляемые на следующие номера телефонов:***

основной номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона: ☐-☐☐☐-☐☐☐-☐☐-☐☐

дополнительный номер телефона:……

Руководитель _____ / _____ / _____
(подпись) *(Ф.И.О.)* *М.П.*

«___» _____ _____ г.

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«__» _____ _____ г.

Приложение 10
к Правилам обслуживания Клиентов с использованием Интернет-технологий
(система ДБО «Интернет-Банк») от 09.12.2009 г. № 21/1045

Форматы электронных документов, используемых при обслуживании Клиентов с использованием Интернет-технологий (система ДБО «Интернет-Банк»)

Платежное поручение (Перевод по России)

№ п.п.	Поле	Требования к содержанию реквизитов электронного документа
1.	Платежное поручение	В состав символов, недопустимых в текстовых реквизитах электронных распоряжений о переводе денежных средств, включены символы, имеющие следующие ASCII-коды: 0-31, 127, 176-223, 240-255.
2.	Номер документа	не может оканчиваться на «000», должен быть отличен от нуля
3.	Дата документа	не ранее 10 календарных дней
4.	Тип платежа	по справочнику
	Плательщик	
5.	ИНН	проверка ключевания
6.	КПП	проверка заполнения, если платеж налоговый
7.	Расчетный счет	проверка ключевания с БИК
8.	Корсчет	проверка ключевания с БИК
9.	БИК	проверка по справочнику БИК
10.	Наименование	
	Получатель	
11.	ИНН	проверка ключевания
12.	КПП	проверка заполнения, если платеж налоговый
13.	Расчетный счет	проверка ключевания с БИК
14.	Корсчет	проверка ключевания с БИК
15.	БИК	проверка по справочнику БИК
16.	Наименование	проверка наименования для внутрибанковских платежей
17.	Вид оплаты	01
18.	Наз.пл.	Резерв
19.	Код	Резерв
20.	Срок плат.	Резерв
21.	Очер. Плат.	выбор 1 – 6
22.	Рез. Поле	Резерв
23.	Код составителя платежа	выбор по справочнику
24.	Код бюджетной классификации	по справочнику на сервере
25.	ОКАТО	длина поля не менее 11 символов
26.	Основание налогового платежа	выбор по справочнику
27.	Налоговый период	«0» или в формате “DD.MM.YYYY”, где DD – 01…31, Д1, Д2, Д3, МС, КВ, ПЛ, ГД
28.	Номер документа	
29.	Дата документа	«0» или формат «DD.MM.YYYY»
30.	Вид платежа для налога	выбор по справочника
31.	Назначение платежа	- не может быть пустым; - если получатель/плательщик нерезидент, то поле должно начинаться с кода 000KNF при печати фраза с НДС должна печататься с новой строки
32.	Налоговый платеж	Поля «КПП» (6, 12) и 23 – 30 должны быть заполнены

Официальное письмо

№ п.п.	Поле	Требования к содержанию реквизитов электронного документа
1.	Номер документа	Присваивается автоматически
2.	Дата документа	
3.	Кому	Указывается подразделение банка в которое адресовано письмо
4.	Текст письма	Не может содержать более 1000 символов
5.	Подпись	Указывается уполномоченное лицо Клиента

Приложение 11

к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

В «Запсибкомбанк» ОАО
(_____ филиал «Запсибкомбанк» ОАО)
от _____
_____
_____
(наименование организации)

Заявление об отказе от подключения сервисов безопасности Системы ДБО «Интернет-Банк»

от «___»_____ _____ года

Прошу не оказывать дополнительные сервисы безопасности Системы ДБО «Интернет-Банк»:
□ ***дополнительный уровень авторизации пользователей через одноразовый пароль, направляемый Банком посредством SMS***

□ ***сервис по информированию пользователей с помощью SMS об успешном подключении к системе «Интернет-Банк»***

С мерами информационной безопасности Системы ДБО ознакомлен и согласен.

Руководитель _____ / _____ / _____
(подпись) *(Ф.И.О.)* *М.П.*

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«___» _____ _____ г.

Приложение 12
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система ДБО «Интернет-Банк»)

В «Запсибкомбанк» ОАО
(_____ филиал «Запсибкомбанк» ОАО)
от _____
_____
_____
(наименование организации)

Заявление об отказе от подключения сервисов безопасности Системы ДБО «Интернет-Банк»

от «___»_____ _____ года

Прошу не оказывать дополнительные сервисы безопасности Системы ДБО «Интернет-Банк»:
дополнительный уровень авторизации пользователей через одноразовый пароль, направляемый Банком посредством SMS

С мерами информационной безопасности Системы ДБО ознакомлен и согласен.

Руководитель _____ / _____ / _____
(подпись) *(Ф.И.О.)* *М.П.*

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. сотрудника Банка)*

«___» _____ _____ г.