ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МУНИЦИПАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК им. СЕРГИЯ ЖИВАГО»

г. Рязань

УТВЕРЖДЕНО
приказом Председателя Правления
ООО «МКБ им. С. ЖИВАГО»
№ 119/1 от «31» июля 2013 г.
(изменения внесены приказами
от 09.03.2017 № 47, от 18.04.2018
№ 91)

Инв.№ 478

РЕГЛАМЕНТ
управления сертификатами ключей проверки электронной подписи в Системе Дистанционного Банковского Обслуживания ООО «МКБ им. С. ЖИВАГО»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МУНИЦИПАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК им. СЕРГИЯ ЖИВАГО» (далее – Банк), имеющее соответствующие лицензии на распространение и техническое обслуживание сертифицированных шифровальных криптографических средств, а также предоставление услуг в области шифрования информации, являющееся организатором системы электронного документооборота, выполняет прием, обработку и исполнение электронных документов клиентов (далее – Клиент), заключивших Договор о расчетном обслуживании с использованием системы дистанционного банковского обслуживания (далее – Договор) с Банком, предусматривающим возможность обмена электронными документами с использованием сертификатов ключей проверки электронной подписи.

1.2. Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим отношения в области использования электронных подписей при проведении расчетных операций по открытому Клиентом в Банке счету в электронной форме.

1.3. Настоящий Регламент определяет условия предоставления и правила пользования услугами Банка по управлению сертификатами ключей проверки электронной подписи в Системе ДБО, включая права, обязанности, ответственность Сторон, основные организационно-технические мероприятия, направленные на обеспечение работы по управлению сертификатами ключей проверки электронной подписи и является неотъемлемой частью Договора, заключенного Банком с Клиентом.

1.4. Уполномоченным структурным подразделением Банка, обеспечивающим управление сертификатами ключей проверки электронной подписи в Системе ДБО, является Отдел защиты информации.

1.5. Уполномоченное подразделение обеспечивает:

изготовление ключей электронной подписи Клиентов и формирование сертификатов ключей проверки электронной подписи;

ведение реестра сертификатов ключей проверки электронной подписи с установлением сроков действия сертификатов ключей проверки электронных подписей;

уникальность ключей проверки электронных подписей в реестре сертификатов;

хранение сертификатов ключей проверки электронной подписи Клиентов в форме электронных документов и выдачу сертификатов ключей проверки электронной подписи с информацией об их действии;

приостановление и возобновление действия сертификатов ключей проверки электронной подписи, а также их аннулирование;

взаимодействие с Клиентами при изготовлении ими своих ключей электронной подписи и запросов на сертификаты ключей проверки электронной подписи;

осуществление подтверждения подлинности электронной подписи в электронном документе;

проведение плановой и внеплановой замены ключей электронной подписи;

замену ключей электронной подписи в случае их компрометации;

иную связанную с использованием электронной подписи деятельность.

1.6. Банк и Клиент принимают к использованию для осуществления передачи электронных документов в Системе ДБО средства электронной подписи, соответствующие требованиям законодательства Российской Федерации.

1.7. В качестве носителей ключей электронной подписи в Системе ДБО могут использоваться:

USB-токен.

1.8. Полномочия владельцев сертификатов ключей проверки электронной подписи Клиента подтверждаются карточкой с образцами подписей и оттиска печати (далее – Карточка) или выданными уполномоченным лицам Клиента доверенностями.

1.9. При замене Карточки в связи с заменой или дополнением подписей лиц, имеющих право распоряжаться счетом, Банк изготавливает новые ключи электронной подписи этим лицам. В свою очередь Банк блокирует доступ к Системе ДБО лицам, исключенным из Карточки, или срок доверенностей которых истек.

1.10. Нормы, содержащиеся в Регламенте, становятся обязательными для Клиента с момента подписания Договора и применяются в течение всего срока действия Договора.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями – документ на бумажном носителе, выданный уполномоченным структурным подразделением Банка и заверенный уполномоченным лицом Банка, который включает в себя ключ проверки электронной подписи уполномоченного лица Клиента, сроки действия ключа и идентифицирует владельца сертификата ключа проверки электронной подписи.

АРМ – автоматизированное рабочее место Клиента в Системе ДБО.

Банк – ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МУНИЦИПАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК им. СЕРГИЯ ЖИВАГО» (ООО «МКБ им. С. ЖИВАГО»).

