Утверждены
Председателем Правления
ЗАО «Райффайзенбанк»
Мониным С.А.
10.09.2012

ПРАВИЛА СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА СПЕЦИАЛИЗИРОВАННОГО ДЕПОЗИТАРИЯ ЗАО «РАЙФФАЙЗЕНБАНК»

Версия 3.1

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила электронного документооборота ЗАО «Райффайзенбанк» *(*далее именуемые Правила*)*, а также приложения к ним определяют общий порядок и принципы осуществления электронного документооборота между ЗАО «Райффайзенбанк» *(*далее именуется Организатор СЭД *или* Банк*)* и лицами, присоединившимися к системе электронного документооборота ЗАО «Райффайзенбанк» *(*далее именуемые Участники ЭДО или Участник ЭДО*)*.

1.2. Настоящие Правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 10 января 2002 года N 1-ФЗ «Об электронно-цифровой подписи», Постановления Правительства РФ от 29 декабря 2007 года № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» и иных нормативных правовых актов Российской Федерации.

1.3. Настоящие Правила становятся обязательными для Участника ЭДО с момента заключения между Участником ЭДО и Организатором СЭД Договора о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк» (по форме, указанной в Приложении №1 к Правилам) *(*далее именуется Договор*)*.

1.4. Документы в электронно-цифровой форме, обмен которыми осуществляется в системе электронного документооборота ЗАО «Райффайзенбанк» (далее именуется СЭД), могут быть подготовлены в соответствии с форматами электронных документов, принятыми и утвержденными Организатором СЭД (в соответствии с перечнем, приведенным в Приложении №2 к Правилам) или сформированы в форматах «.doc», «.xls», «.csv», «.txt», «.bcw» (далее именуются Формализованные документы) либо подготовлены путем сканирования документов в бумажном виде.

1.5. Для обеспечения авторства, целостности и конфиденциальности электронных документов Организатор СЭД и Участники ЭДО используют программное обеспечение, средства криптографической защиты информации *(*далее именуются СКЗИ*)*, ключи и сертификаты ключей, ключевые носители, предоставляемые Организатором СЭД в порядке, установленном настоящими Правилами.

1.6. СЭД обеспечивает обмен электронными документами между Организатором СЭД и Участником ЭДО.

1.7. Настоящие Правила, включая все Приложения, утверждаются Организатором СЭД. Изменения и дополнения в настоящие Правила и Приложения к ним вносятся в одностороннем порядке по решению Организатора СЭД. Организатор СЭД вправе определять и изменять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила и Приложения к ним.

1.8. Настоящие Правила, включая все приложения к ним, Изменения и дополнения к ним, подлежат обязательному опубликованию в сети Интернет на официальной странице Банка - www.raiffeisen.ru.

1.9. Изменения и дополнения в настоящие Правила и приложения к ним, а также решения о сроках и порядке вступления их в силу, доводятся Организатором СЭД до сведения Участников ЭДО путем направления электронного сообщения с уведомлением о данном факте не позднее, чем за 5 (Пять) рабочих дней до вступления в силу изменений в Правила и приложения к ним, а также путем опубликования этой информации в сети Интернет на официальной странице Банка - www.raiffeisen.ru. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО (по форме, указанной в Приложении №4 к настоящим Правилам).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин/ Сокращение	Определение
Авторство электронного документа	Принадлежность электронного документа конкретному Участнику ЭДО. Авторство электронного документа определяется принадлежностью электронно-цифровой подписи конкретному Участнику ЭДО
Агент	Агент по выдаче, погашению и обмену инвестиционных паев
Владелец сертификата ключа подписи	Физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы)
Доставка электронного документа (Доставка)	Процесс перемещения Электронного документа от Отправителя к Получателю, в том числе его получение Получателем
Закрытый (секретный) ключ электронно-цифровой подписи (Закрытый (секретный) ключ)	Уникальная последовательность данных, известная Владельцу сертификата ключа подписи и предназначенная для формирования в электронных документах электронно-цифровой подписи с использованием средств криптографической защиты информации и расшифрования электронного документа его Получателем
Ключевой носитель	Любой носитель информации, содержащий криптографические ключи
Компрометация криптографического ключа (Компрометация ключа)	Констатация лицом, владеющим Закрытым (секретным) ключом электронно-цифровой подписи, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами
Конфиденциальная информация	Документированная и электронная информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и если обладатель информации принимает меры к ее охране
Криптографический ключ (Ключи)	Общее название Открытого ключа электронно-цифровой подписи и Закрытого (секретного) ключа электронно-цифровой подписи
Оператор Удостоверяющего центра (Оператор УЦ) –	Уполномоченный сотрудник Организатора СЭД, осуществляющий взаимодействие с Участником ЭДО в процессе Управления ключами и сертификатами ключей.
Организатор системы электронного	Закрытое акционерное общество «Райффайзенбанк» (ЗАО «Райффайзенбанк»), имеющее лицензии ФСБ России №5142 Х от 20 февраля 2008 года на осуществление технического обслуживания

