УТВЕРЖДЕНЫ

Протоколом Исполнительного комитета «Коммерческого Индо Банка» ООО

(Протокол № 90/2022 от 05.12.2022 г.)

УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ «КОММЕРЧЕСКИМ ИНДО БАНКОМ» ООО УСЛУГИ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»

г. Москва

2022 г.

ОГЛАВЛЕНИЕ

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ
2. ОБЩИЕ ПОЛОЖЕНИЯ
3. ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»
4. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»
5. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ СМЕНЫ КЛЮЧА ЭП ВЛАДЕЛЬЦА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
6. ПОРЯДОК ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ КЛЮЧЕЙ ЭЛЕКТРОННЫХ ПОДПИСЕЙ ЗАЯВИТЕЛЕЙ
7. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ
8. СОПРОВОЖДЕНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛИЕНТА
9. ПРОЦЕДУРЫ, ОСУЩЕСТВЛЯЕМЫЕ ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ И АННУЛИРОВАНИИ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
10. РАСТОРЖЕНИЕ ДОГОВОРА СИСТЕМЫ ДБО ПО ИНИЦИАТИВЕ КЛИЕНТА
11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
12. ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПОДЛИННОСТЬЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ
Приложение 1 Перечень программно-технических средств автоматизированного рабочего места клиента для обеспечения функционирования системы ДБО
Приложение 2 Перечень электронных документов, используемых в системе ДБО
Приложение 3 Требования и рекомендации по обеспечению информационной безопасности АРМ клиента
Приложение 4 Заявление на подключение к услуге ДБО
Приложение 5 Уведомление об изменении параметров подключения к услуге ДБО
Приложение 6 Акт приема-передачи носителей ключевой информации, программного обеспечения и средств криптографической защиты информации
Приложение 7 Акт о вводе в действие услуги БДО
Приложение 8 Заявление на выполнение работ по сопровождению системы ДБО
Приложение 9 Акт приема-сдачи работ
Приложение 10 Доверенность на получение документов и программного обеспечения для работы с сертификатами ключей электронной подписи
Приложение 11 Доверенность на подписание сертификата ключа электронной подписи
Приложение 12 Уведомление о компрометации ключа электронной подписи
Приложение 13 Карточка абонента/оператора системы ДБО
Приложение 14 Заявление на изготовление сертификата ключа проверки электронной подписи для ИП
Приложение 15 Заявление на изготовление сертификата ключа проверки электронной подписи для руководителя
Приложение 16 Заявление на изготовление сертификата ключа проверки электронной подписи для сотрудника
Приложение 17 Заявление на аннулирование сертификата ключа проверки электронной подписи (для юридических лиц и индивидуальных предпринимателей)
Приложение 18 Заявление на установление ограничений по параметрам операций с использованием системы ДБО
Приложение №19 Заявление на создание простой электронной подписи

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящих Правил используются следующие термины и определения:

Абонент системы ДБО (абонент Клиента/Банка) – зарегистрированное в системе ДБО ответственное лицо Банка/Клиента, владеющее ключами ЭП и уполномоченное осуществлять некоторые или все перечисленные действия: подписание ЭД, прием и передача ЭД, шифрование и расшифровывание ЭД.

При этом абонентами Клиента могут быть исключительно лица, указанные в карточке с образцами подписей и оттиска печати Клиента, имеющейся в распоряжении Банка, срок полномочий которых, согласно такой карточке, не истек. Срок полномочий должностного лица Клиента в качестве абонента системы ДБО должен соответствовать сроку полномочий, указанному в карточке с образцами подписей и оттиска печати Клиента.

Абонентами Банка являются его должностные лица, назначенные в качестве таковых решением руководства Банка.

Автоматизированное рабочее место (АРМ) Клиента/Банка – аппаратно-программный комплекс, в состав которого входит:

1. программное обеспечение, предназначенное для:
   - создания ЭД, его подписания ЭП, шифрования и передачи с АРМ Клиента на АРМ Банка и с АРМ Банка на АРМ Клиента;
   - приёма и расшифровывания ЭД, проверки корректности ЭП, обработки информации из принятых ЭД;
   - создания ключей ЭП и запросов на Сертификаты ключей ЭП;
   - обработки и хранения Сертификатов ключей ЭП.

2. аппаратный комплекс, необходимый и достаточный для реализации функционала соответствующего программного обеспечения и соответствующий требованиям, изложенным в Приложении 1 к Условиям.

Администратор АРМ Банка/АРМ Клиента – уполномоченный сотрудник Банка/Клиента, отвечающий за функционирование и работоспособность системы ДБО.

Банк – «Коммерческий Индо Банк» ООО.

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата) - лицо, которому в установленном Законом № 63-ФЗ и настоящими Условиями порядке выдан сертификат ключа проверки электронной подписи, участник электронного взаимодействия в Системе Банка (клиент Банка - юридическое лицо, индивидуальный предприниматель или уполномоченное лицо клиента Банка), получивший в установленном Законом и настоящими Условиями порядке Сертификат ключа.

Закон № 149-ФЗ – Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Закон № 63 - Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи".

Заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, нотариусы и уполномоченные на совершение нотариальных действий лица, обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

Квитанция – ЭСИД, подтверждающий получение ЭД, правильность его расшифровки, корректность ЭП и заверенный ЭП абонента системы ДБО отправляющей Стороны.

Клиент – юридическое лицо (либо индивидуальный предприниматель), заключившее с Банком договор о предоставлении услуги «Дистанционное банковское обслуживание».

Ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи.

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

Компрометация ключа - констатация Владельцем ключей электронной подписи обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами. Следствием компрометации ключа является утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, Договором и настоящими Условиями.

Корректная ЭП – ЭП на ЭД, подлинность которой подтверждена СКЗИ и программным обеспечением АРМ Банка, АРМ Клиента или автоматизированного рабочего места, предназначенного для разбора конфликтных ситуаций, с использованием Сертификата ключа ЭП, принадлежащего Абоненту.

Личный кабинет пользователя удостоверяющего центра - система, позволяющая производить загрузку документов для регистрации пользователей удостоверяющего центра, осуществлять выпуск и управление сертификатами ключа проверки электронной подписи.

Носитель ключевой информации – информационный носитель USB-ключ eToken PRO (Java), на который записаны: ключ ЭП, справочник Сертификатов ключей ЭП абонентов/операторов Клиента с электронными Сертификатами ключей ЭП каждого из абонентов/операторов Банка.

Оператор Удостоверяющего центра – уполномоченный сотрудник Банка.

Оператор системы ДБО (Оператор Клиента) – зарегистрированное в системе ДБО ответственное лицо Клиента, владеющее Технологическим ключом ЭП и уполномоченное осуществлять в системе ДБО перечисленные ниже действия:

- создание шаблона ЭД;
- загрузка из информационных систем Клиента в Систему ДБО шаблона ЭД;
- выгрузка из Системы ДБО в информационные системы Клиента ЭД, полученного от Банка;
- редактирование шаблона ЭД;
- удаление шаблона ЭД;
- просмотр ЭД и шаблонов ЭД;
- прием от Банка и передача в Банк ЭД;
- просмотр и редактирование Справочника системы ДБО.

При этом оператором Клиента может быть любое должностное лицо Клиента, уполномоченное последним в качестве такового. Срок полномочий должностного лица Клиента в качестве оператора системы ДБО должен соответствовать сроку окончания действия полномочий соответствующего должностного лица Клиента.

Содержащиеся в тексте настоящих Условий и Договора положения, действующие в отношении Абонента системы ДБО, имеют силу и в отношении Оператора системы ДБО, кроме случаев, где обратное указано прямо либо действие подобных положений будет противоречить определению «Оператор системы ДБО».

Пакет электронных документов – совокупность ЭПД и/или ЭСИД, являющаяся единицей информационного обмена между Банком и Клиентом.

Платежное поручение – платежное поручение, сформированное в Системе ДБО ф.0401060 (утверждено Положением Банка России от 29.06.2021 N 762-П "О правилах осуществления перевода денежных средств").

Подтверждение подлинности ЭП в ЭД – положительный результат проверки (с использованием СКЗИ, а также Сертификата ключа ЭП) принадлежности ЭП в ЭД абоненту системы ДБО и отсутствия искажений в подписанном данной ЭП ЭД.

Пользовательская документация – документ и/или совокупность документов, определяющий(их) порядок работы с использованием системы ДБО, размещенный(ых) на WEB-сайте Системы ДБО. Пользовательская документация может быть изменена Банком в одностороннем порядке.

Пользователь удостоверяющего центра - юридическое лицо независимо от организационно-правовой формы, физическое лицо или иной хозяйствующий субъект, использующее полученный в Удостоверяющем центре сертификат ключа проверки ЭП, услуги Удостоверяющего центра на основании соответствующего договора об оказании услуг, в том числе на условиях публичной оферты и присоединившийся к Порядку реализации функций аккредитованного удостоверяющего центра ООО «АйтиКом».

Простая электронная подписью - ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

Система дистанционного банковского обслуживания (Система ДБО) - совокупность программно-аппаратных средств, устанавливаемых в помещениях Банка и Клиента и согласованно эксплуатируемых ими с целью предоставления Клиенту услуги «Дистанционное банковское обслуживание» посредством Системы ДБО «BS-Клиент».

Список аннулированных сертификатов - электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия.

Список отозванных Сертификатов – Электронный документ с ЭП Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров аннулированных Сертификатов и Сертификатов, действие которых прекращено.

Справочник системы ДБО – справочник, содержащий информацию, общую для всех пользователей системы ДБО и обновляемую Банком централизованно.

Средства криптографической защиты информации (СКЗИ) – аппаратные и/или программные средства криптографической защиты информации, обеспечивающие реализацию следующих функций:

- создание ЭП в ЭД с использованием закрытого ключа ЭП;
- шифрование и дешифрование ЭД;
- подтверждение подлинности ЭП в ЭД;
- создание ключей ЭП и запросов на Сертификаты ключей ЭП;
- обработка и хранение Сертификатов ключей ЭП.

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

Счет(а) – счет(а) Клиента, открытый(ые) на основании соответствующего договора расчетно-кассового обслуживания.

Тариф – Тариф за оказание банковских услуг Клиентам Банка, утвержденный заседанием Финансового Комитета «Коммерческого Индо Банка» ООО.

Технологический ключ ЭП –ключ ЭП, предназначенный для обеспечения идентификации Оператора системы ДБО и реализации предоставленных Оператору системы ДБО прав.

Содержащиеся в тексте настоящих Условий и Договора положения, касающиеся Ключа ЭП, имеют силу и в отношении Технологического ключа ЭП, кроме случаев, где обратное указано прямо либо действие подобных положений будет противоречить определению «Технологический ключ ЭП».

Удостоверяющий центр – ООО «АйтиКом» - юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом № 63-ФЗ. ООО «АйтиКом» зарегистрировано на территории Российской Федерации в городе Москве (свидетельство о государственной регистрации юридического лица № 017897164, выдано 8 сентября 2016 г. Межрайонной инспекцией Федеральной налоговой службы № 46 по г.

Москве), внесено в Единый государственный реестр юридических лиц за основным государственным регистрационным номером 1167746840843.

Уполномоченное лицо - физическое лицо, действующее от имени Клиента, наделенное правом подписи.

Услуга «Дистанционное банковское обслуживание» – предоставление Клиенту возможности проведения операций, предусмотренных Договором и настоящими Условиями с использованием Системы ДБО.

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.

Электронный документ - документ, информация в котором представлена в электронной форме, способной быть обработанной средствами вычислительной техники.

Электронный платежный документ (ЭПД) – ЭД, подписанный необходимым количеством ЭП уполномоченных абонентов Клиента и являющийся основанием для совершения операций по счетам Клиента.

Электронный служебно-информационный документ (ЭСИД) – ЭД, подписываемый ЭП уполномоченных абонентов передающей стороны и применяемый в системе ДБО для контроля процесса обработки ЭД или ЭПД на АРМ Банка/Клиента, контроля проведения операций по счетам Клиента, а также для передачи информации в произвольном формате.

Эталонная ПЭВМ – персональный компьютер, соответствующий всем требованиям Приложения 1 к настоящим Условиям, свободный от постороннего программного обеспечения или каких-либо вредоносных программ.

WEB-сайт Системы ДБО – расположенная в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbil-moscow.ru страница Банка, посредством доступа Клиента к которой Банк оказывает услуги «Дистанционного банковского обслуживания».

Иные термины и сокращения, используемые в настоящих Условиях, имеют значения, приданные им законодательством Российской Федерации, нормативными актами Банка России, а также заключенным между Банком и Клиентом договором расчетно-кассового обслуживания, если иное не указано прямо или не следует из контекста.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Условия предоставления «Коммерческим Индо Банком» ООО (далее – Банк) услуги «Дистанционное банковское обслуживание» (далее – Условия) являются неотъемлемой частью Договора о предоставлении услуги «Дистанционное банковское обслуживание» (далее – Договор) и регламентируют порядок и условия:

- подключения и предоставления юридическим лицам услуги «Дистанционное банковское обслуживание»;
- электронного документооборота в системе дистанционного банковского обслуживания;
- рассмотрения конфликтных ситуаций, связанных с подлинностью электронных документов.

2.2. Банк осуществляет предоставление услуги «Дистанционное банковское обслуживание» в соответствии с Договором и Условиями, действующими на момент оказания услуги.

2.3. Информационный обмен в рамках системы дистанционного банковского обслуживания осуществляется с использованием информационно-телекоммуникационной сети «Интернет».

2.4. В рамках услуги «Дистанционное банковское обслуживание» Клиент использует Систему ДБО, в котором справочники Клиента находятся на автоматизированном рабочем месте Банка. Электронные документы Клиента формируются на автоматизированном рабочем месте Банка удаленно через информационно-телекоммуникационную сеть «Интернет».

Специализированное программное обеспечение, устанавливаемое на автоматизированном рабочем месте Клиента в соответствии с настоящими Условиями, служит целям криптографической защиты информации.

2.5. Для подключения к услуге «Дистанционное банковское обслуживание» Клиент должен организовать рабочее место в соответствии с Перечнем технических средств автоматизированного

рабочего места Клиента для установки системы дистанционного банковского обслуживания (Приложение 1 к настоящим Условиям).

Для оказания в соответствии с Договором услуги «Дистанционное банковское обслуживание» Банк предоставляет Клиенту Носитель ключевой информации и специализированное программное обеспечение (далее – ПО):

- клиентскую часть Системы ДБО «BS-Client v.3» (разработчик ООО «БСС»);
- программное средство криптографической защиты информации «Message-PRO v.3.x».

2.6. Работа автоматизированного рабочего места Клиента в системе дистанционного банковского обслуживания должна быть организована локально, т.е. все компоненты ПО устанавливаются на одном компьютере.

2.7. В процессе эксплуатации системы дистанционного банковского обслуживания каждая из Сторон на своей территории самостоятельно выполняет необходимые мероприятия, обеспечивающие работоспособность своего автоматизированного рабочего места, каналов связи и защиту закрытых ключей электронной подписи, паролей и ресурсов автоматизированного рабочего места от несанкционированного доступа.