Владелец сертификата ключа проверки электронной подписи – уполномоченный представитель Клиента (физическое лицо), на имя которого Банком выдан сертификат ключа проверки электронной подписи и который владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи подписывать электронные документы.

Договор – договор о расчетном обслуживании с использованием системы дистанционного банковского обслуживания.

Исполнитель – уполномоченный сотрудник Банка, обслуживающий расчетный счет Клиента.

Клиент – юридическое лицо/индивидуальный предприниматель/физическое лицо, занимающееся в установленном законодательством РФ порядке частной практикой, обслуживаемое Банком с использованием Системы ДБО.

Ключ электронной подписи (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 (далее – проверка электронной подписи).

Ключевой носитель – физический носитель, предназначенный для размещения на нем файлов, содержащих ключи электронной подписи и/или ключи проверки электронной подписи.

Компрометация ключа – событие, в результате которого возникает возможность ознакомления неуполномоченных лиц с ключом электронной подписи.

К событиям, связанным с компрометацией ключа ЭП, относятся, включая, но, не ограничиваясь, следующие:

утрата ключевых носителей, в т.ч. с их последующим обнаружением;

увольнение (или перевод на другую работу) сотрудников, имевших доступ к ключам электронной подписи;

нарушение правил хранения и уничтожения ключа электронной подписи;

нерасшифровывание входящих или исходящих сообщений у сторон;

обнаружение или подозрение, что компьютер, на котором установлена Система ДБО, подвергся заражению компьютерными вирусами;

иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к ключу электронной подписи неуполномоченных лиц.

Подтверждение подлинности ЭП в ЭД – положительный результат проверки соответствующим средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в электронном документе, подписанным данной электронной подписью.

Сертификат ключа проверки электронной подписи – электронный документ, изготавливаемый Банком уполномоченному лицу Клиента и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи является действующим на определенный момент времени если:

наступил момент времени начала действия сертификата ключа проверки электронной подписи;

срок действия сертификата ключа проверки электронной подписи не истек;

сертификат ключа проверки электронной подписи не отозван и действие его не приостановлено.

Система ДБО – система Дистанционного Банковского Обслуживания, предназначенная для удаленного управления банковским счетом («Клиент–Банк» или «Интернет–Банк»).

Средства электронной подписи (СЭП) – шифровальные (криптографические) средства, позволяющие установить факт изменения подписанного электронного документа после момента его подписания, обеспечивающие практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа проверки электронной подписи, а также используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Сторона – Банк или Клиент, совместно именуются "Стороны".

Уполномоченное лицо – физическое лицо, наделенное правом подписи электронных документов от имени Стороны на основании распорядительного акта Стороны, либо на основании доверенности, выданной в порядке, установленном законодательством Российской Федерации. Уполномоченное лицо Клиента в обязательном порядке должно быть указано в карточке с образцами подписи и оттиска печати.

Центр сертификации – комплекс программных и аппаратных средств, используемых для реализации функций по созданию (генерации) ключей электронной подписи и выдаче сертификатов ключей проверки электронных подписей.

Электронный документ (ЭД) – электронное сообщение, в котором информация представлена в электронно-цифровой форме, заверенное электронной подписью, подготовленное и переданное с помощью программного обеспечения Системы ДБО в соответствии со всеми процедурами защиты информации.

Электронная подпись (ЭП) – информация в электронной форме, создаваемая с использованием средства электронной подписи, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и получена в результате криптографического преобразования информации с использованием ключа электронной подписи, а также позволяет определить уполномоченное лицо (лиц) подписавшее (подписавших) ЭД и обнаружить факт внесения изменений в подписанный ЭД после момента его подписания. При подписании ЭД Сторонами используется усиленная неквалифицированная электронная подпись.

3. ОРГАНИЗАЦИЯ ОБСЛУЖИВАНИЯ КЛИЕНТА. ПОРЯДОК ФОРМИРОВАНИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СЕРТИФИКАТОВ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

3.1. Клиент предоставляет Банку пакет документов, необходимых для формирования ключей электронной подписи и сертификатов ключей проверки электронной подписи Клиента:

документы, установленные Договором;

доверенность на получение ключей электронной подписи, дистрибутива программного обеспечения Системы ДБО в случае получения установочного комплекта АРМ Клиента и эксплуатационной документации на Систему сотрудником, не являющимся владельцем сертификата ключа проверки электронной подписи.