документооборота (Организатор СЭД)	шифровальных (криптографических) средств, №5143 Р от 20 февраля 2008 года на осуществление распространения шифровальных (криптографических) средств, №5144 У от 20 февраля 2008 года на осуществление предоставления услуг в области шифрования информации и осуществляющее эксплуатацию СЭД
Открытый ключ электронно-цифровой подписи (Открытый ключ)	Уникальная последовательность символов, соответствующая Закрытому (секретному) ключу электронно-цифровой подписи, доступная любому Участнику ЭДО и предназначенная для Подтверждения подлинности электронно-цифровой подписи в электронном документе с использованием средств криптографической защиты информации и шифрования электронного документа его Отправителем
Отправитель электронного документа (Отправитель)	Лицо, которое, или от имени которого, направляется электронный документ
Плановая смена ключей	Смена Ключей с установленной в СЭД периодичностью, не вызванная Компрометацией ключей
Подтверждение подлинности электронно-цифровой подписи в электронном документе	Положительный результат проверки принадлежности электронно-цифровой подписи в электронном документе Владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе. Подтверждение подлинности электронно-цифровой подписи должно осуществляться соответствующим средством электронно-цифровой подписи с использованием сертификата ключа подписи
Получатель электронного документа (Получатель)	Лицо, которому предназначен электронный документ, отправленный Отправителем
Сертификат ключа электронно-цифровой подписи (Сертификат ключа подписи)	Документ на бумажном носителе с собственноручной подписью Уполномоченного лица УЦ, который выдается Участнику ЭДО и включает в себя Открытый ключ электронно-цифровой подписи для Подтверждения подлинности электронно-цифровой подписи и идентификации Владельца сертификата ключа подписи
Система электронного документооборота ЗАО «Райффайзенбанк» (СЭД)	Совокупность правил и программно-технических средств, реализованная в рамках взаимодействия Организатора СЭД с Участниками ЭДО в целях осуществления электронного документооборота и являющаяся корпоративной информационной системой
Средства	Совокупность программно-технических средств, обеспечивающих

криптографической защиты информации (СКЗИ)	применение электронно-цифровой подписи и шифрования/расшифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение
Уполномоченный представитель Участника ЭДО (Уполномоченное лицо Участника ЭДО)	Должностное лицо Участника ЭДО, который в соответствии с учредительными документами вправе действовать от имени Участника ЭДО без доверенности либо лицо, которому предоставлены соответствующие полномочия на основании доверенности. Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ)- должностное лицо Банка наделенное полномочиями по заверению Сертификатов ключей подписей и списков отозванных сертификатов
Управление ключами и сертификатами ключей	Создание (генерация) Ключей и Сертификатов ключей подписи, их хранение, распространение, удаление (уничтожение), учет (ведение реестра), а также действия, необходимые для выполнения функций удостоверяющего центра в соответствии со статьей 9 Федерального закона от 10 января 2002 года №1-ФЗ «Об электронной цифровой подписи»
Участник электронного документооборота (Участник ЭДО)	Лицо, участвующее в электронном документообороте в качестве отправителя и/или получателя электронных документов и заключившее договор о присоединении к Правилам электронного документооборота ЗАО «Райффайзенбанк»
Форматы электронных документов	Утвержденные Банком форматы электронных документов, используемые в СЭД
Шифрование	Криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного электронного документа
Электронное сообщение (Сообщение)	Совокупность данных, закодированная способом, позволяющим обеспечить ее обработку программными и/или аппаратными средствами, передачу по каналам связи и хранение на цифровых носителях информации
Электронно-цифровая подпись (ЭЦП)	Неотъемлемая часть (реквизит) электронного документа, предназначенная для защиты данного электронного документа от подделки и являющаяся аналогом собственноручной подписи должностного лица или уполномоченного представителя юридического лица, представленная в электронно-цифровой форме, как результат криптографического преобразования информации с использованием Закрытого (секретного) ключа электронно-цифровой подписи, который позволяет идентифицировать Владельца сертификата ключа подписи, а также установить отсутствие искажения информации в Электронном документе
Электронный документ	Документ, в котором информация представлена в электронно-