2.8. Обмен информацией между Сторонами производится путем передачи Клиентом в Банк и приема Клиентом из Банка пакета электронных документов.

Каждый пакет электронных документов, передаваемый в Банк или принимаемый из Банка, состоит из произвольного количества электронных документов, подписанных необходимым количеством электронных подписей.

Контроль прав абонентов Клиента, подписавших своей электронной подписью электронный документ, производится в процессе обработки этого электронного документа в Банке.

Перечень электронных документов, используемых в системе дистанционного банковского обслуживания, указан в Приложении 2 к настоящим Условиям.

2.9. За изъятиями, установленными подпунктом «8» пункта 11.5 настоящих Условий, электронный документ (в том числе вложение в электронный документ произвольного формата) порождает права и обязанности Сторон по Договору, договорам расчетно-кассового обслуживания, другим соглашениям, в рамках которых происходит взаимодействие с использованием системы дистанционного банковского обслуживания, если передающей Стороной электронный документ оформлен надлежащим образом, заверен корректными электронными подписями в необходимом количестве (в соответствии с пунктом 2.10 настоящих Условий) и передан по системе дистанционного банковского обслуживания, а принимающей Стороной – получен, проверен и принят.

2.10. Порядок использования электронной подписи при подписании электронного документа:

- электронные документы, необходимые для проведения операций по счету Клиента, подписываются абонентами Клиента;
- электронная подпись каждого из абонентов Клиента в электронном документе по конкретному счету юридически тождественна подписи (подписям) соответствующего (соответствующих) лица (лиц) в карточке с образцами подписей и оттиска печати Клиента, имеющейся в распоряжении Банка.

2.11. Срок действия Ключа ЭП Владельца Сертификата составляет 1 (один) год либо менее 1 (одного) года в случае, если полномочия Владельца сертификата заканчиваются до истечения 1 (одного) года с момента начала срока действия Ключа ЭП. Начало периода действия Ключа ЭП Владельца Сертификата исчисляется с момента начала течения срока действия соответствующего ему Сертификата.

Срок действия Сертификата Владельца Сертификата равен сроку действия Ключа ЭП Владельца Сертификата.

Сроки действия Сертификата Владельца Сертификата - юридического лица и Ключа ЭП, соответствующего такому Сертификату, должны находиться в пределах срока действия полномочий Владельца Сертификата, как он следует из представленных Удостоверяющему центру и Банку документов.

Сроки действия Сертификата Владельца Сертификата - уполномоченного лица индивидуального предпринимателя и Ключа ЭП, соответствующего такому Сертификату, должны находится в пределах срока

действия полномочий указанного Владельца Сертификата, как он следует из представленных Удостоверяющему центру и Банку документов.

Сертификат Владельца является действительным на определенный момент времени, если на такой момент одновременно соблюдаются следующие условия: (1) срок действия Сертификата уже начался, но еще не истек; (2) в Системе Банка отсутствуют сведения о прекращении действия Сертификата или его аннулировании.

Сертификат считается недействительным на определенный момент времени, если на такой момент (1) срок действия, указанный в Сертификате, еще не начался или уже истек; либо (2) в Системе Банка содержатся сведения о прекращении действия Сертификата или его аннулировании.

Ключ ЭП является действительным на определенный момент времени если на такой момент одновременно соблюдаются следующие условия: (1) срок действия Ключа ЭП начался, но еще не истек; (2) Сертификат, соответствующий данному Ключу ЭП, является действительным на указанный момент времени.

2.12. В целях минимизации риска несанкционированного списания денежных средств Клиента, Банк обращает внимание Клиента на необходимость соблюдения соответствующих требований, установленных Приложением 3 к настоящим Условиям. В упомянутых целях Банк рекомендует Клиенту также следовать рекомендациям, изложенным в Приложении 3 к настоящим Условиям.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»

3.1. Одновременно с подписанием Договора, но не позднее 10 (Десяти) рабочих дней со дня его подписания Клиент подает в Банк заявление на подключение к услуге «Дистанционное банковское обслуживание» по форме Приложения 4 к настоящим Условиям (далее – Заявление на подключение).

Заявление на подключение оформляется на бумажном носителе, на нем проставляется собственноручная подпись Владельца Сертификата и / или его уполномоченного лица, а также (если применимо) оттиск печати Владельца Сертификата.

Банк вправе не принимать к исполнению Заявление на подключение, заполненное неразборчиво, содержащее ошибки или не полностью заполненное.

3.2. Для работы в системе ДБО Уполномоченное лицо вправе использовать:

1) сертификат электронной подписи, выданный удостоверяющим центром ФНС (УЦ ФНС),
2) квалифицированный сертификат ключа проверки электронной подписи, оформленный Удостоверяющим центром (далее – квалифицированный сертификат),
3) простую электронную подпись в случаях, предусмотренных п. 3.4. настоящих Условий, по форме Приложения 19 к настоящим Условиям.

3.3. Создание заявки на выпуск ключа проверки электронной подписи осуществляется Оператором Удостоверяющего центра в присутствии заявителя на основании документов и сведений, представленных заявителем Оператору Удостоверяющего центра, при условии установления личности заявителя и получения подтверждения правомочий лица действовать от имени юридического лица без доверенности.

Оператор Удостоверяющего центра заполняет анкету на Уполномоченное лицо с указанием следующих данных:

- ИНН клиента Банка,
- руководитель / уполномоченный представитель клиента Банка,
  - ФИО,
  - Пол,
  - Паспортные данные (серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения),
  - Регион и город адреса регистрации,
  - СНИЛС,
  - ИНН,

- адрес электронной почты и телефон;
- должность и наименование подразделения,

В случае если владельцем сертификата является индивидуальный предприниматель, форма заявления включает следующие сведения:

— наименование;

— ИНН, ОГРНИП;

— область, город/населенный пункт (согласно сведениям, об адресе места нахождения индивидуального предпринимателя);

— сведения об уполномоченном представителе - владельце сертификата:

- ФИО;
- Пол;
- паспортные данные (серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения);
- СНИЛС;
- адрес электронной почты;

В случае, если заявителем не представлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или их достоверность и актуальность не подтверждается, Оператор Удостоверяющего центра имеет право запросить, а заявитель обязан предоставить документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата.

Оператор Удостоверяющего центра имеет право отказать заявителю в регистрации Пользователя Удостоверяющего центра и создании квалифицированного сертификата, в случае, если заявитель не предоставил документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или они не надлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается.

В случае положительного результата проверки заполненных данных, в личный кабинет Оператора Удостоверяющего центра направляется ссылка на генерацию ключа, на основании которой необходимо сформировать ключ проверки электронной подписи согласно инструкциям.

После успешного формирования ключа проверки электронной подписи Владелец ключа проверки электронной подписи подписывает собственноручной подписью Заявление на выпуск ключа проверки электронной подписи (по форме Приложений 14, 15 или 16 соответственно к настоящим Условиям) и согласие на обработку персональных данных (включено в заявление).

После подписания пакета документов Владельцем ключа проверки электронной подписи, Оператор Удостоверяющего центра загружает отсканированные документы, а также паспорт физического лица для отправки в Удостоверяющий центр.

При условии подтверждения достоверности документов и сведений, предоставленных заявителем, Удостоверяющим центром создается ключ электронной подписи и ключ проверки электронной подписи одновременно с созданием квалифицированного сертификата.

Созданный ключ электронной подписи, ключ проверки электронной подписи и квалифицированный сертификат записываются Оператором Удостоверяющего центра на носитель ключевой информации (далее также - ключевой носитель).

При создании ключа электронной подписи и ключа проверки электронной подписи Удостоверяющим центром формируется пароль доступа к ключевой информации. После получения ключа электронной подписи и ключа проверки электронной подписи Заявитель должен произвести смену пароля доступа к ключевой информации.

3.3.1. Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного действующей усиленной квалифицированной ЭП.

В случае, если заявление подается в бумажном виде, подписанное собственноручно, подпись пользователя Удостоверяющего центра на заявлении должна быть идентична подписи, которая зафиксирована в основном документе, удостоверяющем личность. Использование факсимиле (клише подписи) на заявлении не допускается.

3.3.2. При выдаче квалифицированного сертификата Оператор Удостоверяющего центра обязан:

1) идентифицировать заявителя - физическое лицо, обратившееся за получением квалифицированного сертификата. Идентификация заявителя проводится одним из следующих сопособов:

   — при личном присутствии заявителя,

   — посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата,

   — посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Законом N 149-ФЗ. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Закона N 149-ФЗ, удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации;

2) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;

3.3.3. При идентификации Заявителя при его личном присутствии Оператор Удостоверяющего центра руководствуется следующими положениями:

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность.

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства (при наличии официального перевода на русский язык, заверенного нотариусом или дипломатическими (консульскими) органами) или по иному документу, удостоверяющему личность гражданина иностранного государства, признаваемому таковым действующим законодательством.

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

3.3.4. В процессе идентификации устанавливаются:

— в отношении физического лица - фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

— в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, - наименование, организационноправовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица;

— для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, - наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано;

— идентификация заявителя может быть проведена посредством идентификации заявителя без его личного присутствия в порядке, установленном Федеральным законом «Об электронной подписи».

3.3.5. При обращении к Оператору Удостоверяющего центра заявитель представляет следующие документы либо их надлежащим образом заверенные копии и сведения:

1) основной документ, удостоверяющий личность;

2) номер страхового свидетельства государственного пенсионного страхования заявителя страховой номер индивидуального лицевого счета заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица;

4) основной государственный регистрационный номер заявителя - юридического лица;

5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя -индивидуального предпринимателя;

6) номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

7) документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени государственного органа или органа местного самоуправления.

Требования к документу, удостоверяющему личность:

— документ не должен быть просрочен;

— документ не должен быть поврежден или испорчен;

— документ не может содержать неточности и орфографические ошибки.

В случае, если документы и сведения, предоставляемые заявителем, оформлены не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

3.3.6. Порядок создания и выдачи квалифицированного сертификата.

3.3.6.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13 - 15, 17 и 18 Закона № 63 и Порядком реализации функций аккредитованного удостоверяющего центра ООО «АйтиКом» и исполнения его обязанностей.

Квалифицированный сертификат ключа проверки ЭП в электронной форме создается в формате X.509 версии 3, структура квалифицированного сертификата ключа проверки ЭП удовлетворяет требованиям Закона № 63-ФЗ и Приказа ФСБ России от 27.12.2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

После изготовления сертификата ключа проверки ЭП его владельцу направляется официальное уведомление о факте изготовления сертификата в виде сообщения по электронной почте, указанной в заявлении на изготовление сертификата.

Изготовленный сертификат ключа проверки ЭП в электронной форме, подписанный ЭП Уполномоченного лица Удостоверяющего центра, предоставляется его владельцу лично и/или путем отправки по электронной почте с официальным уведомлением в виде прикрепленного файла, который содержит изготовленный сертификат в электронной форме.

Копия сертификата ключа проверки ЭП на бумажном носителе предоставляется его владельцу под роспись при личном обращении в Удостоверяющий центр.

3.3.6.2. Выдача квалифицированного сертификата, созданного Удостоверяющим центром, осуществляется при условии идентификации личности заявителя в Удостоверяющем центре либо Оператором Удостоверяющего центра.

При вручении квалифицированного сертификата владельцу Удостоверяющий центр знакомит его с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с

информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

При выдаче квалифицированного сертификата Удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его Удостоверяющего центра).

При выдаче квалифицированного сертификата Удостоверяющий центр вносит в реестр сертификатов Удостоверяющего центра информацию о выданном квалифицированном сертификате и сведения о владельце сертификата.

3.3.7. Начало периода действия ключа ЭП пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП пользователя Удостоверяющего центра.

Максимальный срок действия ключа ЭП пользователя Удостоверяющего центра, соответствующего сертификату ключа проверки ЭП, владельцем которого он является, определяется требованиями СКЗИ, использующим данный ключ ЭП.

3.3.8. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата заявителя с момента получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, а также надлежаще оформленных документов и сведений, представленных заявителем Оператору Удостоверяющего центра для получения квалифицированного сертификата, зависит от сроков и результатов получения сведений, запрашиваемых Удостоверяющим центром с использованием инфраструктуры из государственных информационных ресурсов, но не может превышать 3 (трех) рабочих дней со дня получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата.

В случае, если заявитель, после получения от Оператора Удостоверяющего центра уведомления о необходимости предоставления документов либо их надлежащим образом заверенные копий и сведений, необходимых для создания и выдачи квалифицированного сертификата, не представил их, Оператор Удостоверяющего центра по истечении 30 (тридцати) дней со дня получения соответствующего заявления на создание и выдачу квалифицированного сертификата отказывает в создании и выдаче квалифицированного сертификата и направляет соответствующее уведомление заявителю.

3.4. Простая электронная подпись оформляется абоненту Клиенту в случае, если абонент Клиента одновременно соответствует следующим критериям:

- является нерезиденом Российской Федерации,
- не имеет действующую рабочую визу и разрешения на работу в Российской Федерации,
- не имеет СНИЛС.

Под простой электронной подписью понимается электронная подпись, которая формируется без использования криптографических преобразований и подтверждает факт формирования электронной подписи определенным лицом посредством использования кодов и паролей.

Простой электронной подписью является сочетание 2 элементов - идентификатора и пароля ключа. Идентификатором является TIN (PAN, DIN или иной идентификационный номер лица, который является функциональным аналогом TIN в юрисдикции получателя) номер заявителя – абонента Клиента, полученный в том государстве, резидентом которого он является, а паролем ключа - последовательность символов, созданная в соответствии с настоящими Условиями.

Оператор Удостоверяющего центра в случае получения ключа непосредственно у него обязан установить личность заявителя - физического лица или уполномоченного лица, обратившегося за получением ключа.

Установление личности заявителя может быть осуществлено одним их следующих способов:

— предъявление абонентом Клиента основного документа, удостоверяющего личность, а также документа, подтверждающего его право действовать от имени юридического лица без доверенности либо соответствующая доверенность (в случае подачи заявления при личном приеме);
— подтверждение сведений, представленных заявителем путем использования индивидуальных средств коммуникации абонента. При этом абонент Клиента обязан предоставить в Банк выписку, выданную провайдером телефонной (сотовой) связи и подтверждающую принадлежность телефонного номера абоненту Клиента Банка на дату оформления ключа простой электронной подписи с нотариально заверенным переводом на русский язык либо нотариально удостоверенное заявление, подписанное единоличным исполнительным органом клиента Банка, с нотариально заверенным переводом на русский язык (при оформлении в иностранном государстве).

Использование простой электронной подписи осуществляется с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие Банка и Клиента в электронной форме.

Первичный ключ простой электронной подписи выдается абоненту Клиента одним из следующих способов и с соблюдением следующих условий:

— непосредственно у Оператора Удостоверяющего центра;
— отправкой запечатанного конверта, содержащего карточку абонента/оператора Клиента; реквизиты первичного персонального пароля абонента/оператора Клиента (в том числе первичный пароль носителя ключевой информации) по адресу Уполномоченного лица, указанному в Заявлении на создании сертификата, почтой России или курьерской службой;
— путем использования индивидуальных средств коммуникации абонента Клиента, предусматривающих возможность получения ключа с помощью короткого текстового сообщения на абонентский номер абонента Клиента, указанного в отправленного с корпоративного телефонного номера Банка.