3.2. Банк осуществляет проверку правильности указанных Клиентом данных в предоставленных документах.

3.3. Клиент оплачивает услуги Банка в соответствии с установленными Тарифами на расчетно-кассовое обслуживание.

3.4. При положительных результатах проверки указанных Клиентом данных в переданных документах Банк в течение 1 рабочего дня от даты заключения Договора формирует установочный комплект АРМ Клиента, который включает в себя:

ключевой носитель;

для системы «Интернет–Банк»: PIN-конверт, содержащий коды доступа к Системе ДБО;

дистрибутив АРМ Клиента.

3.5. Генерация ключа электронной подписи уполномоченного лица Клиента производится самостоятельно Клиентом либо уполномоченным структурным подразделением Банка на ключевой носитель, указанный Клиентом в Заявлении, и Актом к Договору о расчетном обслуживании с использованием системы дистанционного банковского обслуживания (прилагается к Договору).

3.6. Уполномоченное структурное подразделение Банка изготавливает сертификат ключа проверки электронной подписи уполномоченного лица Клиента и Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями, подписываемый обеими Сторонами (Приложение № 1).

3.7. Ключевой носитель с ключом электронной подписи выдается только владельцу сертификата ключа проверки электронной подписи, либо представителю Клиента по доверенности.

3.8. Ключи электронной подписи Клиента начинают действовать с даты, указанной в Акте признания сертификата ключа проверки электронной подписи для обмена сообщениями.

3.9. Клиент обязуется не позднее 10 рабочих дней со дня получения возвратить Банку один экземпляр Акта признания сертификата ключа проверки электронной подписи для обмена

сообщениями, подписанный владельцем сертификата ключа проверки электронной подписи, руководителем организации Клиента и заверенный печатью Клиента. В случае непредставления Клиентом Акта в указанный срок, Банк имеет право приостановить действие данного сертификата ключа проверки электронной подписи.

3.10. Установка АРМ Системы ДБО у Клиента, в зависимости от выбранного Клиентом способа, осуществляется Клиентом самостоятельно, либо сотрудниками Банка. Установка осуществляется на рабочее место, соответствующее требованиям к АРМ, указанным в Договоре. В случае несоответствия требованиям установка Системы не производится.

3.11. В случае выбора Клиентом услуги «Установка системы сотрудником банка» Банк в течение 10 рабочих дней от даты получения Клиентом ключей электронной подписи производит установку Клиенту Системы ДБО (при наличии технической возможности и при предоставлении Клиентом доступа к оборудованию и рабочему месту для работы в Системе ДБО), а также передает Клиенту эксплуатационную документацию на Систему и проводит консультацию Клиента по работе с программным обеспечением.

3.12. При самостоятельной установке Системы ДБО уполномоченный сотрудник Клиента прибывает в Банк для получения дистрибутива АРМ Клиента и эксплуатационной документации на Систему. В случае получения установочного комплекта АРМ Клиента лицом, не являющемся владельцем сертификата ключа проверки электронной подписи, установочный комплект АРМ выдается по доверенности на его получение.

3.13. При невозможности восстановления силами Клиента программного обеспечения Системы ДБО, испорченного не по вине Банка (вирусы, техническая неисправность компьютера и др.), оно подлежит восстановлению работниками Банка. Услуга оплачивается Клиентом в соответствии с действующими тарифами Банка.

4. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ

4.1. Срок действия ключа электронной подписи Банка составляет один год.

4.2. Срок действия ключа электронной подписи Клиента составляет один год.

4.3. Начало периода действия ключа электронной подписи Клиента исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

4.4. Срок действия сертификата ключа проверки электронной подписи Клиента составляет один год.

4.5. В Системе ДБО автоматически выполняется контроль срока действия сертификатов ключей проверки электронной подписи. Уполномоченное лицо не может подписать электронный документ своей электронной подписью или произвести зашифрование информации в текущий момент времени, если к этому времени истек срок действия его сертификата ключа проверки электронной подписи. Также уполномоченное лицо не может проверить электронную подпись электронного документа или произвести расшифрование информации, если истек срок действия сертификата ключа проверки электронной подписи, необходимого для выполнения соответствующей операции.

5. ПОРЯДОК ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ

5.1. Проведение плановой смены ключей электронной подписи Клиента.

5.1.1. За 30 суток до окончания срока действия ключей электронной подписи Клиент при входе в Систему ДБО получает уведомление о необходимости смены ключей.