(Документ)	цифровой форме, а также: · документ подготовлен в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде; · документ подписан электронно-цифровой подписью.
Электронный документооборот (ЭДО)	Обмен Электронными документами, зашифрованными и подписанными ЭЦП, в соответствии с настоящими Правилами и приложениями к нему, посредством электронной почты или с помощью иных способов передачи документов в электронно-цифровой форме в процессе осуществления Банком своей деятельности

3. ПОРЯДОК ДОПУСКА УЧАСТНИКА ЭДО К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СЭД

3.1. Участник ЭДО и Организатор СЭД должны выполнить поэтапно следующие действия, необходимые для получения допуска к осуществлению ЭДО в СЭД:

- заключение договора с Организатором СЭД о присоединении к настоящим
Правилам;
- установка Участником ЭДО выданного Организатором СЭД СКЗИ на свои программно-технические средства. Инсталляция производится сотрудником Участника ЭДО, который удовлетворяет требованиям п. 7.4 настоящих Правил;
- выполнение Оператором УЦ процедуры генерации криптографических ключей Участника ЭДО;
- изготовление Уполномоченным лицом УЦ сертификата ключа электронно-цифровой подписи для уполномоченного лица Участника ЭДО. Сертификат ключа выдается в форме электронного документа и в форме документа на бумажном носителе. Сертификат ключа в форме документа на бумажном носителе формируется в 2 (двух) экземплярах, которые заверяются собственноручными подписями уполномоченного лица Участника ЭДО и Уполномоченного лица УЦ, а также печатью удостоверяющего центра (далее - УЦ).

3.2. После выполнения действий, указанных в п. 3.1 настоящих Правил, производится тестовая эксплуатация СЭД. Срок тестовой эксплуатации - не более 30 (тридцати) рабочих дней с момента начала эксплуатации. По окончании тестовой эксплуатации Организатор СЭД и Участник ЭДО подписывают Акт о начале электронного документооборота (по форме, указанной в Приложении №3 к настоящим Правилам) в двух экземплярах по одному для каждой из сторон.

3.3. Перед началом обмена Электронными документами в СЭД Участник ЭДО и Организатор СЭД обмениваются Анкетами (по форме, указанной в Приложении № 4 и № 5 к настоящим Правилам). В дальнейшем в случае каких-либо изменений данных Анкеты одна сторона предоставляет другой стороне новую Анкету. При этом предыдущая Анкета утрачивает силу.

3.4. Участник ЭДО из числа своих сотрудников назначает ответственных лиц, имеющих право работать со СКЗИ с указанием их полномочий и срока действия этих полномочий.

4. ОСОБЕННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА

4.1. Требования к Электронному документу и порядок использования Электронного документа.

4.1.1. Электронный документ, сформированный в рамках СЭД, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящими Правилами.

4.1.2. Электронное сообщение приобретает статус Электронного документа при его соответствии настоящим Правилам.

4.1.3. Электронный документ должен быть подготовлен в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде.

4.1.4. Все действия с Электронными документами, оформленными, переданными и/или полученными в соответствии с настоящими Правилами признаются Участниками ЭДО совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

4.1.5. Документы, передаваемые в рамках СЭД, должны содержать сведения, в точности соответствующие сведениям, содержащимся в документах, оформленных в бумажном виде.