3.5. За создание квалифицированного сертификата и ключа простой электронной подписи Банк взимает комиссионное вознаграждение в соответствии с Тарифами.

3.6. Если в соответствии с Заявлением на подключение или Заявлением на внесение изменений установка ПО производится силами Банка, уполномоченный представитель Клиента по телефону согласует с Банком порядок и срок установки, который не должен превышать 10 (Десяти) рабочих дней.

В согласованный срок представитель Банка прибывает к Клиенту для установки Системы ДБО. При этом, указанный в пункте 3.6 подпункт 1 настоящих Условий пакет, Клиенту может быть доставлен представителем Банка. В этом случае Клиент после проверки содержимого пакета подписывает 2 (Два) экземпляра подписанного со стороны Банка Акта приема-передачи носителей ключевой информации, программного обеспечения и средств криптографической защиты информации (Приложение 6 к настоящим Условиям). Один подписанный экземпляр каждого из указанных выше документов передается представителю Банка, второй экземпляр остается у Клиента. На экземпляре Банка представитель Клиента ставит отметку о получении документа.

За выезд представителя Банка Клиент уплачивает Банку вознаграждение в соответствии с Тарифами.

Представитель Банка производит установку ПО, настройку и проверку функционирования АРМ Клиента, обучение сотрудников Клиента приемам и методам работы с системой, а также методике проверки достоверности ЭП, смены ключей ЭП и т.п.

Клиент проверяет работоспособность системы ДБО и по результатам подписывает в 2 (Двух) экземплярах Акт о вводе в действие услуги «Дистанционное банковское обслуживание» и передает 1 (Один) экземпляр представителю Банка. На экземпляре Банка представитель Клиента ставит отметку о получении документа.

3.7. В случае если установка АРМ Клиента производилась силами Клиента, в течение 3 (трех) рабочих дней после получения конверта с документами и носителем ключевой информации, Клиент направляет в Банк через систему ДБО подписанный экземпляра Акта о вводе в действие услуги «Дистанционное банковское обслуживание» и в течение 10 (десяти) рабочих дней возвращает в Банк 2 (Два) подписанных экземпляра Акта о вводе в действие услуги «Дистанционное банковское обслуживание»,.

Подключение АРМ Клиента к системе ДБО в режиме исполнения ЭД производится Банком не позднее трех рабочих дней, следующих за днем получения Банком всех необходимых для подключения к системе ДБО.

ПРАВА И ОБЯЗАННОСТИ ВЛАДЕЛЬЦА СЕРТИФИКАТА

3.7. Владелец Сертификата имеет право:

- обратиться в Банк или Удостоверяющий центр для получения услуг, оказываемых Удостоверяющим центром в соответствии с настоящим Порядком, в том числе для регистрации в Удостоверяющем центре в качестве Пользователя Удостоверяющего центра и получения квалифицированного сертификата;
- получить квалифицированный сертификат Удостоверяющего центра в форме электронного документа и его копию на бумажном носителе, заверенную Удостоверяющим центром, при условии установления Удостоверяющим центром личности лица, обращающегося за получением данного сертификата и подтверждения его правомочий;
- при получении квалифицированного сертификата получить ключ электронной подписи и ключ проверки электронной подписи Пользователя Удостоверяющего центра, созданные Удостоверяющим центром;
- применять квалифицированные сертификаты, выданные Удостоверяющим центром, для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в квалифицированных сертификатах;
- получать средства электронной подписи, обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи;
- создавать с использованием средства электронной подписи ключ электронной подписи и ключ проверки электронной подписи;
- обращаться в Удостоверяющий центр для проведения проверки подлинности электронной подписи, основанной на квалифицированном сертификате, выданном Удостоверяющим центром;
- обращаться в Банк или Удостоверяющий центр для прекращения действия (отзыва) квалифицированного сертификата, владельцем которого он является, в течение срока действия данного квалифицированного сертификата;
- обращаться в Банк или Удостоверяющий центр для получения консультаций и технической поддержки по вопросам использования электронной подписи, средств электронной подписи, вопросам обеспечения безопасности использования электронной подписи и средств электронной подписи.

3.8. Владелец Сертификата обязан:

- исполнять требования, установленные Законом № 63-ФЗ, принимаемыми в соответствии с ним нормативными правовыми актами и настоящими Условиями;
- предоставлять в соответствии с настоящими Условиями в Банк или Удостоверяющий центр актуальные и достоверные документы, их надлежащим образом заверенные копии и сведения, в том числе необходимые для получения квалифицированного сертификата, регистрации квалифицированного сертификата в единой системе идентификации и аутентификации и (или) регистрации владельца сертификата в единой системе идентификации и аутентификации;
- при подаче заявления указать действующий электронный почтовый адрес владельца для получения извещений, уведомлений от Удостоверяющего центра, связанных с применением ЭП, его аннулированием;
- использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом «Об электронной подписи»;
- при создании или проверке электронной подписи осуществлять проверку действительности квалифицированного сертификата на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;
- при проверке электронной подписи осуществлять проверку принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, а также осуществлять проверку отсутствия изменений, внесенных в этот документ после его подписания;
- применять для формирования электронной подписи только действующий личный ключ;
- не использовать ключ электронной подписи, срок действия которого истек;

— обеспечивать конфиденциальность используемых ключей электронных подписей, в частности принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования, не допускать использование ключей электронных подписей иными лицами без своего согласия;
— уведомлять Банк о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
— не использовать ключ электронной подписи и немедленно обратиться в Банк или Удостоверяющий центр для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена, в том числе в случае утери, кражи, а также в случае, если Владельцу электронной подписи стало известно, что ключ используется или использовался ранее другими лицами;
— не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление на прекращение, действия которого подано в Банк или Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр до момента времени официального уведомления о прекращении действия квалифицированного сертификата, либо об отказе в прекращении действия;
— не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, который аннулирован или действие которого прекращено;
— информировать Банк или Удостоверяющий центр об изменении регистрационных данных владельца сертификата, влияющих на актуальность сведений, содержащихся в квалифицированном сертификате, и обратиться в Удостоверяющий центр для прекращения действия такого сертификата в случае наличия оснований полагать, что несоответствие данных о владельце сертификата и сведений, содержащихся в квалифицированном сертификате, может повлиять на результат проверки электронной подписи при осуществлении обмена информацией с иными участниками информационного взаимодействия.

4. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»

4.1. При необходимости изменения параметров подключения к системе ДБО Клиент на бумажном носителе или по системе ДБО вложением в ЭД с указанием в поле «Тема» - «Уведомление об изменении параметров подключения» направляет в Банк Уведомление об изменении параметров подключения к услуге «Дистанционное банковское обслуживание» по форме Приложения 5 к настоящим Условиям (далее – «Уведомление об изменении параметров подключения»).

4.2. Для исключения ошибок обработки ЭД Клиент должен заблаговременно направить в Банк все подписанные ЭД, а непосредственно перед началом периода ввода в действие новых параметров подключения получить из Банка подготовленные в его адрес ЭД.

4.3. При изменении полномочий абонента Клиента, Клиент одновременно с Уведомлением об изменении параметров подключения направляет в Банк документы, подтверждающие полномочия fбонента. В этом случае Банк не позднее 5-ти рабочих дней со дня получения данных документов, вводит в действие в системе ДБО соответствующий Сертификат с учетом новых полномочий.

4.4. При подключении к Системе ДБО новых абонентов/операторов Клиента в течение 5 (Пяти) рабочих дней после получения Банком Уведомления об изменении параметров подключения Стороны согласовывают сроки передачи пакета, указанного в п. 3.6. настоящих Условий.

Процедура подключения новых абонентов/операторов производится аналогично процедуре подключения абонентов/операторов, описанной в разделе 3 настоящих Условий.

4.5. Подключение новых счетов происходит в течение следующего рабочего дня после дня приема Уведомления об изменении параметров подключения. Клиент информируется о подключении счетов соответствующим сообщением посредством Системы ДБО.

4.6. В дату согласованного ввода в действие новых параметров подключения администраторы АРМ Банка и АРМ Клиента производят перенастройку Системы ДБО, в том числе (при необходимости) системы криптографической защиты информации.

Подключение (отключение) сервиса системы ДБО или замена одного сервиса системы ДБО, установленного у Клиента, на другой сервис системы ДБО производится в следующем порядке:

1) Клиент подает в Банк Уведомление об изменении параметров подключения;

2) подключение Клиента к новому сервису системы ДБО осуществляется аналогично порядку, установленному в разделе 3 настоящих Условий;

3) подключаемый сервис Системы ДБО вводится в эксплуатацию не позднее рабочего дня, следующего за днем предоставления Клиентом в Банк Акта о вводе в действие услуги «Дистанционное банковское обслуживание» (Приложение 7 к настоящим Условиям), свидетельствующего о работоспособности нового сервиса Системы ДБО. Заменяемый сервис Системы ДБО (в случае его отключения при замене одного сервиса Системы ДБО на другой) считается выведенным из эксплуатации в дату введения в эксплуатацию нового сервиса Системы ДБО. Отключение сервиса системы ДБО происходит в течение следующего рабочего дня после дня приема Уведомления об изменении параметров подключения.

4.7. При необходимости установления ограничений по параметрам операций с использованием системы дистанционного банковского обслуживания Клиент заполняет Заявление на установление ограничений по параметрам операций с использованием системы дистанционного банковского обслуживания при форме Приложения 21 к настоящим Условиям.

Устанавливаемые ограничения вводится в эксплуатацию не позднее рабочего дня, следующего за днем предоставления Клиентом в Банк Заявление на установление ограничений по параметрам операций с использованием системы дистанционного банковского обслуживания.

5. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ СМЕНЫ КЛЮЧА ЭП ВЛАДЕЛЬЦА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

5.1. За 30 (Тридцать) дней до истечения срока действия ключа ЭП абонента/оператора Клиента Система ДБО начинает при каждой загрузке предлагать абоненту/оператору произвести плановую смену его ключа ЭП.

5.2. Смена ключа ЭП осуществляется владельцем сертификата в следующих случаях:

1) в связи с истечением установленного срока действия ключа электронной подписи;

2) на основании заявления, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

3) не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

4) установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

5) вступило в силу решение суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию;

6) в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или договором оказания услуг удостоверяющего центра.

В случае наступления обстоятельств, указанных в подпунктах 3) – 5) пункта 5.2. настоящих Условий, Удостоверяющий центр аннулирует квалифицированный сертификат владельца сертификата и уведомляет об этом владельца сертификата. Информация о прекращении действия сертификата вносится Удостоверяющим центром в реестр сертификатов в течение 12 (двенадцати) часов с момента наступления указанных обстоятельств, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

5.3. Смена ключа электронной подписи Пользователя Удостоверяющего центра осуществляется в соответствии процедурами создания ключей электронных подписей и ключей проверки электронных подписей, приведенной в раделе 4 настоящих Условий.

Создание Удостоверяющим центром нового ключа электронного подписи осуществляется одновременно с созданием и выдачей Пользователю Удостоверяющего центра ключа проверки электронной подписи и квалифицированного сертификата на основании документов, представленных Оператору Удостоверяющего центра.

Заявление на смену ключа ЭП владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной ЭП владельца квалифицированного сертификата.

5.4. Для сохранения возможности реализации всех соответствующих прав абонента/оператора Клиента в Системе ДБО Владелец Сертификата обязан представить в Банк заявление на изготовление ключа ЭП и ключа проверки ЭП и выполнить все процедуры, предусмотренные п. 3.3. настоящих Условий не позднее, чем за 3 рабочих дня до срока истечения действия Сертификата

5.5. Если абонент/оператор Клиента не произвел своевременную плановую смену ключа ЭП, то у него прекращается возможность реализации всех соответствующих прав абонента/оператора Клиента в Системе ДБО. В случае необходимости восстановления возможности реализации всех соответствующих прав абонента/оператора Клиента в Системе ДБО, Клиент должен осуществить действия в соответствии с разделом 4 настоящих Условий.

5.6. В случае если абонент/оператор Клиента не произвел своевременную плановую смену ключа ЭП, но при этом Договор ДБО не расторгнут, комиссия за пользование системой ДБО продолжает взиматься до дня расторжения договора ДБО.

6. ПОРЯДОК ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ КЛЮЧЕЙ ЭЛЕКТРОННЫХ ПОДПИСЕЙ ЗАЯВИТЕЛЕЙ

6.1. Конфиденциальность ключей электронных подписей заявителей обеспечивается Удостоверяющим центром в период времени получения носителя ключевой информации от заявителя и записи на него ключей электронной подписи, созданных Удостоверяющим центром, до момента передачи ключевого носителя заявителю, при этом создание и запись ключа электронной подписи на ключевой носитель, представленный заявителем осуществляется Удостоверяющим центром только в случае личного прибытия заявителя в Удостоверяющий центр и в его присутствии.

6.2. После создания Удостоверяющим центром ключа электронных подписи заявителя и его записи на носитель ключевой информации, представленный непосредственно перед созданием ключа электронных подписи заявителем, данный носитель ключевой информации, в том числе содержащий ключ электронной подписи, указанный ключевой носитель выдается заявителю под расписку, при этом вносится запись в соответствующий журнал учета Удостоверяющего центра о выдаче ключа электронной подписи и соответствующего ему квалифицированного сертификата, с которой заявитель должен быть ознакомлен под расписку.

6.3. Удостоверяющий центр не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи заявителя (владельца сертификата).

6.4. В случае, если заявитель направил в Удостоверяющий в электронном виде ключ электронной подписи по информационно-телекоммуникационной сети или иными способами, не гарантирующими обеспечение конфиденциальности ключа электронной подписи, такой ключ считается скомпрометированным в связи нарушением конфиденциальность ключа электронной подписи, при этом заявитель обязан провести процедуру его внеплановой смены. В случае наличия действующего квалифицированного сертификата, соответствующего указанному ключу электронной подписи, такой квалифицированный сертификат прекращает действие, при этом владелец сертификата обязан обратится в Удостоверяющий центр с заявлением о прекращении его действия.

6.5. Владелец сертификата, получивший квалифицированный сертификат в Удостоверяющем центре обеспечивает конфиденциальность ключей электронных подписей и обязан:

- хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;
- не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;
- уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

— не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

7. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

7.1. К событиям, связанным с компрометацией ключей, относятся (включая, но не ограничиваясь) следующие:

1) потеря ключевых носителей;
2) потеря ключевых носителей с их последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) нарушение правил хранения и уничтожения (после окончания срока действия);
5) возникновение подозрений на утечку информации или ее искажение;
6) нарушение печати на сейфе с ключевыми носителями;
7) 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 несанкционированных действий злоумышленника).

7.2. Различаются два вида компрометации ключа ЭП: явную и неявную. События, указанные в пп 1)-4) пункта 7.1. настоящих Условий трактуются как явная компрометация ключей. События, указанные в пп 5)-7) настоящих Условий требуют специального рассмотрения в каждом конкретном случае.