5.1.2. Не позднее, чем за 1 рабочий день до даты фактического истечения срока действия ключа электронной подписи, Клиент обязан самостоятельно инициировать перегенерацию ключей или получить новые ключи электронной подписи в Банке. В противном случае работа Клиента по Системе ДБО приостанавливается до момента обращения Клиента в Банк и генерации для него новых ключей электронной подписи.

5.1.3. Смена ключей электронной подписи на АРМ Клиента (удаленная перегенерация).

5.1.3.1. При формировании Клиентом своих новых ключей электронной подписи замена ключевого носителя не требуется. Новые ключи записываются на старый ключевой носитель.

5.1.3.2. Клиент средствами Системы ДБО генерирует новый ключ электронной подписи, формирует запрос на сертификат ключа проверки электронной подписи, подписывает его действующим на момент формирования запроса ключом электронной подписи и передает его в Банк по Системе ДБО. Действующие ключи электронной подписи должны быть сохранены до ввода в действие новых ключей.

5.1.3.3. Уполномоченное лицо Банка, получив запрос на изготовление сертификата ключа проверки электронной подписи уполномоченного лица Клиента, проверяет данные из запроса (проверяется соответствие параметров запроса конкретному физическому лицу и правильность ЭП под запросом на сертификат ключа проверки электронной подписи). При положительных результатах проверки, не позднее следующего рабочего дня обрабатывает запрос на сертификат ключа проверки электронной подписи в Системе ДБО и получает изготовленный новый сертификат ключа проверки электронной подписи Клиента, который отправляется Клиенту средствами Системы ДБО.

5.1.3.4. Если результат проверки отрицательный, Банк и Клиент проводят расследование, в ходе которого выясняется и устраняется причина несоответствия.

5.1.3.5. При получении из Банка нового сертификата ключа проверки электронной подписи Клиент либо завершает формирование нового комплекта ключей и ввод их в эксплуатацию, либо откладывает переход на новый комплект ключей. При этом новый комплект ключей должен быть введен в эксплуатацию до истечения срока действия старого комплекта.

5.1.3.6. После перехода на новые ключи Клиент обязан забрать в Банке у своего исполнителя на подпись документы – Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями, и вернуть в Банк в течение 10 рабочих дней надлежащим образом заверенные экземпляры Банка. В противном случае Банк имеет право приостановить работу Клиента по Системе ДБО до момента получения подписанных Актов. Получение Актов признания сертификата ключа проверки электронной подписи для обмена сообщениями у исполнителя может производиться только уполномоченным лицом Клиента или лицом, имеющим доверенность на получение документов по расчетному счету, либо лицом, имеющим отдельную доверенность на получение конкретных документов.

5.1.4. Смена ключей электронной подписи Клиента в Банке.

5.1.4.1. В случае если Клиент не успел или не смог самостоятельно перейти на новые ключи электронной подписи при плановой смене, Клиент обращается непосредственно в уполномоченное подразделение Банка.

5.1.4.2. Генерация ключа электронной подписи уполномоченного лица Клиента производится уполномоченным структурным подразделением Банка на старый ключевой носитель, имеющийся у Клиента, либо на новый ключевой носитель.

5.1.4.3. Уполномоченное структурное подразделение Банка изготавливает сертификат ключа проверки электронной подписи уполномоченного лица Клиента и Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями, подписываемый обеими Сторонами.

5.1.4.4. Ключевой носитель с ключом электронной подписи выдается только владельцу сертификата ключа проверки электронной подписи, либо представителю Клиента по доверенности.

5.1.4.5. Клиент обязуется не позднее 10 рабочих дней со дня получения возвратить Банку один экземпляр Акта признания сертификата ключа проверки электронной подписи для обмена сообщениями, подписанный владельцем сертификата ключа проверки электронной подписи, руководителем организации Клиента и заверенный печатью Клиента. В случае непредставления Клиентом Акта в указанный срок, Банк имеет право приостановить действие данного сертификата ключа проверки электронной подписи.

5.2. Проведение плановой смены ключей электронной подписи Банка.

5.2.1. Плановая смена ключей Банка (ключа электронной подписи и соответствующего ему ключа проверки электронной подписи) выполняется за 6 месяцев до окончания срока действия ключа электронной подписи Банка.

5.2.2. Процедура плановой смены ключей Банка осуществляется в следующем порядке:

5.2.2.1. Уполномоченное лицо Банка генерирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи Банка.