4.1.6. Управляющая компания и/или Агент, передавая Электронные документы для формирования и ведения реестра владельцев инвестиционных паев, в том числе анкеты, заявления, учредительные документы, заявки на выдачу/погашение/обмен инвестиционных паев, платежные документы, подтверждает, что:

- Управляющей компанией и/или ее Агентами были приняты соответствующие документы в бумажном виде;
- Управляющая компания и/или ее Агенты осуществили все необходимые проверки (достоверность принимаемых ею первичных документов и содержащихся в них сведений, правильность оформления данных документов, наличие образца подписи пайщика на анкете и наличие подписи (пайщика или его представителя) в других документах, полномочия указанных в документах лиц и т.д.);
- на всех документах, принятых от заявителя имеются необходимые отметки, заверенные печатью и подписью уполномоченного представителя Управляющей компании;
- сведения в передаваемых специализированному депозитарию документах, подписанных электронно-цифровой подписью, полностью соответствуют сведениям, содержащимся в документах, оформленных в бумажном виде.

4.1.7. В случае передачи Электронного документа в соответствии с Форматами электронных документов, Управляющая компания и/или Агент гарантирует корректность оформления соответствующего документа на бумажном носителе, в том числе заполнение всех обязательных полей в документе, наличие подписи и образца подписи (в случае передачи Анкеты зарегистрированного физического лица).

4.2. Порядок использования электронно-цифровой подписи и шифрования.

4.2.1. Электронный документ должен быть подписан Закрытым (секретным) ключом электронно-цифровой подписи, который соответствует Открытому ключу электронно-цифровой подписи, указанному в действующем Сертификате ключа подписи, содержащем область использования, применение которой допускается в СЭД.

4.2.2. Действительность Закрытых (секретных) ключей электронно-цифровой подписи на

момент проверки не влияет на юридическую силу Электронного документа, если он был подписан действующим на момент подписания Закрытым (секретным) ключом электронно-цифровой подписи в соответствии с настоящими Правилами. Моментом подписания Электронного документа считается время и дата, включаемые Отправителем в подписываемый электронный документ. Все передаваемые Электронные документы должны содержать время и дату подписания документа. Достоверность времени и даты подписания Электронного документа контролируется на стороне Получателя.

4.2.3. Каждый Участник ЭДО должен иметь свой индивидуальный Закрытый (секретный) ключ электронно-цифровой подписи для подписания исходящих от него Электронных документов.

4.2.4. Любой Электронный документ должен быть зашифрован.

4.2.5. Полученный зашифрованный Электронный документ должен быть расшифрован, после чего проводится проверка электронно-цифровой подписи.

4.2.6. Электронный документ принимается к дальнейшей обработке и исполнению только после положительного результата проверки электронно-цифровой подписи.

4.2.7. Участниками ЭДО используются программное обеспечение, СКЗИ, а также открытые и закрытые (секретные) ключи и соответствующие сертификаты ключей, полученные от Организатора СЭД в порядке, установленном настоящими Правилами.

4.3. Порядок признания подлинника Электронного документа.

4.3.1. Все экземпляры Электронного документа, зафиксированные у Организатора СЭД и Участников ЭДО, являются подлинниками данного Электронного документа.

4.3.2. Подлинником Электронного документа считается документ с воспроизведенным содержанием и электронно-цифровой подписью.

4.3.3. Подлинник Электронного документа не существует, если нет ни одного учтенного Организатором СЭД или Участником ЭДО экземпляра данного Электронного документа.

4.3.4. Подлинник Электронного документа не существует, если получение или восстановление экземпляра данного Электронного документа невозможно.

4.3.5. Подлинник Электронного документа не существует, если нет способа установить подлинность электронно-цифровой подписи.

4.3.6. Электронный документ не может иметь копий в электронном виде.

4.3.7. Электронный документ может иметь неограниченное количество экземпляров.

4.4. Порядок формирования копии Электронного документа на бумажном носителе.

4.4.1. Копии Электронного документа на бумажном носителе должны быть заверены собственноручной подписью Уполномоченного представителя Участника ЭДО или Организатора СЭД.

4.4.2. Копии Электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.

4.4.3. Информация, содержащаяся в копии Электронного документа на бумажном носителе, должна быть идентична информации, содержащейся в самом Электронном документе.