7.3. При выявлении одной из Сторон признаков несанкционированного использования ключа ЭП (в том числе несанкционированного списания или попытки списания денежных средств со счета), Сторона, выявившая признаки несанкционированного использования ключа ЭП должна незамедлительно уведомить другую Сторону о данном факте.

7.4. Владелец Сертификата самостоятельно принимает решение о нарушении конфиденциальности или угрозе нарушения конфиденциальности своего Ключа ЭП, в частности, в соответствии с положениями настоящих Условий. В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности Ключа ЭП Владелец Сертификата обязан обратиться, а Клиент Банка - обеспечить обращение Владельца Сертификата в Банк для прекращения (аннулирования) действия Сертификата в порядке, предусмотренном разделом 8 настоящих Условий. Правилами Системы может быть установлена обязанность Владельца Сертификата / Уполномоченного лица или право Банка совершить дополнительные действия в случае нарушения конфиденциальности Ключа ЭП Владельца Сертификата.

7.5. Действия в случае компрометации ключа ЭП Клиента:

1) решение о компрометации ключа ЭП может быть принято абонентом/оператором Клиента, на имя которого выпускался ключ ЭП, либо единоличным исполнительным органом Клиента;

2) работа на скомпрометированном ключе ЭП должна быть полностью остановлена немедленно после обнаружения факта/подозрения в компрометации ключа ЭП;

3) в случае принятия решения о компрометации ключа ЭП Клиент незамедлительно должен уведомить об этом Банк по телефону. При этом Клиент должен сообщить следующую информацию:

   – номер Договора и дату его заключения,

   – фамилию, имя, отчество абонента/оператора Клиента, которому принадлежит скомпрометированный ключ ЭП,

   – идентификатор (UID) скомпрометированного ключа ЭП.

Получив предварительное сообщение по телефону о компрометации ключа ЭП, Банк немедленно приостанавливает обработку электронных документов, подписанных скомпрометированным ключом ЭП, до получения уведомления о компрометации ключа ЭП в форме документа на бумажном носителе или по Системе ДБО;

4) не позднее рабочего дня, следующего за датой получения Банком по телефону предварительного сообщения о компрометации ключа ЭП, Клиент должен предоставить в Банк Уведомление о компрометации ключа ЭП по форме Приложения 12 к настоящим Условиям (далее – Уведомление о компрометации). Уведомление о компрометации может быть направлено в Банк:

- на бумажном носителе, подписанное единоличным исполнительным органом Клиента либо лицом, действующим на основании надлежащим образом оформленной доверенности в рамках предоставленных ему полномочий, и заверенное оттиском печати Клиента, или
- с использованием системы ДБО путем направления Уведомления о компрометации как вложение в ЭД с указанием в поле «Тема» сообщения «Уведомление о компрометации ключа ЭП» (уведомление направляется с использованием действующих (нескомпрометированных) ключей, при их наличии у Клиента).

В случае если в подтверждение предварительного сообщения о компрометации ключа ЭП, полученного от Клиента по телефону, Банк не получит Уведомление о компрометации в указанной в настоящем подпункте форме и в установленный срок, Банк возобновляет обработку электронных документов, подписанных соответствующим ключом ЭП до получения от Клиента надлежащим образом оформленного Уведомление о компрометации;

5) после получения Уведомления о компрометации ключа ЭП Банк отзывает Сертификат скомпрометированного ключа ЭП путем помещения его в список отозванных Сертификатов и направляет Клиенту данный список через Систему ДБО;

7.6. Действия в случае компрометации ключа ЭП абонента Банка:

1) о компрометации ключа ЭП своего абонента Банк немедленно уведомляет Клиента по Системе ДБО путем передачи соответствующего сообщения и прекращает передачу ЭД, подписанных с помощью скомпрометированного ключа ЭП;
2) получив сообщение о компрометации ключей ЭП, Клиент немедленно прекращает приём и обработку ЭД, подписанных с помощью скомпрометированного ключа ЭП абонента Банка;
3) Клиент продолжает приём и обработку ЭД, подписанных с помощью других (не скомпрометированных) ключей ЭП абонентов Банка;
4) Клиент осуществляет визуальный контроль полученного Сертификата абонента Банка;
5) Клиент начинает приём и обработку ЭД, подписанных с помощью вновь созданных ключей ЭП абонента Банка.

8. СОПРОВОЖДЕНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛИЕНТА

8.1. При возникновении вопросов по работе с системой ДБО или в случае сбоев в работе программного обеспечения системы ДБО Клиента (в том числе баз данных хранения документов) Клиент:

1) обращается в Банк за консультацией;
2) в случае невозможности решения проблемы по телефону Клиент отправляет Заявление на выполнение работ по сопровождению Системы ДБО (Приложение 8 к настоящим Условиям) (далее – Заявление на выполнение работ):
   - на бумажном носителе в 1 (Одном) экземпляре;
   - по Системе ДБО, при наличии такой возможности, по форме Заявления на выполнение работ, подтвержденного ЭП, вложением, с указанием в поле «Тема» - «Заявление на выполнение работ по сопровождению Системы ДБО».

8.2. В случае невозможности выезда представителя Банка в дату, указанную Клиентом в Заявлении на выполнение работ, Банк по телефону или на бумажном носителе уведомляет об этом Клиента, и согласовывает с ним иной разумный срок начала работ.

8.3. По окончании работ Клиент и Банк подписывают Акт приема-сдачи работ (Приложение 9 к настоящим Условиям) об отсутствии претензий по указанному в этом Акте перечню работ в 2 (двух) экземплярах по одному для каждой Стороны. Представитель Клиента ставит отметку на экземпляре Банка о получении документа.

8.4. Оплата услуг по сопровождению Системы ДБО производится согласно действующему Тарифу.

9. ПРОЦЕДУРЫ, ОСУЩЕСТВЛЯЕМЫЕ ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ И АННУЛИРОВАНИИ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

9.1. Квалифицированный сертификат прекращает свое действие:

— в связи с истечением установленного срока действия квалифицированного сертификата; на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

— в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;

— в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или соглашением (договором оказания услуг Удостоверяющего центра) с владельцем сертификата.

9.2. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

— не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

— установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

— вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию.

9.3. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалифицированного сертификата

Прекращение действия (аннулирование) сертификата ключа проверки ЭП, изготовленного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению на аннулирование сертификата его владельца.

Заявитель имеет право предоставить в Удостоверяющий центр заявление о прекращении действия квалифицированного сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

Заявление о прекращении действия квалифицированного сертификата направляется заявителем в Удостоверяющий центр в случае:

— принятия Пользователем, решения о прекращении действия квалифицированного сертификата владельца сертификата;

— изменились сведения о владельце сертификата, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными;

— прекращения полномочий владельца сертификата;

— нарушена конфиденциальность ключа электронной подписи владельца сертификата.

9.4. Заявление о прекращении действия квалифицированного сертификата оформляется по форме Приложения № 17 к настоящим Условиям, и должно соответствовать следующим требованиям:

В случае, если заявителем является юридическое лицо, заявление должно быть заверено печатью юридического лица, а также содержать:

— сведения о квалифицированном сертификате, действие которого прекращается;

— дата письма;

— собственноручную подпись владельца сертификата;

— причину прекращения действия квалифицированного сертификата.

9.5. После поступления заявления о прекращении действия квалифицированного сертификата и его регистрации в Удостоверяющем центре осуществляется:

— проверка заявления на соответствие требованиям, указанным в пункте 9.4. настоящих Условий;

— проверка соответствия сведений, указанных в заявлении, и сведений, которые имеются в Удостоверяющем центре о владельце сертификата и выданном ему квалифицированном сертификате;

— проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата.

9.6. Проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата, и удостоверение его личности и осуществляются в порядке, предусмотренном для процедуры создания и выдачи сертификата, с соблюдением следующих условий:

С заявлением о прекращении действия квалифицированного сертификата, владельцем которого является юридическое лицо, имеет право обращаться физическое лицо, имеющее право действовать от имени этого юридического лица без доверенности. Полномочия физического лица, имеющего право действовать от имени этого юридического лица без доверенности, подтверждаются Удостоверяющим центром с использованием инфраструктуры и актуальных сведений, полученных Удостоверяющим центром из государственных информационных ресурсов.

В случае, если заявление не соответствует условиям и требованиям в соответствии с пунктом 9.4. настоящих Условий, в том числе в случае, если квалифицированный сертификат, сведения о котором указаны в заявлении о прекращении действия квалифицированного сертификата, не выдавался Удостоверяющим центром, либо сведения, указанные в заявлении, не соответствуют сведениям о владельце сертификата, либо не подтверждены полномочия владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата, Удостоверяющий центр отказывает в проведении процедуры прекращения действия квалифицированного сертификата и направляет соответствующее уведомление заявителю в течение 1 (одного) рабочего дня со дня получения сведений из государственных информационных ресурсов, в случае, если полномочия лица, обращающегося для прекращения действия квалифицированного сертификата, не подтверждены, но не позднее 3 (трех) рабочих дней со дня получения заявления о прекращении действия квалифицированного сертификата.

В случае, если причиной заявления о прекращении действия квалифицированного сертификата является нарушение конфиденциальность ключа электронной подписи владельца сертификата, то в таком случае Заявитель не имеет право предоставить в Удостоверяющий центр заявление о прекращении действия квалифицированного сертификата в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

10. РАСТОРЖЕНИЕ ДОГОВОРА СИСТЕМЫ ДБО ПО ИНИЦИАТИВЕ КЛИЕНТА

10.1. Сторона, намеренная расторгнуть Договор, письменно уведомляет другую Сторону о своих намерениях не менее, чем за 30 (тридцать) календарных дней до даты расторжения Договора.

Для расторжения Договора ДБО Клиент оформляет в произвольной форме соответствующее уведомление и передает его в Банк одним из следующих способов:

— на бумажном носителе – заявление должно быть подписано уполномоченным должностным лицом и заверено печатью Клиента – 1 (один) экземпляр;
— по Системе ДБО с указанием в поле «Тема» соответственно: «Заявление о расторжении Договора ДБО».

Уведомление должно содержать подтверждение Клиента об уничтожении им всех принадлежащих ему ключей ЭП и паролей.

Договор считается расторгнутым по истечении периода, указанного в уведомлении о расторжении, но не ранее, чем по истечении 30 (тридцати) календарных дней со дня получения Стороной уведомления о расторжении Договора.

В случае если Договор расторгается по инициативе Удостоверяющего центра, соответствующее уведомление передается Владельцу Сертификата Банком от имени Удостоверяющего центра.

11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

11.1. Настоящий раздел определяет общий порядок электронного документооборота с использованием Системы ДБО.

11.2. Для передачи в Банк ЭД/приема из Банка ЭД Клиенту необходимо установить соединение с Банком, руководствуясь правилами, приведенными в Пользовательской документации.

11.3. Каждый передаваемый Клиентом ЭД подписывается ЭП в количестве и составе, соответствующем пункту 2.10 настоящих Условий, а также карточке с образцами подписей и оттиска печати Клиента, имеющейся в распоряжении Банка.

11.4. Текущая стадия обработки ЭД в Системе ДБО, как на АРМ Клиента, так и на АРМ Банка, отражается статусом документа, который устанавливается на АРМ на основании полученных ЭСИД, удостоверенных ЭП абонента Банка.

11.5. **Подготовка и отправка в Банк ЭД в Системе ДБО**:

1) абонент/оператор Клиента производит подготовку ЭД, руководствуясь правилами, приведенными в пункте 10.5 настоящих Условий, а также законодательством Российской Федерации и нормативными актами Банка России, и сохраняет подготовленные ЭД в базе данных Системы ДБО. Подготовленные и сохраненные ЭД получают статус «Новый»;
2) абоненты Клиента, обладающие правом подписи, подписывают ЭД Клиента с помощью принадлежащих им ключей ЭП. При этом Система ДБО автоматически проверяет корректность каждой ЭП. Если ЭП некорректна или абонент не имеет соответствующих полномочий, данная ЭП не сохраняется и ЭД считается неподписанным;
3) если ЭД подписан необходимым количеством корректных ЭП, документ приобретает статус «Подписан»;
4) абонент/оператор Клиента выбирает из общего списка документов ЭД, подлежащие отправке и находящиеся в статусе «Подписан», и передаёт их на обработку в Банк;
5) Система ДБО последовательно проводит автоматический контроль корректности ЭП и реквизитов каждого ЭД. Если ЭД подписан необходимым количеством корректных ЭП абонентов Клиента, то он получает статус «Принят»;
6) ЭД с некорректными ЭП и/или с ошибками реквизитов не принимаются Банком в обработку и остаются в прежнем статусе. АРМ Клиента отображает сообщение с расшифровкой ошибок;
7) время присвоения ЭД статуса «Принят» считается временем поступления документа в Банк;
8) ЭД Клиента, перечисленные в подпункте а) пункта 1 Приложения 2 к настоящим Условиям Перечень электронных документов, используемых в системе дистанционного банковского обслуживания, суммой от 0,01 копейки по желанию Клиента могут подтверждаться одноразовыми паролями СМС.

Одноразовый пароль СМС отправляется на телефонный номер Клиента, предоставляемый оператором связи Российской Федерации, указанный в подпункте «g» пункта 3.1. Договора ДБО. Срок действия направленного одноразового пароля - 5 минут. По истечение 5 минут либо в случае, если при вводе одноразового пароля допущена ошибка, Клиенту направляется второй одноразовый пароль СМС. По истечение 5 минут либо в случае, если при вводе одноразового пароля допущена ошибка, Клиенту направляется третий одноразовый пароль СМС. Если по истечению трех попыток ЭД Клиента не подтверждён, ЭД присваивается статус «Не принят».

Авторизация средствами "одноразовый пароль СМС" не предусматривается для ЭД, перечисленных в подпункте б) пункта 1 и пункте 2 Приложения 2 к настоящим Условиям.

a) присвоение ЭД статуса «Принят» не означает безусловного принятия Банком обязательства исполнить ЭД, т.к. документ еще должен пройти различные виды банковского контроля, в том числе на соответствие требованиям законодательства РФ;
b) поступившие ЭД исполняются в сроки, установленные Договором банковского счета, а также иными соглашениями и договорами, заключенными Сторонами.

11.6. **Обработка ЭПД Клиента Банком**:

a) статус «Не принят банком» присваивается ЭПД (Приложение 2 к настоящим Условиям), если Банк не подтвердил по данному документу списание средств со счета Клиента (комментарии Банка содержатся в разделе «Отметки банка»);
b) статус «Исполнен» присваивается документу, если Банк подтвердил списание средств со счета Клиента (документ исполнен со счета Клиента);
c) Клиент может направить в Банк средствами Системы ДБО «Запрос на отзыв документа», подписанный ЭП. При наличии у Банка такой возможности, последний исполняет Запрос и присваивается ЭПД статус «Отозван», а Запросу - «Исполнен»;
d) при любых изменениях статуса ЭПД, перечисленных в настоящем разделе, Банк направляет Клиенту соответствующую квитанцию;

e) электронным служебно-информационные документам (Приложение 2 к настоящим Условиям) в случае их принятия Банком присваивается статус «Принят ВК»; в случае непринятия - «Отказан ВК»;

11.7. О совершении рублевого платежа, проведенного с использованием Системы ДБО, и превышающего сумму в 30 000 (тридцать тысяч) рублей, Банк информирует Клиента посредством направления sms-сообщения на телефонный номер Клиента, предоставляемый оператором связи Российской Федерации, указанный в подпункте c) пункта 3.1. Договора ДБО.