5.2.2.2. Уполномоченное лицо Банка изготавливает новый сертификат ключа проверки электронной подписи Банка.

5.2.2.3. Банк оповещает Клиентов о проведении смены ключей Банка путем распространения нового сертификата ключа проверки электронной подписи Банка средствами Системы ДБО.

5.2.2.4. Не позднее, чем за 2 рабочих дня до даты фактического истечения срока действия рабочих ключей электронной подписи Банка, Клиент обязан произвести регистрацию новых ключей Банка средствами Системы ДБО. Если Клиент не произвел регистрацию новых ключей электронной подписи Банка, его обслуживание в Системе ДБО приостанавливается. Возобновление обслуживания в Системе ДБО производится после обращения Клиента в Банк.

6. ПОРЯДОК ВНЕПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ

6.1. Внеплановая смена ключей осуществляется в следующих случаях:

6.1.1. При компрометации ключа электронной подписи Клиента.

6.1.2. При компрометации ключа электронной подписи Банка.

6.1.3. При выходе из строя ключевого носителя.

6.1.4. При смене уполномоченных лиц Клиента.

6.1.5. При изменении регистрационных данных владельца сертификата ключа проверки электронной подписи (например, смена фамилии).

6.1.6. В иных случаях, вызванных форс-мажорными обстоятельствами.

6.2. В случае принятия решения Клиентом о компрометации своих ключей электронной подписи Клиент обязан по телефону, указанному в Договоре, сообщить в Банк о факте компрометации используемых ключей электронной подписи и прекратить их использование.

6.3. Банк приостанавливает расчеты с использованием Системы ДБО до письменного заявления Клиента.

6.4. В течение следующего рабочего дня Клиент обязан направить на имя Председателя Правления Банка письменное заявление о факте компрометации, подписанное руководителем организации и заверенное печатью Клиента.

6.5. Банк в течение одного рабочего дня от получения письменного заявления о компрометации ключей электронной подписи осуществляет отзыв сертификата ключа проверки электронной подписи и блокирует действие скомпрометированных ключей. Дата, с которой сертификат ключа проверки электронной подписи считается недействительным, устанавливается равной дате отзыва сертификата.

6.6. Для проведения внеплановой смены ключей электронной подписи в случаях, определенных в п.п. 6.1.1., 6.1.3., 6.1.4., 6.1.5. настоящего Регламента, Клиент обращается в уполномоченное подразделение Банка.

6.7. Генерация ключа электронной подписи уполномоченного лица Клиента производится уполномоченным структурным подразделением Банка на старый ключевой носитель, имеющийся у Клиента, либо на новый ключевой носитель.

6.8. Уполномоченное структурное подразделение Банка изготавливает сертификат ключа проверки электронной подписи уполномоченного лица Клиента и Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями, подписываемый обеими Сторонами.

6.9. Ключевой носитель с ключом электронной подписи выдается только владельцу сертификата ключа проверки электронной подписи, либо представителю Клиента по доверенности.

6.10. Клиент обязуется не позднее 10 рабочих дней со дня получения возвратить Банку один экземпляр Акта признания сертификата ключа проверки электронной подписи для обмена сообщениями, подписанный владельцем сертификата ключа проверки электронной подписи, руководителем организации Клиента и заверенный печатью Клиента. В случае непредставления Клиентом Акта в указанный срок, Банк имеет право приостановить действие данного сертификата ключа проверки электронной подписи.

6.11. Вышедший из-под контроля ключевой носитель многократного использования подлежит дальнейшему использованию только после гарантированного уничтожения содержащейся на нем информации согласно технологии, принятой для данного вида носителей.

6.12. В случае физической порчи ключевого носителя Клиента ключ электронной подписи формируется на новый ключевой носитель.

6.13. В случае компрометации ключа электронной подписи Банка (или физической порче ключевого носителя) сертификат ключа проверки электронной подписи Банка прекращает свое действие. Дата, с которой сертификат ключа проверки электронной подписи считается недействительным, устанавливается равной дате отзыва сертификата.

6.14. Банк оповещает Клиентов о факте компрометации с использованием средств Системы ДБО. Банк производит замену ключей электронной подписи Банка способом, описанным в п. 5.2. настоящего Регламента.