5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Этапы Электронного документооборота

ЭДО включает в себя следующие этапы:

- формирование Электронного документа;
- отправка Электронного документа;
- Доставка Электронного документа;
- проверка целостности Электронного документа;
- подтверждение о Доставке Электронного документа;
- отзыв Электронного документа;
- ведение архива Электронных документов;
- создание дополнительных экземпляров Электронного документа;
- создание бумажных копий Электронного документа.

5.2. Порядок формирования Электронного документа и его регистрации.

5.2.1. Электронный документ составляется в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде.

5.2.2. В наименовании сформированного Электронного документа в обязательном порядке должно содержаться указание на тип документа (Справка о стоимости чистых активов, Заявка на приобретение паев, Отчет агента и т.п.), дату документа, наименование инвестиционного фонда (если применимо), номер документа (далее совместно именуемые Реквизиты электронного документа).

5.2.3. Сформированный Электронный документ подписывается электронно-цифровой подписью и зашифровывается; дата и время подписи Электронного документа должны включаться в подписываемый Электронный документ.

5.3. Порядок отправки и Доставки электронного документа

5.3.1. Электронный документ отправляется Отправителем или лицом, уполномоченным на это Отправителем.

5.3.2. Участник ЭДО посредством специального программного модуля, предоставленного Организатором СЭД, подписывает документы ЭЦП и осуществляет их Шифрование.

5.3.3. Отправка Электронного документа Участником ЭДО или Организатором СЭД осуществляется посредством электронной почты стандартными программными средствами, в которых предусмотрена возможность генерировать и возвращать отправителю сообщения о получении письма, либо сообщения об ошибке при Доставке электронного документа в случае, если Электронный документ был отправлен, но не доставлен Получателю. Отправка электронного сообщения, а также подтверждения о получении Электронных документов, осуществляется с адреса электронной почты, указанного в Анкете.

5.3.4. Тема электронного сообщения с вложенным в него Электронным документом должна в обязательном порядке содержать Реквизиты электронного документа.

5.3.5. Отправитель самостоятельно контролирует Доставку электронного сообщения Получателю. После отправки Электронного документа Участник ЭДО обязан удостовериться в отсутствии сбоев при Доставке. В случае сбоя при Доставке Электронный документ не

считается отправленным, а Участник ЭДО должен повторить процедуру подготовки и/или отправки Электронного документа.

5.3.6. Полученный Электронный документ проверяется на целостность, т.е. его Доставку в неискаженном (по отношению к первоначальному) виде, путем расшифрования и обязательной проверки электронно-цифровой подписи. Получателем также проверяется достоверность информации о дате и времени подписания и Шифрования Электронного документа.

5.3.7. В случае невозможности расшифрования Электронного документа, при отрицательном результате проверки целостности Электронного документа и подлинности ЭЦП или при несоответствии информации о дате или времени подписания и Шифрования Электронного документа текущему времени/дате Электронный документ считается не полученным и не подлежит дальнейшей обработке и исполнению. В этом случае Получатель Электронного документа направляет по электронным каналам связи Электронное сообщение, подписанное ЭЦП, об ошибке при расшифровании или проверки целостности или подлинности ЭЦП Электронного документа с указанием Реквизитов электронного документа.

5.3.8. Участник ЭДО должен хранить все полученные и отправленные Электронные сообщения с файлом, содержащим Электронный документ, в течение сроков, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации для хранения соответствующих документов. Участник ЭДО должен принять меры по периодическому резервному копированию полученных и отправленных электронных сообщений с файлом, содержащим Электронный документ

5.4. Порядок отзыва Электронного документа

5.4.1. Отправитель имеет право отозвать отправленный Электронный документ путем отправки Получателю Электронного документа, подписанного ЭЦП Отправителя, с уведомлением об отзыве.

5.4.2. В уведомлении об отзыве указывается основание отзыва Электронного документа, а также Реквизиты электронного документа.

5.4.3. Электронный документ может быть отозван только до начала его исполнения Получателем.

5.4.4. Электронный документ считается отозванным после получения Отправителем подтверждения о получении отправленного уведомления об отзыве электронного документа.

5.5. Порядок учета Электронных документов

5.5.1. Участник ЭДО осуществляет учет Электронных документов путем ведения журнала учета входящих Электронных документов и журнала учета исходящих Электронных документов. Ведение учетных журналов осуществляется с использованием электронной базы данных с возможностью их формирования на бумажных носителях.