SMS-сообщения передаются Банком один раз. Вне зависимости от возможности передачи сообщений на номер телефона: номер телефона не существует, аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины) SMS-сообщение считается отправленным Клиенту, что может быть подтверждено оператором связи.

Сообщение со статусом «Получено» или «Received», сформированное системой «Сервер нотификации», используемой Банком, а равно подтверждающий соответствующий факт документ оператора связи, обслуживающего телефонный номер Клиента, указанный в подпункте c) пункта 3.1. Договора ДБО, является необходимым и достаточным доказательством того, что sms-сообщение было доставлено адресату в указанное в таком сообщении/документе время.

Информация о любом рублевом платежном документе, принятом Банком, направляется также на адрес электронной почты, указанный в подпункте b) пункта 3.1. Договора ДБО.

11.8. **Получение выписки по счету**:

a) ежедневно по рабочим дням Банк формирует и предоставляет Клиенту возможность получения выписки в виде ЭД по всем счетам, обслуживаемым в Системе ДБО. В выписке отражаются все операции, проведенные по счету Клиента, за предыдущий операционный день Банка;

b) Клиент может просмотреть выписку по счёту за произвольный период (не превышающий календарный месяц).

12. ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПОДЛИННОСТЬЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

12.1. Владельцы Сертификатов направляют претензии, вытекающие из Договора, Удостоверяющему центру через Банк

Ощий порядок разрешения двух типов конфликтных ситуаций между Клиентом и Банком, связанных с подлинностью ЭД:

— отказ Банка (Клиента) от ЭД, т.е. Банк (Клиент) утверждает, что его абонент не подписывал принятый Клиентом (Банком) ЭД, а Клиент (Банк) утверждает обратное),

— отказ Банка (Клиента) от факта получения ЭД, т.е. Клиент (Банк) утверждает, что посланный им ЭД был принят Банком (Клиентом), а Банк (Клиент) это отрицает);

1) инициатор рассмотрения конфликтной ситуации (далее – Заявитель) должен подготовить и направить другой стороне (далее – Ответчик) документ (заявление), подписанный уполномоченным должностным лицом, с изложением всех обстоятельств случившегося. До подачи заявления Заявителю рекомендуется убедиться в неизменности используемой ЭП, а также отсутствии фактов/признаков несанкционированных действий со стороны его персонала. В заявлении должно быть указано:

   — наименование Заявителя,

   — дата и номер оспариваемого ЭД,

   — тип, характер и возможно полное описание претензии;

2) Ответчик в течение 10 (Десяти) дней с момента получения заявления рассматривает его, и либо удовлетворяет претензию Заявителя, либо передает Заявителю письменный отказ в удовлетворении претензии с обоснованием причины отказа;

3) в случае несогласия с мотивировочной частью отказа Заявитель направляет Ответчику письменное заявление о своем несогласии и требование о формировании экспертной комиссии для рассмотрения конфликтной ситуации;

4) на основании указанного заявления, не позднее 10 (Десяти) дней с момента его получения Ответчиком, совместным решением Банка и Клиента создается экспертная комиссия для

рассмотрения возникшей конфликтной ситуации. Представителями в экспертной комиссии от Заявителя и Ответчика могут быть лица, как из числа их сотрудников (в равном количестве от каждой стороны), так и иных компетентных организаций. Полномочия представителей Сторон подтверждаются в установленном законом порядке. Состав экспертной комиссии согласовывается Банком и Клиентом и утверждается двусторонним актом. Рекомендуется следующий состав экспертной комиссии:

— абоненты, участвовавшие в обмене ЭД, со стороны Заявителя и Ответчика,

— представители технических подразделений Заявителя и Ответчика.

В случае необходимости могут привлекаться независимые эксперты и технические специалисты, в том числе из организаций-изготовителей ПО;

5) в течение 3 (Трех) дней с момента формирования экспертной комиссии Банк и Клиент предоставляют экспертной комиссии следующие материалы:

— заявление Заявителя с изложением сути претензии,

— мотивированный письменный отказ Ответчика в удовлетворении претензии Заявителя,

— оспариваемые ЭД, подписанные ЭП, а также квитанции на эти ЭД,

— распечатки Сертификатов ключей ЭП абонентов Сторон и полный набор Сертификатов ключей ЭП абонентов Банка и Клиента, запросов на указанные Сертификаты от Сертификата, соответствующего распечатке, до Сертификата ключей ЭП, соответствующих закрытым ключам ЭП, с использованием которых формировалась ЭП спорного ЭД и ЭП квитанции на него на дискетах или иных носителях информации (компакт-дисках, флэш-накопителях и т.д.) в виде файлов,

— ранее оформленные сторонами Уведомления об изменении параметров подключения к Системе ДБО.

Банк предоставляет экспертной комиссии:

— эталонную ПЭВМ для автоматизированного рабочего места разбора конфликтной ситуации,

— полученный от производителя средств ЭП инсталляционный комплект эталонного ПО, предназначенного для проверки ЭП оспариваемого ЭД,

— другие материалы, имеющие отношение к сути рассматриваемой претензии;

6) Стороны обязаны способствовать работе экспертной комиссии и своевременно предоставлять все необходимые данные и материалы;

7) экспертная комиссия на территории Банка рассматривает спорную ситуацию. При этом проверка корректности ЭП на оспариваемых ЭД осуществляется в следующем порядке:

— в присутствии членов экспертной комиссии администратор АРМ Банка устанавливает на автоматизированное рабочее место разбора конфликтной ситуации (эталонную ПЭВМ) эталонное ПО с предоставленного экспертной комиссии инсталляционного комплекта,

— экспертная комиссия убеждается в работоспособности эталонного ПО,

— экспертная комиссия с помощью эталонного ПО производит проверку корректности ЭП, которой подписан оспариваемый ЭД,

— экспертная комиссия не позднее 7 (Семи) дней после получения всех материалов, указанных в подпункте 11.1 6) настоящих Условий, большинством голосов членов принимает решение о виновности той или иной Стороны, оформляет его в виде акта на бумажном носителе, который подписывается всеми членами экспертной комиссии;

8) акт экспертной комиссии является окончательным и пересмотру не подлежит. Предписываемые данным актом действия обязательны для Сторон;

9) акт экспертной комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта;

10) в случае невозможности принятия решения экспертной комиссией, а также в случае несогласия одной из Сторон с принятым экспертной комиссией решением, уклонения одной из Сторон от формирования экспертной комиссии, препятствования участию второй Стороны в

работе экспертной комиссии, каждая из Сторон вправе передать спор на рассмотрение в Арбитражный суд по месту нахождения Банка.

12.2. Порядок принятия экспертной комиссией решения по конфликту в связи с отказом Стороны от факта направления/подписания электронного документа (Заявитель утверждает, что его абонент не подписывал принятый и исполненный Ответчиком ЭД, а Ответчик утверждает обратное):

a) запрашивается спорный ЭД от Ответчика. В случае отказа Ответчика предоставить спорный ЭД - конфликт разрешается в пользу Заявителя;

b) проверяется корректность ЭП абонента для предоставленного ЭД в соответствии с процедурой, установленной пунктом 11.4 настоящих Условий. Если ЭП признается некорректной, конфликт разрешается в пользу Заявителя;

c) в остальных случаях конфликт разрешается в пользу Ответчика.

12.3. Порядок принятия экспертной комиссией решения по конфликту в связи с отказом Стороны от факта получения электронного документа **(**Заявитель утверждает, что созданный им ЭД с корректными ЭП в соответствии с правилами эксплуатации Системы ДБО был передан Ответчику и принят последним, а Ответчик отрицает факт приема данного ЭД):

1) запрашивается спорный ЭД и соответствующая квитанция о его доставке от Заявителя. В случае отказа Заявителя предъявить спорный ЭД или квитанцию о его приеме конфликт разрешается в пользу Ответчика;

2) проверяется корректность ЭП абонента Заявителя в ЭД в соответствии с процедурой, установленной пунктом 11.4 настоящих Условий. В случае некорректности ЭП конфликт разрешается в пользу Ответчика;

3) проверяется корректность ЭП абонента Ответчика в квитанции в соответствии с процедурой, установленной пунктом 11.4 настоящих Условий. В случае некорректности ЭП конфликт разрешается в пользу Ответчика;

4) проверяется соответствие квитанции ЭД. В случае несоответствия квитанции ЭД конфликт разрешается в пользу Ответчика;

5) в остальных случаях конфликт разрешается в пользу Заявителя.

12.4. Процедура проверки корректности электронной подписи на электронном документе при разрешении вопроса о подлинности ЭД или его квитанции:

1) от стороны, предоставившей ЭД, запрашивается Сертификат ключа ЭП, с использованием которого была сформирована ЭП для спорного ЭД и/или квитанции. Проверяется ЭП спорного ЭД на автоматизированном рабочем месте разбора конфликтных ситуаций в соответствии с пользовательской документацией. Если программа не признает ЭП корректной на момент её создания, то принимается решение о некорректности ЭП ЭД;

2) если у одной из сторон возникают сомнения в принадлежности Сертификата ключа ЭП абоненту, осуществляется процедура проверки принадлежности этого Сертификата согласно пункту 11.5 настоящих Условий;

3) в случае если Сертификат признается не принадлежащим данному абоненту, ЭП ЭД признается некорректной;

4) в остальных случаях принимается решение о корректности ЭП абонента для ЭД.

12.5. Процедура проверки принадлежности Сертификата абоненту (действующего или выведенного из действия и хранящегося в архиве);

1) для проверки принадлежности Сертификата абоненту Клиента у Банка запрашивается распечатка Сертификата ключа ЭП абонента Клиента и полный набор Сертификатов открытых ключей ЭП абонента Клиента и запросов на Сертификаты от Сертификата, соответствующего распечатке, до Сертификата, принадлежность которого проверяется. Если распечатка Сертификата ключа ЭП абонента Клиента или набор Сертификатов Банком не предъявляется или имеются разрывы в цепочке запрос-Сертификат, конфликт разрешается в пользу Клиента;

2) если предъявляется полный набор Сертификатов и распечатка Сертификата ключа ЭП абонента Клиента, то сначала проверяется соответствие первого Сертификата распечатке Сертификата ключа ЭП абонента Клиента. В случае совпадения их содержимого осуществляется проверка

всей цепочки запросов на Сертификаты и Сертификатов на автоматизированном рабочем месте разбора конфликтной ситуации. По результатам проверки принимается решение о принадлежности или не принадлежности Сертификата абоненту Клиента;

3) для проверки принадлежности Сертификата ключа ЭП абоненту Банка у Клиента запрашивается заверенная Банком распечатка Сертификата Центра сертификации Банка, Сертификат Центра сертификации Банка и Сертификат абонента Банка, чья ЭП оспаривается. В случае отказа Клиента представить вышеуказанные документы, конфликт разрешается в пользу Банка;

4) если Клиентом предъявляются необходимые документы, то сначала проверяется соответствие Сертификата Центра сертификации Банка его распечатке. В случае совпадения их содержимого осуществляется проверка корректности ЭП Центра сертификации Банка для Сертификата абонента Банка на автоматизированном рабочем месте разбора конфликтной ситуации. По результатам проверки принимается решение о принадлежности или не принадлежности Сертификата абоненту Банка.

Приложение 1 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

ПЕРЕЧЕНЬ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛИЕНТА ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Для подключения к услуге «Дистанционное банковское обслуживание» персональный компьютер Клиента должен иметь следующую минимальную конфигурацию:

a) Intel-совместимая платформа с процессором Pentium-4 или выше;

b) Оперативная память объемом не менее 2 гигабайт;

c) Видеоподсистема, обеспечивающая область экрана размером не менее 1024 на 768 пикселей;

d) Постоянное запоминающее устройство (жесткий диск типа HDD или SSD) объемом не менее 10 гигабайт;

e) USB порт;

f) Клавиатура – 101 клавиша, поддерживающая русский и латинский языки;

g) Манипулятор типа «мышь»;

h) Доступ к информационно-телекоммуникационной сети «Интернет» с шириной канала не менее 512 кб/с;

i) Одна из нижеуказанных лицензионных операционных систем:

- Windows 8.1;
- Windows 7 x86 и x64;
- Windows 10;

j) Браузер Microsoft Internet Explorer версии 7.0, 8.0, 9.0, 10.0, 11.0;

k) Один из продуктов компании Adobe или аналогичный программный продукт для чтения файлов формата .PDF;

l) Права администратора АРМ Клиента на момент первичного входа, первичной установки программного обеспечения, обновления программного обеспечения Системы ДБО;

m) Отсутствие на АРМ Клиента иного крипто-шифрующего программного обеспечения.

Приложение 2 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ИСПОЛЬЗУЕМЫХ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

1. Электронные документы, направляемые Клиентом в Банк с использованием системы дистанционного банковского обслуживания:

a) Электронные платежные документы:
- —платежные поручения,
- —валютные переводы,
- —поручения на покупку иностранной валюты за валюту Российской Федерации,
- —поручения на продажу иностранной валюты за валюту Российской Федерации,
- —поручения на совершение конверсионной операции,
- —распоряжения на списание средств с транзитного валютного счета (распоряжения на перечисление средств без осуществления продажи иностранной валюты);

b) Электронные служебно-информационные документы:
- —контракты для постановки на учет;
- —кредитные договоры для постановки на учет,
- —зачвление об изменении сведений о ктнтракте (кредитном договоре),
- —заявление о снятии с учета контракта (кредитного договора),
- —сведения о валютных операциях,
- —справки о подтверждающих документах,
- —запросы на отзыв документа,
- —произвольные документы в Банк (иные документы или письма, составленные в произвольной форме, в том числе договоры и иные документы по проводимым операциям, представляемые по запросу Банка; сведения о выгодоприобретателях по проводимым операциям и т.п.).

2. Электронные служебно-информационные документы, получаемые Клиентом из Банка с использованием системы дистанционного банковского обслуживания:
- —выписки, содержащие информацию о движении средств по счетам;
- —иные документы произвольного формата.

3. Входящие и исходящие электронные служебно-информационные документы о конечном статусе обработки электронных документов («ЭП не верна», «Не принят», «Исполнен», «Удален», «Отозван» и другие).

Приложение 3 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АРМ КЛИЕНТА

РАЗДЕЛ I (ТРЕБОВАНИЯ)

Размещение АРМ:

1. Размещение, специальное оборудование, охрана и организация режима помещений, в которых расположены АРМ и хранятся носители ключевой информации, должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

2. Помещения, предназначенные для размещения АРМ и хранения носителей ключевой информации, должны быть оборудованы прочными дверьми, замками повышенной секретности и сигнализацией. Окна помещений, расположенных на первых или последних этажах зданий, а также находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, должны быть оборудованы решетками и/или сигнализацией.

Защита АРМ и закрытых ключей ЭП от несанкционированного доступа:

1. Клиентом должны быть разработаны нормативные документы, регламентирующие правила хранения, доступа и использования закрытых ключей ЭП.