7. ПРЕКРАЩЕНИЕ/ПРИОСТАНОВЛЕНИЕ ОБСЛУЖИВАНИЯ КЛИЕНТА ПО СИСТЕМЕ ДБО

7.1. Обслуживание Клиента по системе ДБО прекращается автоматически при расторжении Договора банковского счета (при закрытии расчетного счета Клиента), а также в случаях, предусмотренных Договором.

7.2. Сертификаты ключей подписи, владельцами которых являются уполномоченные лица Клиента, аннулируются (отзываются) уполномоченным подразделением Банка не позднее рабочего дня, следующего за днем прекращения обслуживания. Временем прекращения действия сертификата ключа проверки электронной подписи признается время его отзыва.

7.3. Банк может самостоятельно принять решение о прекращении действия сертификата ключа проверки электронной подписи Клиента в случаях, предусмотренных Договором, а также в случаях:

7.3.1. Получения Банком сведений о компрометации ключа электронной подписи Клиента.

7.3.2. Получения Банком сведений о ставших недействительными данных, содержащихся в сертификате ключа проверки электронной подписи (например, при смене карточки с образцами подписей и оттиска печати либо Банку стало известно из достоверных источников, что владелец сертификата ключа проверки электронной подписи более не является уполномоченным лицом Клиента).

7.4. Банк может самостоятельно принять решение о приостановлении действия сертификата ключа проверки электронной подписи Клиента в случаях, предусмотренных Договором, а также, если сочтет, что имеются достаточные основания сомневаться в подлинности подписи уполномоченного лица или оттиска печати Клиента в Акте признания сертификата ключа проверки электронной подписи для обмена сообщениями.

7.5. В случае вынесения решения о прекращении либо приостановлении действия сертификата ключа проверки электронной подписи Клиента Банк уведомляет Клиента об этом средствами Системы ДБО.

8. ПРАВА И ОБЯЗАННОСТИ СТОРОН

8.1. Банк обязан:

8.1.1. Информировать Клиента об условиях и о порядке использования электронных подписей и средств электронной подписи, рисках, связанных с использованием средств электронной подписи, и мерах, необходимых для обеспечения безопасности при работе в Системе ДБО. Информирование осуществляется путем размещения информации на сайте Банка по электронному адресу www.zhivagobank.ru, информационных рассылках, направляемых Клиенту через Систему ДБО, почтовой связью.

8.1.2. Обеспечивать актуальность информации, содержащейся в реестре Центра сертификации, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

8.1.3. Обеспечивать конфиденциальность созданных Банком ключей электронных подписей. В том числе обеспечить защиту от несанкционированного доступа ключа электронной подписи Центра сертификации Банка.

8.1.4. Изготовить сертификат ключа проверки электронной подписи Клиента в соответствии с порядком, определенным в настоящем Регламенте.

8.1.5. Предоставить Клиенту сертификат ключа проверки электронной подписи Банка в электронной форме.

8.1.6. Предоставить Клиенту сертификат ключа проверки электронной подписи Центра сертификации Банка в электронной форме.

8.1.7. Обеспечить уникальность значений ключей проверки электронной подписи в изготовленных сертификатах ключей проверки электронной подписи Клиентов.

8.1.8. Внести в реестр Центра сертификации информацию о прекращении действия сертификата ключа проверки электронной подписи Клиента в случаях, определенных настоящим Регламентом.

8.1.9. Хранить сертификаты ключей проверки электронной подписи в течение всего периода их действия и пять лет после истечения срока их действия или аннулирования (отзыва). По истечении указанного срока хранения сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

8.2. Клиент обязан:

8.2.1. Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

8.2.2. Обратиться в Банк с заявлением о факте компрометации ключа электронной подписи в случае потери, раскрытия, искажения ключа электронной подписи, а также в случае, если Клиенту стало известно, что этот ключ несанкционированно используется или использовался ранее другими лицами, не позднее следующего рабочего дня со дня получения информации о таком нарушении.

8.2.3. Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

8.2.4. Применять для формирования электронной подписи только действующий ключ электронной подписи.

8.2.5. Самостоятельно контролировать сроки действия своих ключей и своевременно инициировать процедуру их плановой смены в соответствии с п. 5.1. настоящего Регламента.

8.2.6. По требованию Банка сгенерировать новые ключи электронной подписи и зарегистрировать новые ключи проверки электронной подписи Клиента в Банке.

8.2.7. В случае перегенерации ключей электронной подписи в течение 10 рабочих дней предоставить в Банк подписанный со своей стороны Акт признания сертификата ключа проверки электронной подписи для обмена сообщениями.