5.5.2. Запись в журнале учета входящих Электронных документов должна содержать:

- дата и время получения Электронного документа;
- наименование документа;
- идентификатор Отправителя электронного документа;

5.5.3 Запись в журнале учета исходящих Электронных документов должна содержать:

- наименование документа;
- идентификатор Отправителя электронного документа;
- идентификатор Получателя электронного документа;
- дата и время отправки электронного документа;

5.5.4 Организатор СЭД и Участники ЭДО обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения учетных данных, содержащихся в журналах учета Электронных документов.

5.6 Порядок подтверждения получения Электронного документа

5.6.1. В качестве подтверждения получения Электронного документа не реже чем раз в день (не позднее 18:00) Получатель направляет Отправителю журнал учета входящих Электронных документов Получателя, полученных от Отправителя в текущем дне, подписанный ЭЦП Получателя. В случае если документы были получены в текущем дне после отправки подтверждения, они должны включаться в следующий журнал учета входящих документов.

В случае несоответствия состава документов в журнале учета исходящих Электронных документов, переданных Получателю, с составом документов в журнале учета входящих документов Получателя, переданного в качестве подтверждения получения Электронных документов, Отправитель электронного документа выясняет причину несоответствия и при необходимости незамедлительно осуществляет повторную отправку Электронных документов

5.6.2. В случае получения электронного документа с уведомлением об отзыве, Получатель незамедлительно направляет Отправителю подтверждение о получении этого электронного документа с указанием информации об электронном документе, содержащейся в Журнале учета входящих документов.

5.6.3. Электронный документ считается не полученным, если электронный адрес Отправителя или Получателя не соответствует электронному адресу, указанному в Анкете.

5.7. Порядок ведения архива Электронных документов

5.7.1. Все Электронные документы, сформированные, отправленные и полученные Участниками ЭДО, хранятся в течение сроков, установленных действующим законодательством для соответствующих документов в бумажном виде. Электронные документы, для которых законодательством не установлены сроки их хранения, хранятся в течение 5 (Пяти) лет.

5.7.2. Электронные документы должны храниться в формате, в котором они были получены.

5.7.3. Хранение Электронных документов сопровождается хранением Сертификатов ключей подписи.

5.7.4. Закрытые (секретные) ключи электронно-цифровой подписи хранятся у их владельцев в соответствующем электронном архиве в случае хранения Электронных документов в зашифрованном виде.

5.7.5. При ведении архива Электронных документов, Закрытых (секретных) ключей электронно-цифровой подписи и Сертификатов ключей подписи реализуются принципы резервного копирования и восстановления информации.

5.7.6. Организатор СЭД и Участники ЭДО должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения архивных данных.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В СЭД ЗАО «Райффайзенбанк»

6.1. Общие положения.

6.1.1. В СЭД ЗАО «Райффайзенбанк» используются только сертифицированные ФСБ средства криптографической защиты информации (СКЗИ).

6.1.2. После подписания Участником ЭДО договора о присоединении к настоящим Правилам Организатор СЭД передает ему программное обеспечение, СКЗИ и Ключевые носители для целей использования только в СЭД ЗАО «Райффайзенбанк», а также обеспечивает ключевой информацией, необходимой для работы.

6.1.3. Программное обеспечение, СКЗИ и Ключевые носители, предоставляемые Участнику ЭДО, принадлежат Организатору СЭД и являются его собственностью.

6.1.4. Для обеспечения криптографической защиты информации в СЭД используются СКЗИ с открытым распределением Ключей. При этом каждый Уполномоченный представитель Участника ЭДО имеет свой Закрытый (секретный) ключ электронно-цифровой подписи, а также соответствующий ему Открытый ключ электронно-цифровой подписи, который не является секретным и доступен другим участникам информационного обмена. При формировании Закрытого (секретного) ключа электронно-цифровой подписи с помощью специализированного программного обеспечения одновременно формируется соответствующий ему Открытый ключ электронно-цифровой подписи. После издания в УЦ производится распечатка Сертификата ключа подписи, на которой имеются все атрибуты Открытого ключа. Подписанный Уполномоченным представителем Участника ЭДО и заверенный печатью Сертификат ключа подписи является документом, который подтверждает принадлежность ключа электронно-цифровой подписи Уполномоченному представителю Участника ЭДО. Один экземпляр Сертификата ключа подписи хранится в УЦ.