2. Клиент, эксплуатирующий АРМ, должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства АРМ, изменение их состава, появление на АРМ и в системе ДБО вредоносных программ, а также программ, направленных на разрушение или модификацию программного обеспечения системы ДБО, ЭД, либо на перехват паролей, закрытых ключей ЭП и другой конфиденциальной информации.

3. На АРМ должен быть реализован комплекс мер и средств защиты от угроз информационно-телекоммуникационной сети «Интернет», обеспечивающий защиту данных от несанкционированного доступа. Клиент, эксплуатирующий АРМ, должен использовать антивирусное программное обеспечение и своевременно осуществлять его обновление, а также обновления системы дистанционного банковского обслуживания, операционной системы и web-браузеров.

4. Запрещается установка на АРМ Клиента программных средств, не предназначенных для выполнения служебных обязанностей абонентов/операторов Клиента, допущенных к работе на АРМ.

5. Носители ключевой информации должны находиться на поэкземплярном учете в специально выделенных для этих целей журналах.

6. Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

7. Брандмауэр АРМ Клиента необходимо настроить исключительно на доступ к WEB-сайту Системы ДБО.

8. При выявлении признаков нарушения информационной безопасности АРМ Клиента последний должен остановить его эксплуатацию.

Меры, необходимые для обеспечения безопасности электронных подписей и их проверки

Для хранения электронных ключей и средств ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).
Использовать автоматизированное рабочее место (АРМ) с установленными средствами ЭП необходимо в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.
При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка операционной системы (ОС)

без запроса пароля. При этом должны быть реализованы дополнительные организационно - режимные меры, исключающие несанкционированный доступ к этим АРМ.
Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ с установленными средствами ЭП.
Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами ЭП.
Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
Администрирование должно осуществляться доверенными лицами.
Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов.
После получения электронного ключа в Удостоверяющем центре рекомендуется произвести смену стандартного пин-кода электронного ключа на свой собственный. Длина пароля должна быть не менее 6 символов.
В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей электронной подписи, к которым он имел доступ.
Хранение носителей ключевой информации допускается в хранилище, используемом совместно с другими сотрудниками, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца носителей ключевой информации и исключающей возможность негласного доступа к ним посторонних лиц.
Запрещается передавать носители ключевой информации другим лицам, выводить сертификаты ключей ЭП на дисплей или принтер, оставлять носители ключевой информации без присмотра, а также записывать на носитель ключевой информации постороннюю информацию.

Требования к абонентам/операторам Клиента:

1. Сотрудники, допущенные к работе на АРМ, назначаются приказом и должны иметь утвержденные должностные инструкции.

2. Непосредственная работа сотрудников на АРМ возможна только после прохождения обучения и проверки знания ими правил эксплуатации АРМ.

3. Каждый сотрудник, имеющий доступ к носителям ключевой информации, паролям и другой конфиденциальной информации, должен быть проинформирован об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства о неразглашении конфиденциальной информации.

4. Храните ключи только на предоставленном Банком съемном информационном носителе eToken PRO (Java). Хранение носителей ключевой информации должно быть организовано в месте, недоступном для посторонних лиц. Установка носителей ключевой информации на АРМ допускается только непосредственно на время работы с Системой ДБО; после окончания сеанса работы в Системе ДБО ключи должны быть извлечены и помещены в недоступное для посторонних лиц место.

5. Для контроля доступа к носителю ключевой информации в обязательном порядке сменить первичный пароль носителя ключевой информации при первом входе в Систему ДБО. Не сообщайте никому пароль для доступа к носителю ключевой информации, в том числе сотрудникам Банка или сотрудникам Вашей организации.

6. Запрещено работать с Системой ДБО с не доверенных компьютеров (интернет-кафе и т.п.), так как это существенно увеличивает риск хищения Ваших учетных и ключевых данных.

7. После окончания работы в Системе ДБО обязательно корректно завершите работу (выйдите из Системы ДБО с использованием кнопки «Выход») и/или закройте используемый web-браузер. Извлеките из компьютера носитель ключевой информации.

8. Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на АРМ. Действие вирусов может быть направлено на перехват Вашей ключевой и/или парольной информации и передаче её третьим лицам.

9. Установите и настройте персональный брандмауэр (Firewall) на АРМ. Это позволит Вам запретить несанкционированный удаленный доступ к АРМ из информационно-телекоммуникационной сети

«Интернет» и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа.

10. Используйте на АРМ только лицензионное программное обеспечение. Регулярно устанавливайте обновления для операционной системы и web-браузера.

11. Права пользователя, работающего с Системой ДБО, на АРМ должны быть максимально ограниченными (наличие у абонента/оператора Клиента администраторских прав на АРМ запрещено, кроме случаев первичного входа, первичной установки программного обеспечения, обновления программного обеспечения Системы ДБО).

Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи:

- обеспечить конфиденциальность ключей электронных подписей;
- применять для формирования электронной подписи только действующий ключ электронной подписи;
- не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;
- не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия, которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;
- обеспечить сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;
- обеспечить сохранение в тайне пин-кодов для доступа к электронным ключам и средствам ЭП;
- обеспечить соответствующие условий хранения электронных ключей, исключающих возможность доступа к ним посторонних лиц, несанкционированного использования или копирования средств ЭП;

1. Порядок применения средств квалифицированной электронной подписи

Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи, размещенной на официальном сайте Удостоверяющего центра ООО «Айтиком» https://uc-itcom.ru или на сайте производителя.

Для предотвращения заражения компьютера с установленными средствами квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского. программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

В помещениях владельцев средств квалифицированной электронной подписи для хранения выданных им носителей ключей электронной подписи. эксплуатационной и технической документации, инсталлирующих средства квалифицированной электронной подписи. необходимо иметь достаточное число надежно запираемых шкафов (ящиков. хранилищ) индивидуального пользования. оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих владельцев средств квалифицированной электронной подписи.

Заявителем Удостоверяющего центра соответствующими приказами должны быть разработаны нормативные документы. регламентирующие вопросы безопасности информации и эксплуатации этих средств; средства квалифицированной ЭП и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.

Риски использования электронной подписи

При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

- риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу;
- риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом;
- риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;
- риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение;
- риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избегания помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

Иные ограничения:

1. В случае если Клиент активирует фильтрацию абонентов/операторов Клиента по статическому(им) IP-адресу(ам) в целях обеспечения повышенного уровня безопасности операций в Системе ДБО, доступ абонентов/операторов Клиента к Системе ДБО может быть предоставлен Банком исключительно с согласованного(ых) Сторонами IP-адреса(ов). В указанном выше случае доступ абонентов/операторов Клиента к Системе ДБО с иных IP-адресов (помимо согласованных Сторонами) невозможен.

РАЗДЕЛ II (РЕКОМЕНДАЦИИ)

Рекомендации, направленные на обеспечение повышенного уровня безопасности при использовании Системы ДБО:

1. На АРМ Клиента не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в Системе ДБО.

2. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи (мобильные и стационарные телефоны, WEB-сайт, обычная и электронная почта и т.п.), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.

3. Клиенту рекомендуется использовать предоставляемую Банком возможность фильтрации абонентов/операторов Клиента по статическому(им) IP-адресу(ам) (следует отметить соответствующее поле в разделе 4 Заявления на подключение (Приложение 4 к Условиям) или в разделе 4 Уведомления об изменении параметров подключения (Приложение 5 к Условиям).

4. SMS уведомление.

Приложение 4 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ» от «____» _____ 20__ г.

_____

(полное наименование Клиента)

_____

(сокращенное наименование Клиента)

_____

(наименование Клиента на иностранном языке)

_____

(адрес места нахождения Клиента)

_____

(адрес места нахождения Клиента на иностранном языке)

ИНН/КИО: _____

в лице _____, действующего на основании _____, и в соответствии с условиями Договора № ____ о предоставлении услуги «Дистанционное банковское обслуживание» от _____20__г., в целях осуществления электронного документооборота с Банком просит:

1. Подключить к услуге «Дистанционное банковское обслуживание» и предоставить программное обеспечение, необходимое для установки Системы ДБО:

□ силами Банка

желаемый срок установки «___» ___ 20__ г. адрес установки: _____

□ силами Клиента

желаемый срок получения пакета, упомянутого в п. 3.6 Условий «___» _____ 20__ г.

2. Подключить к Системе дистанционного банковского обслуживания счета, открытые в рамках договора расчетно-кассового обслуживания № ____ от _____

3. Изготовить сертификаты ключа проверки электронной подписи / простую электронную подпись для следующих абонентов/операторов:*

№ п/п	Фамилия, имя, отчество (полностью)[1]	Срок полномочий	Право подписи	Технологический ключ
1				

4. Также просим Вас[2]:

	АКТИВИРОВАТЬ в Системе ДБО фильтрацию указанных выше в пункте 3 абонентов/операторов по статическому(им) IP-адресу (ам) в целях обеспечения повышенного уровня безопасности операций в Системе ДБО. Об ограничениях в использовании Системы ДБО извещены.		**НЕ АКТИВИРОВАТЬ** в Системе ДБО фильтрацию абонентов/операторов по статическому(им) IP-адресу(ам). О повышен ных рисках, связанных с использованием Системы ДБО осведомлены.
	информация о соответствующем(их) статическом(их) IP-адресе(ах) и абонентах/операторах: **АКТИВИРОВАТЬ** в Системе ДБО направление Банком sms-сообщений в целях подтверждения платежей в соответствии с подп. «g» п. 3.1 Договора		**НЕ АКТИВИРОВАТЬ** в Системе ДБО направление Банком sms-сообщений в целях подтверждения платежей в соответствии с подп. «g» п. 3.1 Договора

5. ***Адрес электронной почты, предназначенный для информирования Банком Клиента согласно подп. «b» п. 3.1 Договора:*** **_____.**

Телефонный номер, предназначенный для информирования Банком Клиента согласно подп. «c» п. 3.1 Договора:
+7_____.

Телефонный номер, предназначенный для информирования Банком Клиента согласно подп. «g» п. 3.1 Договора:
+7_____.

Контактное лицо / _____
(должность, ФИО, телефон, email)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)
М.П. /

Заполняется сотрудником Банка

Заявление на подключение к услуге «Дистанционное банковское обслуживание» получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) (подпись) (фамилия и инициалы)

* В полях, определяющих права абонентов/операторов системы ДБО, проставить символ X или V.

[1] Лица, обладающие правом подписи, должны быть указаны в карточке с образцами подписей и оттиска печати Клиента, имеющейся в распоряжении Банка. Указанные лица, а также оператор Системы ДБО должны обладать документальным подтверждением их полномочий на право использования ключей электронной подписи. Информация о сочетании подписей лиц, уполномоченных на распоряжение денежными средствами, принимается на основании действующего Соглашения о сочетании подписей. Срок полномочий указанных лиц должен соответствовать сроку полномочий, указанному в карточке с образцами подписей и оттиска печати Клиента.

[2] Проставить символ X или V в соответствующем поле. / Проставить символ X или V в соответствующем поле.

Приложение 5 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

УВЕДОМЛЕНИЕ
ОБ ИЗМЕНЕНИИ ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ К УСЛУГЕ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»

от «____» _____ 20__ г.

_____

_____

(полное наименование Клиента)

_____

(сокращенное наименование Клиента)

_____

_____

ИНН/КИО: _____

в лице _____, действующего на основании _____, и в соответствии с условиями Договора № ____ о предоставлении услуги «Дистанционное банковское обслуживание» от «___» _____ 20__г., в целях осуществления электронного документооборота с Банком просит:

1. Изготовить сертификаты ключа проверки электронной подписи/ простую электронную подпись для следующих абонентов/операторов:

№ п/п	Фамилия, имя, отчество[1] (полностью)	Срок полномочий	Право подписи	Право единственной подписи /	Право технологической подписи	Номер(а) счета(ов)
1						

2. Установить права (изменить права) для следующих абонентов/операторов, владельцев ключей электронной подписи:

№ п/п	Фамилия, имя, отчество[2] (полностью)	Срок полномочий	Право подписи	Право единственной подписи	Право технологической подписи	Номер(а) счета(ов)
1						

3. Отозвать сертификаты ключа проверки электронной подписи/ простую электронную подпись, принадлежащие следующим абонентам/операторам:

№ п/п	Фамилия, имя, отчество (полностью)	Серийный номер Сертификата ключа ЭП	Причина отзыва Сертификата ключа ЭП
1			

4. Также просим Вас[3]:

☐ **АКТИВИРОВАТЬ** в Системе ДБО фильтрацию указанных выше в пункте 3 абонентов/операторов по статическому(им) IP-адресу (ам) в целях обеспечения повышенного уровня безопасности операций в Системе ДБО. Об ограничениях в использовании Системы ДБО извещены.

информация о соответствующем(их) статическом(их) IP-адресе(ах) и абонентах/операторах:

☐ **НЕ АКТИВИРОВАТЬ** в Системе ДБО фильтрацию абонентов/операторов по статическому(им) IP-адресу(ам). О повышен ных рисках, связанных с использованием Системы ДБО осведомлены.

☐ **АКТИВИРОВАТЬ** в Системе ДБО направление Банком sms-сообщений в целях подтверждения платежей в соответствии с подп. «g» п. 3.1 Договора

☐ **НЕ АКТИВИРОВАТЬ** в Системе ДБО направление Банком sms-сообщений в целях подтверждения платежей в соответствии с подп. «g» п. 3.1 Договора

Контактное лицо _____
(должность, ФИО, телефон, email)

_____ _____ _____
(наименование должности руководителя) *(подпись)* *(фамилия и инициалы)*

Заполняется сотрудником Банка

Уведомление об изменении параметров подключения к услуге «Дистанционное банковское обслуживание» получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) *(подпись)* *(фамилия и инициалы)*

[1] Лица, обладающие правом подписи, должны быть указаны в карточке с образцами подписей и оттиска печати Клиента, имеющейся в распоряжении Банка. Указанные лица, а также оператор Системы ДБО должны обладать документальным подтверждением их полномочий на право использования ключей электронной подписи. Информация о сочетании подписей лиц, уполномоченных на распоряжение денежными средствами, принимается на основании действующего Соглашения о сочетании подписей. Срок полномочий указанных лиц должен соответствовать сроку полномочий, указанному в карточке с образцами подписей и оттиска печати Клиента.

[2] Аналогично сноске 1

[3] Проставить символ X или V в соответствующем поле.

Приложение 6 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

АКТ
ПРИЕМА-ПЕРЕДАЧИ НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

г. Москва

Настоящий Акт составлен в том, что «Коммерческий Индо Банк» ООО (далее – Банк), в лице _____, действующего на основании _____, передал,
а _____, (далее – Клиент), в лице _____, действующего на основании _____, принял следующие материалы:

- 1 (Один) экземпляр запечатанного именного конверта для каждого из указанных ниже абонентов/операторов Клиента, содержащий: a) карточку абонента/оператора Клиента; b) реквизиты первичного персонального пароля абонента/оператора Клиента (в том числе первичный пароль носителя ключевой информации);
- 1 (Один) экземпляр информационного носителя USB-ключ ruToken PRO (Java) для каждого из указанных ниже абонентов/операторов Клиента с правом использования (лицензией) на средство криптографической защиты информации;
- 2 (Два) экземпляра акта о вводе в действие услуги «Дистанционное банковское обслуживание»;

№ п/п	Фамилия, имя, отчество абонента/оператора Клиента (полностью)	Основание для выдачи ключа ЭП	Серийный номер носителя USB-ключ ruToken PRO (Java)
1			

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу, один из которых передается Клиенту, а другой – Банку.