8.2.8. Известить Банк об изменениях в карточке с образцами подписей и оттиска печати, местонахождения, правового статуса, телефонов, иной контактной информации в течение трех рабочих дней. До поступления сообщения об указанных изменениях все действия,

совершенные по ранее указанным Клиентом реквизитам, считаются совершенными законно и засчитываются как выполнение Сторонами своих обязательств.

8.2.9. Эксплуатировать средства электронной подписи в соответствии с требованиями Договора.

8.3. Банк имеет право:

8.3.1. Запросить у Клиента, заключившего Договор, документы, подтверждающие следующую информацию:

8.3.1.1.Полное фирменное наименование юридического лица и основной государственный регистрационный номер.

8.3.1.2.Идентификационный номер налогоплательщика (ИНН).

8.3.1.3.Копии протоколов либо иных документов о назначении руководителя организации Клиента (в соответствии с учредительными документами).

8.3.1.4.Копии документов о предоставлении уполномоченным лицам Клиента права подписи ЭД.

8.3.1.5.Сведения, необходимые для идентификации уполномоченных лиц Клиента: фамилия, имя, отчество, серия и номер паспорта, дата и кем выдан.

8.3.2. Отказать в изготовлении сертификата ключа проверки электронной подписи Клиента в случае ненадлежащего оформления заявления о компрометации ключа электронной подписи или в случае не подтверждения подлинности электронной подписи владельца сертификата ключа проверки электронной подписи в запросе сертификата для обмена сообщениями при удаленной перегенерации ключей электронной подписи Клиента.

8.3.3. Отказать Клиенту в передаче ключа электронной подписи в случае отсутствия у представителя Клиента доверенности на получение ключевого носителя.

8.3.4. Приостановить действие сертификата ключа проверки электронной подписи Клиента, если сочтет, что имеются достаточные основания сомневаться в подлинности подписи уполномоченного лица или оттиска печати Клиента в Акте признания сертификата ключа проверки электронной подписи для обмена сообщениями.

8.3.5. Назначать своих уполномоченных лиц, имеющих право обслуживать программно-технические средства Системы ДБО.

8.4. Клиент имеет право:

8.4.1. В любое время генерировать новые ключи электронной подписи.

8.4.2. Обратиться в Банк с заявлением на изготовление сертификата ключа проверки электронной подписи.

8.4.3. Обратиться в Банк для аннулирования (отзыва) рабочего сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.

8.4.4. Обратиться в Банк за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием ключа электронной подписи, связанного с сертификатом ключа проверки электронной подписи, владельцем которого он является.

8.4.5. Получить сертификат ключа проверки электронной подписи Банка в электронном виде.

8.4.6. Получить сертификат ключа проверки электронной подписи Центра сертификации в электронном виде.

8.4.7. Применять сертификат ключа проверки электронной подписи Центра сертификации для проверки электронной подписи Центра сертификации в сертификатах ключей проверки электронной подписи.

8.4.8. Для хранения ключа электронной подписи применять любой носитель, указанный в п. 1.7.

9. ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. Сторона, виновная в неисполнении или ненадлежащем исполнении своих обязанностей по настоящему Регламенту, возмещает другой Стороне все связанные с этими

нарушениями убытки в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной, в соответствии с действующим законодательством Российской Федерации. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

9.2. Стороны несут ответственность за обеспечение сохранности ключей электронной подписи, за надлежащее использование программного обеспечения средств электронной подписи, исключающее порчу и утрату ключей электронной подписи, а также их использование третьими лицами.

9.3. Стороны не несут ответственность в случае сбоев в сети телекоммуникаций, посредством которых Стороны осуществляют информационный обмен по настоящему Регламенту, приведших к утере или невозможности доставки передаваемой информации, если такие сбои были вне зоны влияния Сторон.

9.4. Банк не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Банк обоснованно полагался на сведения, указанные в заявлениях Клиента.

9.5. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется в соответствии с законодательством Российской Федерации.

10. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

10.1. Ключ электронной подписи Клиента, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией владельца сертификата ключа проверки электронной подписи. Банк не осуществляет хранение ключей электронной подписи Клиентов.

10.2. Персональная и корпоративная информация о владельцах сертификатов ключей проверки электронной подписи и представителях Клиента является конфиденциальной.