6.1.5. Для Шифрования информации Отправителю необходим только Открытый ключ Получателя информации. Для цифровой подписи документа необходим только собственный Закрытый (секретный) ключ электронно-цифровой подписи. Для расшифрования информации Получателем используется только собственный Закрытый (секретный) ключ электронно-цифровой подписи Получателя. Для проверки подписи документа необходим только Открытый ключ Отправителя.

6.1.6. Реализованные в СКЗИ алгоритмы Шифрования и подписи гарантируют невозможность восстановления Закрытого (секретного) ключа электронно-цифровой подписи Отправителя по его Открытому ключу, что обеспечивает целостность, подлинность и конфиденциальность переданной Отправителем информации.

6.1.7. Закрытый (секретный) ключ электронно-цифровой подписи Уполномоченного представителя Участника ЭДО находится только на Ключевом носителе, передаваемом Участнику ЭДО.

6.1.8. При работе в СЭД каждый Участник ЭДО использует необходимое количество действующих Криптографических ключей.

6.1.9. Порядок работы с Ключевыми носителями лиц, непосредственно работающих с СКЗИ, определяется самим Участником ЭДО с учетом настоящих Правил.

6.1.10.Ключевая информация, необходимая для работы СКЗИ в СЭД, вырабатывается Оператором Удостоверяющего центра (УЦ). Непосредственная генерация ключей и запись их на носители производится также Оператором УЦ на «Автоматизированном рабочем месте (АРМ) Администратора УЦ». Программное обеспечение ПАК КриптоПро УЦ имеет сертификат соответствия ФСБ и соответствуют требованиям ФСБ России к информационной безопасности класса КС2 УЦ систем ЭДО, предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну, с применением средств электронной цифровой подписи.

6.1.11.Участник ЭДО обязуется выполнять указанные в настоящих Правилах требования

порядка предоставления услуг по криптографической защите, порядка обеспечения информационной безопасности и общих требований к режиму эксплуатации СКЗИ, указанные в п.7 настоящих Правил.

6.1.12.Участник ЭДО обязуется выполнять требования эксплуатационной документации на СКЗИ.

6.1.13.По окончании срока действия договора о присоединении к настоящим Правилам или в случае его расторжения Участник ЭДО обязуется провести деинсталляцию установленного программного обеспечения и СКЗИ и вернуть Организатору СЭД полученные от него лицензии программного обеспечения и СКЗИ и Ключевые носители.

6.2. Порядок предоставления СКЗИ и передачи Криптографических ключей.

6.2.1. Порядок получения СКЗИ и регистрации Уполномоченного представителя Участника ЭДО в УЦ.

6.2.1.1. Для получения СКЗИ Участнику ЭДО необходимо оформить и предоставить Организатору ЭДО Заявку на предоставление программного обеспечения, СКЗИ и ключевых носителей (по форме, указанной в Приложении №6 к настоящим Правилам), а также доверенность на получение программного обеспечения, СКЗИ и ключевых носителей на Уполномоченного представителя Участника ЭДО (по форме, указанной в Приложении №7 к настоящим Правилам).

6.2.1.2. Под регистрацией понимается внесение регистрационной информации о физическом лице, являющемся Уполномоченным представителем Участника ЭДО и намеревающемся получить в УЦ Организатора ЭДО Закрытый (секретный) ключ электронно-цифровой подписи и Сертификат ключа подписи.

6.2.1.3. Регистрация уполномоченного представителя Участника ЭДО осуществляется на основании Заявления на регистрацию (по форме, указанной в Приложении № 8 к настоящим Правилам), составленного в двух экземплярах, при личном прибытии физического лица, проходящего процедуру регистрации в офис Организатора ЭДО.

6.2.1.4. Если Уполномоченный представитель Участника ЭДО не может прибыть в УЦ Организатора ЭДО лично, Заявление на регистрацию может быть принято от уполномоченного Участником ЭДО лица, прибывающего в УЦ лично и действующего на основании доверенности (по форме, указанной в Приложении № 9 к настоящим Правилам).