БАНК:
«Коммерческий Индо Банк» ООО
Место нахождения: 109147, г. Москва, ул. Марксистская, д. 16

КЛИЕНТ:
_____
_____
_____
_____
_____
_____
_____

От имени Банка:

От имени Клиент:

Приложение 7 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

АКТ О ВВОДЕ В ДЕЙСТВИЕ УСЛУГИ «ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ»

г. Москва «_____» _____ 20__ г.

Мы, нижеподписавшиеся, представитель Банка _____, действующий на основании _____, с одной стороны, и представитель Клиента _____, действующий на основании _____, с другой стороны, составили настоящий Акт о том, что согласно Договору № ____ от «_____» _____ 20__ г. о предоставлении услуги «Дистанционное банковское обслуживание» полностью выполнены следующие работы:

1. Банком / Клиентом (*нужное подчеркнуть*) на АРМ Клиента проведена установка программного обеспечения Системы ДБО и программного средства криптографической защиты информации.
2. Представитель Банка провел обучение абонентов/операторов Клиента приемам и методам работы с Системой ДБО (методике проверки достоверности ЭП, смены ключей ЭП и т.д.) и администратора АРМ Клиента (в случае установки Системы ДБО силами Банка).
3. Проведена настройка взаимодействия АРМ Клиента с Банком.
4. Проверена работоспособность ПО АРМ Клиента.
5. Проведен сеанс связи с Банком. В Банк передано и из Банка получено тестовое сообщение.
6. Абоненты/операторы Клиента, ознакомлены и обязуются выполнять требования по обеспечению информационной безопасности АРМ Клиента, указанные в Разделе I Приложения 3 к Условиям.
7. АРМ Клиента готово к вводу в эксплуатацию.

Дополнительная информация:
_____
_____

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу, один из которых передается Клиенту, а другой – Банку.

БАНК:
«Коммерческий Индо Банк» ООО
Место нахождения: 109147, г. Москва, ул. Марксистская, д. 16

КЛИЕНТ:
_____
_____
_____
_____
_____
_____
_____
_____

От имени Банка:

От имени Клиента:

Приложение 8 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

ЗАЯВЛЕНИЕ
НА ВЫПОЛНЕНИЕ РАБОТ ПО СОПРОВОЖДЕНИЮ СИСТЕМЫ ДБО
от «____» _____ 20__ г.

(полное наименование Клиента)

(сокращенное наименование Клиента, если имеется)

(наименование Клиента на иностранном языке, если имеется)

(адрес места нахождения Клиента)

_____
_____
(адрес места нахождения Клиента на иностранном языке, если имеется

ИНН/КИО: _____ ОКПО: _____ КПП: _____ резидент РФ/нерезидент РФ (ненужное зачеркнуть)
ОГРН: _____. Дата государственной регистрации: «____» _____ _____ г.

в лице _____, действующего на основании _____, и в соответствии с условиями Договора № ___ о предоставлении услуги «Дистанционное банковское обслуживание» от «___» _____ 20__г., в целях осуществления электронного документооборота с Банком просит организовать выезд специалиста Банка по адресу:
_____
(адрес проведения работ)
для проведения следующих работ: _____
_____
_____

Желательная дата выезда специалиста Банка «____» _____ 20__ г.

Контактное лицо

_____
(должность, ФИО, телефон, email)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)

Заполняется сотрудником Банка
Заявление на выполнение работ по сопровождению системы ДБО получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) (подпись) (фамилия и инициалы)

Приложение 9 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

АКТ ПРИЕМА-СДАЧИ РАБОТ

г. Москва «_____» _____ 20__ г.

Мы, нижеподписавшиеся, представитель Банка _____, действующий на основании _____, с одной стороны и представитель Клиента _____, действующий на основании _____, с другой стороны, составили настоящий Акт о том, что согласно Договору № ___ от «____» _____ 20__г. о предоставлении услуги «Дистанционное банковское обслуживание» в период: с «____» _____ 20__ г. по «____» _____ 20__ г., Банком на территории Клиента были надлежащим образом выполнены следующие работы:

_____
_____
_____
_____
_____

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу, один из которых передается Клиенту, а другой – Банку.

БАНК:
«Коммерческий Индо Банк» ООО
Место нахождения: 109147, г. Москва, ул. Марксистская, д. 16

КЛИЕНТ
_____
_____
_____
_____
_____
_____
_____
_____
_____

От имени Банка

От имени Клиента

Приложение 10 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

ДОВЕРЕННОСТЬ НА ПОЛУЧЕНИЕ ДОКУМЕНТОВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАБОТЫ С СЕРТИФИКАТАМИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Настоящая доверенность исполнена в городе _____, Российская Федерация, _____ _____ две тысячи _____ года,

_____,
(полное наименование Клиента)

государственный регистрационный номер _____, ИНН/КИО _____, имеющего место нахождения по адресу: _____, г. _____, ул. _____, д. _____, далее – Клиент, в лице _____, действующего на основании
(должность, фамилия, имя, отчество)

_____, уполномочивает: _____

_____
(должность, фамилия, имя, отчество уполномоченного лица)

_____
(паспортные данные уполномоченного лица: серия, номер, наименование органа, выдавшего паспорт, дата выдачи, телефон для связи)

на выполнение следующих действий от имени и в интересах Клиента в рамках подписанного между «Коммерческим Индо Банком» ООО и Клиентом Договора № ___ от «____» _____ 20___ г. о предоставлении услуги «Дистанционное банковское обслуживание»:

- получение запечатанного конверта на каждого абонента/оператора Клиента, содержащего: конверт (1 (Один) экземпляр на каждого абонента/оператора Клиента), содержащий: 1) карточку абонента/оператора Системы ДБО; 2) реквизиты первичного персонального пароля (в том числе первичный пароль носителя ключевой информации);
- носитель ключевой информации абонента/оператора Клиента – 1 (Один) экземпляр на каждого абонента/оператора Клиента;
- Акт о вводе в действие услуги «Дистанционное банковское обслуживание» – 2 (Два) экземпляра;
- получение запечатанного пакета, содержащего все или часть вышеуказанных документов/материалов. ***Право вскрытия указанного пакета не предоставляется;***
- подписание Акта приема-передачи носителей ключевой информации, программного обеспечения и средств криптографической защиты информации.

Настоящая доверенность действительна до «_____» _____ 20__ года.

Подпись _____ удостоверяю
(наименование должности и ФИО уполномоченного лица) (подпись)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)

Приложение 11 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

ДОВЕРЕННОСТЬ НА ПОДПИСАНИЕ СЕРТИФИКАТА КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

Настоящая доверенность исполнена в городе _____, Российская Федерация, _____ _____ две тысячи _____ года,

_____,
(полное наименование Клиента)

государственный регистрационный номер _____, ИНН/КИО _____, имеющего место нахождения по адресу: _____, г. _____, ул. _____, д. _____, далее – Клиент, в лице

_____,
(должность, фамилия, имя, отчество)

действующего на основании _____, уполномочивает:

_____
(должность, фамилия, имя, отчество уполномоченного лица)

_____

_____
(паспортные данные уполномоченного лица: серия, номер, наименование органа, выдавшего паспорт, дата выдачи, телефон для связи)

на выполнение следующих действий от имени и в интересах Клиента в рамках подписанного между «Коммерческим Индо Банком» ООО и Клиентом Договора № ___ от «____» _____ 20__ г. о предоставлении услуги «Дистанционное банковское обслуживание»:

на подписание собственноручной подписью от имени и в интересах Клиента Сертификатов ключей электронной цифровой подписи в форме документов на бумажном носителе, для последующего их использования в системе дистанционного банковского обслуживания в рамках подписанного между «Коммерческим Индо Банком» ООО и Клиентом Договора № ___ от «____» _____ 20__ г. о предоставлении услуги «Дистанционное банковское обслуживание».

Настоящая доверенность действительна до «_____» _____ 20__ года.

Подпись _____ удостоверяю /
(наименование должности и ФИО уполномоченного лица) (подпись)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)

Приложение 12 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

УВЕДОМЛЕНИЕ
О КОМПРОМЕТАЦИИ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ
от «____» _____ 20__ г.

_____
(полное наименование Клиента)

_____
(сокращенное наименование Клиента, если имеется)

_____
(наименование Клиента на иностранном языке, если имеется)

_____
(адрес места нахождения Клиента)

ИНН/КИО: _____ ОКПО: __ _____ КПП: _____ резидент РФ/нерезидент РФ (ненужное зачеркнуть)
ОГРН: _____. Дата государственной регистрации: «____» _____ _____ г.

в лице _____ ___ _____, действующего на основании _____, и в соответствии с условиями Договора № _____ о предоставлении услуги «Дистанционное банковское обслуживание» от «___» _____ _ 20__г., уведомляет о компрометации ключей электронной цифровой подписи, принадлежащих следующим абонентам/операторам:

№ п/п / # seq.	Фамилия, имя, отчество абонента/оператора Клиента (полностью)	Серийный номер Сертификата ключа ЭП	Причина компрометации
1			
2			
…			

Контактное лицо
_____
(должность, ФИО, телефон, email)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)

Заполняется сотрудником Банка
Уведомление о компрометации ключа ЭП получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) (подпись) (фамилия и инициалы)

Приложение 13 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

КАРТОЧКА АБОНЕНТА/ОПЕРАТОРА СИСТЕМЫ ДБО

Ф.И.О. абонента/оператора: [pUserName]

Логин: / Login: [pLogin]
Идентификатор пароля: / Password identifier: [pPassID]

Адреса доступа к сервисам: / Addresses of access to services:
Интернет-Клиент (Платеж.) / Internet-Client (Payment)
cbil-moscow.ru / cbil-moscow.ru

Максимальное количество сессий: [pMaxSessionCount] / Maximum number of sessions: [pMaxSessionCount]
Требуется смена пароля при первом входе: [pIsChangePass] / Change of the password is required at the first login: [pIsChangePass]

Протокол защиты канала: [pProtocol] / Channel protection protocol: [pProtocol]
Фильтрация по внутренним IP-адресам ([pIntIPEnabled]): [pIntIPFilter] / Filtration by internal IP addresses ([pIntIPEnabled]): [pIntIPFilter]
Фильтрация по внешним IP-адресам (шлюзам) ([pExtIPEnabled]): [pExtIPFilter] / Filtration by external IP addresses (gateways) ([pExtIPEnabled]): [pExtIPFilter]

[EndSection]
[BeginSection:CustomersHeader]

Перечень организаций: / List of organizations:
[EndSection]
[BeginSection:CustomersBody]

ID Орг. / Org. ID:	Название организации / Name of the organization	Название подразделения банка / Name of the bank's branch	Сервис / Service
[pCustID]	**[pCustName]**	**[$ParseText(pBranchName)]**	**[pService]**

[EndSection][BeginSection:CustomersFooter]
[EndSection][BeginSection:SignsHeader]

Реквизиты ЭП: / DS details:

Название криптопрофиля / Encryption profile	АРМ (ID Организаций) / AWS (Organization ID)	Право подписи / Right of signature
[pProfileName]	[pClientID] [pCustID]	[pSignDocRights]

[EndSection]
[BeginSection:CertificateHeader]
Реквизиты Сертификатов:

Название криптопрофиля / Encryption profile	Идентификатор (UID) ключа / Key identifier (UID)	Тип ключа[EndSection][BeginSection:CertificateBody] / Key type[EndSection][BeginSection:CertificateBody]
[pProfileName]	[pCryptoUID]	[pType][EndSection][BeginSection:CertificateFooter]

[EndSection]
[BeginSection:Footer]

Дата и время вывода на печать: [pCurrentDateTime] / Printing date and time: [pCurrentDateTime]
Подготовил и распечатал: _____ _____
(подпись сотрудника Банка) *(ФИО и должность сотрудника Банка)* / Prepared and printed by:
_____ _____
(signature of the Bank's employee) *(name and title of the Bank's employee)*

[EndSection]

Приложение № 14 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

Заявка на сертификат №_____
Генеральному директору ООО «Айтиком» Е.Н. Мельниковой

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки электронной подписи

1. я индивидуальный предприниматель **_____(ФИО)** (основание полномочий - свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя, серия ___ номер _____, дата выдачи свидетельства ___.___._____ прошу зарегистрировать и сформировать ключ электронной подписи, записать сформированный ключ электронной подписи на ключевой носитель и изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «Айтиком» в соответствии с указанными в настоящем заявлении данными:

	Ключ №1
Наименование организации (organizationName)	
Общее имя (CommonName)	**ФИО**
Улица, дом (streetAddress)	
Город (localityName)	**Город**
Область, край (stateOrProvinceName)	**Область**
Страна (countryName)	**RU**
Электронная почта (E-Mail (E))	**Почта**
ИНН (INN)	**ИНН**
ОГРН организации (OGRN)	
ОГРНИП организации (OGRNIP)	**ОГРНИП**
Неструктурированное имя (unstructuredName)	
Ограничения использования квалифицированного сертификата	
Информация о владельце квалифицированного сертификата (по требованию заявителя)	
Подразделение организации (organizationUnitName)	
Должность (title)	
Фамилия (surname)	**Фамилия**
Имя и отчество (givenName)	**Имя и отчество**
Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)	**СНИЛС**

Ключ №1 выпускается для_____
Ключевая фраза, использующаяся для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов: нет
2. Я, индивидуальный предприниматель, **ФИО**, в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту УЦ ООО «Айтиком» по выпуску квалифицированных сертификатов ключей проверки электронной подписи от 18.03.2019 года, условия которого определены ООО «Айтиком» и опубликованы на сайте Удостоверяющего центра ООО «Айтиком» по адресу http://uc-itcom.ru/files/reglamentITCOM.pdf. Руководство по обеспечению безопасности использования ЭП и средств ЭП получил в печатном виде и ознакомился.
С регламентом Удостоверяющего центра по выпуску квалифицированных сертификатов ключа проверки электронной подписи и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.
3. Я, **ФИО** паспорт серии _____ № _____, выдан _____(дата выдачи и кем выдан паспорт) , код подразделения _____, дата рождения _____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», с целью получения квалифицированного сертификата ключа проверки электронной подписи и осуществления действий, предусмотренных регламентом Удостоверяющего центра ООО «АйтиКом», даю согласие ООО «АйтиКом» (далее – Удостоверяющий центр), расположенному по адресу: 127083, г. Москва, ул. Верхняя Масловка, д.20, стр.1, пом.3, ком.10, а также ООО «ИТК», расположенному по адресу: 350051, Краснодарский край, Краснодар, ул. Дальняя, д. 39/3, пом. 140 (лицо, осуществляющее обработку персональных данных по поручению ООО «АйтиКом») на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных: фамилия, имя, отчество, пол, дата и место рождения; адрес места жительства, реквизиты основного документа, удостоверяющего личность (серия, номер, дата выдачи, орган, осуществившей выдачу, код подразделения); место работы, должность; фотоизображение, контактная информация (электронная почта, телефон), идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), фотокопии основного документа, удостоверяющего личность, страхового свидетельства обязательного пенсионного страхования (СНИЛС), собственноручная подпись, иные персональные данные, необходимые для выпуска квалифицированного сертификата ключа проверки электронной подписи, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу) обезличивание, блокирование, уничтожение, а также осуществление любых иных действий, предусмотренных нормативными правовыми актами в области электронной подписи. Я соглашаюсь с включением моих персональных данных в общедоступные источники, которыми являются сертификат ключа проверки электронной подписи, реестр сертификатов ключей проверки электронной подписи; а также на передачу моих персональных данных в единую систему идентификации и аутентификации в объеме, необходимом для регистрации в системе идентификации и аутентификации в соответствии с требованиями действующего законодательства. Подтверждаю, что обладаю правами доступа, достаточными для чтения и отправки электронных сообщений с помощью ящика электронной почты rasul_shalabaev@mail.ru и даю согласие на использование этого ящика для информационного взаимодействия с ООО «Айтиком». Настоящее согласие на обработку персональных данных действует с момента подписания бессрочно и может быть отозвано мной в порядке, установленном Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 года №152-ФЗ, в любое время на основании моего письменного заявления в произвольной форме.
4. Я, **ФИО**, подтверждаю достоверность данных, указанных в настоящем Заявлении.
Подписи:
Пользователь Удостоверяющего центра_____ФИО
___.___.20__