10.3. Банк имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

11. РАЗРЕШЕНИЕ СПОРОВ

11.1. При возникновении споров Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

11.2. Сторона, получившая от другой Стороны претензию, обязана в течение 30 календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

11.3. При разрешении споров для проведения процедуры технической экспертизы, заключающейся в подтверждении подлинности электронной подписи Клиента в электронных документах в отношении выданных Банком сертификатов ключей проверки электронной подписи, а также подтверждении подлинности электронной подписи Центра сертификации в изданных им сертификатах ключей проверки электронной подписи, Стороны руководствуются Договором.

11.4. Стороны обязуются принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

11.5. Спорные вопросы между Сторонами, не урегулированные в претензионном порядке, решаются в Арбитражном суде города Рязани.

12. ФОРС-МАЖОР

12.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после заключения Договора.

12.2. Форс-мажорными обстоятельствами признаются чрезвычайные и непредотвратимые при указанных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

12.3. Сторона обязана известить другую Сторону в письменной форме о возникновении и прекращении действия форс-мажорных обстоятельств, препятствующих исполнению обязательств по настоящему Регламенту, при этом срок выполнения обязательств по настоящему Регламенту переносится соразмерно времени, в течение которого действовали такие обстоятельства.

12.4. При невозможности полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту, обусловленной действием форс-мажорных обстоятельств свыше одного месяца, каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

13. СРОК ДЕЙСТВИЯ РЕГЛАМЕНТА. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТОЯЩИЙ РЕГЛАМЕНТ

13.1. Настоящий Регламент вступает в силу с даты подписания Договора и действует в течение срока действия Договора банковского счета или Договора, если Стороны не предусмотрят иное.

13.2. Настоящий Регламент размещен в электронной форме на сайте Банка по электронному адресу www.zhivagobank.ru.

13.3. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Банком в одностороннем порядке.

13.4. Новая версия Регламента публикуется на сайте Банка по электронному адресу www.zhivagobank.ru.

13.5. Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется Банком путем рассылки Клиентам электронных сообщений через Систему ДБО. Рассылка производится в день размещения информации на сайте Банка.

13.6. Все изменения (дополнения), вносимые в настоящий Регламент в установленном порядке, вступают в силу и становятся обязательными по истечении 14 календарных дней с даты публикации новой редакции Регламента на сайте Банка.

13.7. Любые изменения (дополнения), вносимые в настоящий Регламент, с даты их вступления в силу равно распространяются на всех Клиентов, заключивших Договор, в том числе заключивших Договор ранее даты вступления изменений (дополнений) в силу.

13.8. В случае несогласия с изменениями (дополнениями) Клиент имеет право до вступления в силу таких изменений (дополнений) на расторжение Договора в порядке, предусмотренном разделом 11 Договора, при этом комиссия, уплаченная Банку в соответствии с тарифами, Клиенту не возвращается.

Приложение № 1
к Регламенту управления сертификатами ключей проверки электронной подписи в Системе ДБО ООО «МКБ им. С.ЖИВАГО»

АКТ
признания сертификата ключа проверки электронной подписи для обмена сообщениями

“____“_____20__г. г. Рязань

Настоящим Актом признаётся ключ проверки электронной подписи, принадлежащий уполномоченному представителю организации: _____
(ФИО представителя организации)

(Название пользователя: _____).
(наименование пользователя (криптопрофиля) в Системе)

Параметры ключа:
Алгоритм:_____
Начало срока действия:_____
Окончание срока действия:_____

Ключ проверки электронной подписи:

Дополнительные поля ключа проверки электронной подписи:
Серийный номер ключа:_____
Имя владельца ключей:_____
Организация: _____, C=_____, S=_____,
L=_____
Данные об издателе: CN=_____ (ООО «МКБ им. С. ЖИВАГО», 390000, г. Рязань, ул. Почтовая, д. 64, тел. 8-800-100-64-44, факс (4912) 27-52-42)

Ключ зарегистрирован и может использоваться для обмена сообщениями.

Личная подпись владельца ключа ЭП _____ /_____/
(подпись) (ФИО)

От БАНКА:
_____
(должность сотрудника Банка)

_____ /_____/
(подпись) (ФИО)

Доверенность № ___ от __.__.20__ г.,
выданная ООО «МКБ им. С. ЖИВАГО»

М.П.

От КЛИЕНТА:
Руководитель организации

_____ /_____/
(подпись) (ФИО)

М.П.