Приложение №15 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

Заявка на сертификат №_____
Генеральному директору ООО «Айтиком» Е.Н. Мельниковой

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки электронной подписи

1. я **_____,** генеральный директор, действующий(ая) от имени ООО "_____" (основание полномочий - устав), прошу зарегистрировать и сформировать ключ электронной подписи, записать сформированный ключ электронной подписи на ключевой носитель и изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «АйтиКом» в соответствии с указанными в настоящем заявлении данными:

	Ключ №1
Наименование организации (organizationName)	
Общее имя (CommonName)	
Улица, дом (streetAddress)	
Город (localityName)	
Область, край (stateOrProvinceName)	
Страна (countryName)	
Электронная почта (E-Mail (E))	
ИНН (INN)	
ОГРН организации (OGRN)	
ОГРНИП организации (OGRNIP)	
Неструктурированное имя (unstructuredName)	
Ограничения использования квалифицированного сертификата	
Информация о владельце квалифицированного сертификата (по требованию заявителя)	
Уполномоченный представитель:	
Подразделение организации (organizationUnitName)	**Руководство**
Должность (title)	**Генеральный директор**
Фамилия (surname)	
Имя и отчество (givenName)	
Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)	

Ключ №1 выпускается для_____
Ключевая фраза, использующаяся для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов: нет

2. Я, **_____,** действующий(ая) от имени ООО "_____", в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту УЦ ООО «АйтиКом» по выпуску квалифицированных сертификатов ключей проверки электронной подписи от 18.03.2019 года, условия которого определены ООО «АйтиКом» и опубликованы на сайте Удостоверяющего центра ООО «АйтиКом» по адресу https://uc-itcom.ru/files/reglamentITCOM.pdf. Руководство по обеспечению безопасности использования ЭП и средств ЭП получил в печатном виде и ознакомился.
С регламентом Удостоверяющего центра по выпуску квалифицированных сертификатов ключа проверки электронной подписи и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.

3. Я, _____ паспорт серии ____ № _____, выдан __.__.____ (когда) _____ (кем) код подразделения ___-___, дата рождения __.__.____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», с целью получения квалифицированного сертификата ключа проверки электронной подписи и осуществления действий, предусмотренных регламентом Удостоверяющего центра ООО «АйтиКом», даю согласие ООО «АйтиКом» (далее – Удостоверяющий центр), расположенному по адресу: г. Москва, ул. Верхняя Масловка, д.20, стр.1, пом.3, ком.10, а также ООО «ИТК», расположенному по адресу: 350051, Краснодарский край, Краснодар, ул. Дальняя, д. 39/3, пом. 140 (лицо, осуществляющее обработку персональных данных по поручению ООО «АйтиКом») на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных: фамилия, имя, отчество, пол, дата и место рождения; адрес места жительства, реквизиты основного документа, удостоверяющего личность (серия, номер, дата выдачи, орган, осуществившей выдачу, код подразделения); место работы, должность; фотоизображение, контактная информация (электронная почта, телефон), индикационный номер налогоплательщика, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), фотокопии основного документа, удостоверяющего личность, страхового свидетельства обязательного пенсионного страхования (СНИЛС), собственноручная подпись, иные персональные данные, необходимые для выпуска квалифицированного сертификата ключа проверки электронной подписи, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу) обезличивание, блокирование, уничтожение, а также осуществление любых иных действий, предусмотренных нормативными правовыми актами в области электронной подписи. Я соглашаюсь с включение моих персональных данных в общедоступные источники, которыми являются сертификат ключа проверки электронной подписи, реестр сертификатов ключей проверки электронной подписи; а также на передачу моих персональных данных в единую систему идентификации и аутентификации в объеме, необходимом для регистрации в системе идентификации и аутентификации в соответствии с требованиями действующего законодательства. Подтверждаю, что обладаю правами доступа, достаточными для чтения и отправки электронных сообщений с помощью ящика электронной почты ppppp@mail.ru и даю согласие на использование этого ящика для информационного взаимодействия с ООО «АйтиКом». Настоящее согласие на обработку персональных данных действует с момента подписания бессрочно и может быть отозвано мной в порядке, установленном Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 года №152-ФЗ, в любое время на основании моего письменного заявления в произвольной форме.

4. Я, **ФИО**, подтверждаю достоверность данных, указанных в настоящем Заявлении.

Подписи:

Пользователь Удостоверяющего центра_____ФИО
___.___.20___

Приложение №16 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

Заявка на сертификат №_____
Генеральному директору ООО «Айтиком» Е.Н. Мельниковой

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки электронной подписи

1. я **_____,** генеральный директор, действующий(ая) от имени ООО "_____" (основание полномочий - устав), прошу зарегистрировать и сформировать ключ электронной подписи, записать сформированный ключ электронной подписи на ключевой носитель и изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «АйтиКом» в соответствии с указанными в настоящем заявлении данными:

	Ключ №1
Наименование организации (organizationName)	
Общее имя (CommonName)	
Улица, дом (streetAddress)	
Город (localityName)	
Область, край (stateOrProvinceName)	
Страна (countryName)	
Электронная почта (E-Mail (E))	
ИНН (INN)	
ОГРН организации (OGRN)	
ОГРНИП организации (OGRNIP)	
Неструктурированное имя (unstructuredName)	
Ограничения использования квалифицированного сертификата	
Информация о владельце квалифицированного сертификата (по требованию заявителя)	
Уполномоченный представитель:	
Подразделение организации (organizationUnitName)	
Должность (title)	
Фамилия (surname)	
Имя и отчество (givenName)	
Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)	

Ключ №1 выпускается для_____
Ключевая фраза, использующаяся для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов: нет
2. Я, **_____,** действующий(ая) от имени ООО "_____", в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту УЦ ООО «АйтиКом» по выпуску квалифицированных сертификатов ключей проверки электронной подписи от 18.03.2019 года, условия которого определены ООО «АйтиКом» и опубликованы на сайте Удостоверяющего центра ООО «АйтиКом» по адресу https://uc-itcom.ru/files/reglamentITCOM.pdf. Руководство по обеспечению безопасности использования ЭП и средств ЭП получил в печатном виде и ознакомился.
С регламентом Удостоверяющего центра по выпуску квалифицированных сертификатов ключа проверки электронной подписи и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.
3. Я, _____ паспорт серии ____ № _____, выдан __.__.____ (когда) _____ (кем) код подразделения ___-___, дата рождения __.__.____, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», с целью получения квалифицированного сертификата ключа проверки электронной подписи и осуществления действий, предусмотренных регламентом Удостоверяющего центра ООО «АйтиКом», даю согласие ООО «АйтиКом» (далее – Удостоверяющий центр), расположенному по адресу: г. Москва, ул. Верхняя Масловка, д.20, стр.1, пом.3, ком.10, а также ООО «ИТК», расположенному по адресу: 350051, Краснодарский край, Краснодар, ул. Дальняя, д. 39/3, пом. 140 (лицо, осуществляющее обработку персональных данных по поручению ООО «АйтиКом») на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных: фамилия, имя, отчество, пол, дата и место рождения; адрес места жительства, реквизиты основного документа, удостоверяющего личность (серия, номер, дата выдачи, орган, осуществившей выдачу, код подразделения); место работы, должность; фотоизображение, контактная информация (электронная почта, телефон), индикационный номер налогоплательщика, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), фотокопии основного документа, удостоверяющего личность, страхового свидетельства обязательного пенсионного страхования (СНИЛС), собственноручная подпись, иные персональные данные, необходимые для выпуска квалифицированного сертификата ключа проверки электронной подписи, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу) обезличивание, блокирование, уничтожение, а также осуществление любых иных действий, предусмотренных нормативными правовыми актами в области электронной подписи. Я соглашаюсь с включение моих персональных данных в общедоступные источники, которыми являются сертификат ключа проверки электронной подписи, реестр сертификатов ключей проверки электронной подписи; а также на передачу моих персональных данных в единую систему идентификации и аутентификации в объеме, необходимом для регистрации в системе идентификации и аутентификации в соответствии с требованиями действующего законодательства. Подтверждаю, что обладаю правами доступа, достаточными для чтения и отправки электронных сообщений с помощью ящика электронной почты ppppp@mail.ru и даю согласие на использование этого ящика для информационного взаимодействия с ООО «АйтиКом». Настоящее согласие на обработку персональных данных действует с момента подписания бессрочно и может быть отозвано мной в порядке, установленном Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 года №152-ФЗ, в любое время на основании моего письменного заявления в произвольной форме.
4. Я, **ФИО**, подтверждаю достоверность данных, указанных в настоящем Заявлении.
5. Я, **ФИО**, подтверждаю, что _____**(ФИО Пользователя)**
Является уполномоченным представителем ООО «_____» и занимает должность _____;
Обладает полномочиями выступать в роли Пользователя Удостоверяющего центра;
Обладает правом использования квалифицированного сертификата ключа проверки электронной подписи с учётом указанных в нём ограничений;
Обладает правом расписываться и совершать все действия, связанные с выполнением данного поручения.
Подписи:
Пользователь Удостоверяющего центра _____ ФИО
Руководитель организации _____ФИО
___.___.20___

Приложение №17 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

Генеральному директору ООО «АйтиКом»
Мельниковой Е.Н.
129366, г Москва, ВН.ТЕР.Г. Муниципальный округ Алексеевский
ул. Ярославская, дом 13А, стр.1, пом. 6

Заявление
на аннулирование сертификата ключа проверки электронной подписи
(для юридических лиц и индивидуальных предпринимателей)

«_____» _____ 20_____ г.

_____

(наименование организации, включая организационно-правовую форму)

в лице _____
(должность, фамилия, имя, отчество)

действующего на основании _____

прошу аннулировать сертификат ключа проверки электронной подписи, в связи с

_____

Серийный номер	
Фамилия (surname (SN))	
Неструктурированное имя (unstructuredName (UN))	
Общее имя (commonName (CN))	
Адрес электронной почты (E-Mail (E))	
Наименование организации (organizationName (O))	
Наименование подразделения	
Город (localityName (L))	
Область (stateOrProvinceName (S))	
Страна/регион (countryName (C))	
СНИЛС (SNILS)	

Пользователь Удостоверяющего центра ООО «АйтиКом»

_____ _____
(Подпись) *(ФИО.)*

_____ _____ _____
(*Должность руководителя организации*) (*Подпись*) (*Ф.И.О.)*

М.П. «_____ » _____ 20_____ г.

Приложение 18 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

На бланке Клиента

ЗАЯВЛЕНИЕ НА УСТАНОВЛЕНИЕ ОГРАНИЧЕНИЙ ПО ПАРАМЕТРАМ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

_____

(полное наименование Клиента)

_____

(сокращенное наименование Клиента, если имеется)

_____

(наименование Клиента на иностранном языке, если имеется)

_____

(адрес места нахождения Клиента)

_____

(адрес места нахождения Клиента на иностранном языке, если имеется)

ИНН/КИО: _____ ОКПО: _____ КПП: _____ резидент РФ/нерезидент РФ (ненужное зачеркнуть)
ОГРН: _____ . Дата государственной регистрации: «____» _____ 20___ г.
в лице _____, действующего на основании _____, и
в соответствии с условиями Договора № ____ о предоставлении услуги «Дистанционное банковское обслуживание» от «____» _____ 20___г. (далее - Договор), в целях осуществления электронного документооборота с Банком просит установить ограничения по параметрам операций по следующим счетам:
счет № _____

счет № _____

счет № _____

№ п/п	*Поставить отметку X/Y*	*Типы ограничений по параметрам операций*
1		На максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени: _____ рублей (указывается максимальная сумма перевода денежных средств в валюте счета) _____ рублей (указывается максимальная сумма перевода денежных средств в валюте счета) за период времени _____ дней
2		На перечень возможных получателей денежных средств (указываются наименование и реквизиты получателей денежных средств) - - -
3		На временной период, в который могут быть совершены переводы денежных средств (указывается временной период приема распоряжений):
4		На географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение электронных сообщений[1] (указываются доверенные регионы):
5		На перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений[i] (указываются IP-адреса, с которых может осуществляться отправка распоряжений):
6		На перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств (указываются типы разрешенных распоряжений и услуг)

_____ _____ _____
(наименование должности руководителя) (подпись) (фамилия и инициалы)
М.П.

Заполняется сотрудником Банка
Заявление на установление ограничений по параметрам операций с использованием системы дистанционного банковского обслуживания получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) (подпись) (фамилия и инициалы)

Приложение №19 к Условиям предоставления услуги «Дистанционное банковское обслуживание»

Заявление на создание простой электронной подписи

Я **_____,** действующий(ая) от имени ООО "_____" на основании устава / доверенности № _____ от _____), прошу сформировать ключ простой электронной подписи в соответствии с указанными в настоящем заявлении данными:

	Наименование клиента Банка	
	ИНН клиента Банка	
	Фамилия, Имя, Отчество Уполномоченного лица	
	Должность Уполномоченного лица	
	TIN Уполномоченного лица	
	Серия и номер основного документа, удостоверяющего личность, кем и когда выдан	
	Электронная почта (E-Mail) Уполномоченного лица	
	Номер мобильного телефона	
	Адрес местонахождения	
	Слово или фраза, предназначенные для идентификации Оператора Удостоверяющего центра при обращении по телефону[1]	

Уполномоченное лицо _____ _____

(подпись) (инициалы, фамилия)

« ____ » _____ 20_ г.

Руководитель клиента Банка _____ _____

(подпись) (инициалы, фамилия)

М.П.

« ____ » _____ 20_ г.

[1] Поле не заполняется в заявлении на создание Сертификата Владельца Сертификата - юридического лица.