6.2.1.5. При проведении процедуры регистрации УЦ Организатора ЭДО вправе запросить документы, подтверждающие:

- место регистрации и адрес места жительства Уполномоченного представителя Участника ЭДО;
- сведения, необходимые для идентификации Уполномоченного представителя Участника ЭДО, а именно: фамилию, имя, отчество, наименование документа, удостоверяющего личность, номер этого документа, дату и место его выдачи;
- информацию о должности Уполномоченного представителя Участника ЭДО.

6.2.1.6. При положительном исходе идентификации Уполномоченного представителя Участника ЭДО по паспорту или иному документу, удостоверяющему личность, Оператор УЦ осуществляет регистрацию Уполномоченного Участника ЭДО.

6.2.1.7. При регистрации Уполномоченного представителя Участника ЭДО Оператор УЦ вносит специальную парольную фразу в соответствующий реестр УЦ Организатора ЭДО и передает ее в запечатанном конверте, выполняет действия по внесению иной регистрационной информации в реестры УЦ Организатора ЭДО.

6.2.2. Порядок передачи СКЗИ, изготовления и получения Криптографических ключей и

Сертификатов ключа подписи.

6.2.2.1. Создание Ключа и Сертификата ключа подписи осуществляется УЦ Организатора ЭДО при личном прибытии Владельца сертификата ключа подписи в УЦ Организатора ЭДО на основании следующих документов:

- Заявления на получение ключей и сертификатов ключей подписи (по форме, указанной в Приложении № 10 к настоящим Правилам), подаваемого в двух экземплярах;
- документа, подтверждающего права Уполномоченного представителя Участника ЭДО на подписание определенного типа информации: нотариально заверенной копии учредительных документов или доверенности, выданной на имя Уполномоченного представителя частника ЭДО (по форме, указанной в Приложении №11 к настоящим Правилам), на подписание определенного типа информации в соответствии с Областью действия сертификатов криптографических ключей Пользователя (по форме, указанной в Приложении №12 к настоящим Правилам).

6.2.2.2. В случае если Владелец сертификата ключа подписи не может прибыть в УЦ Организатора ЭДО лично, Заявление на получение ключей и сертификатов ключей подписи может быть принято от уполномоченного Участником ЭДО лица, прибывающего в УЦ Организатора ЭДО лично и действующего на основании доверенности (по форме, указанной в Приложении № 9 к настоящим Правилам).

6.2.2.3. Оператор УЦ выполняет идентификацию Владельца сертификата ключа подписи (или иного должным образом уполномоченного лица) путем установления его личности по паспорту или иному документу, удостоверяющему личность.

6.2.2.4. При положительном исходе идентификации Оператор УЦ принимает документы, подтверждающие соответствующие полномочия, на рассмотрение.

6.2.2.5. УЦ может быть отказано в изготовлении Ключей и Сертификатов ключей подписи в следующих случаях:

- представление Заявления на получение Ключей и сертификатов ключей подписи, не соответствующего требованиям настоящего Порядка;
- несоответствие информации, указанной в Заявлении на получение ключей и сертификатов ключей подписи, информации, содержащейся в документах, представленных вместе с Заявлением на получение ключей и сертификатов ключей подписи;
- отсутствие соответствующих полномочий у лица, представившего Заявление на получение ключей и сертификатов ключей подписи.

6.2.2.6. В случае отказа в изготовлении Ключей и Сертификатов ключей подписи Заявление на получение ключей и сертификатов ключей подписи вместе с приложениями возвращается заявителю с отметкой УЦ Организатора ЭДО о причинах отказа.

6.2.2.7. При принятии положительного решения Оператор УЦ выполняет следующие действия:

- генерирует в соответствии с настоящим Порядком, ключевую пару Владельца сертификата ключа подписи;
- записывает ключевую пару в электронной форме на отчуждаемый Ключевой носитель;
- формирует в электронной форме запрос на выпуск Сертификата ключа подписи и передает Уполномоченному лицу УЦ для изготовления Сертификата ключа подписи.
- после изготовления Сертификата ключа подписи Уполномоченным лицом УЦ

Оператор УЦ записывает Сертификат ключа в электронной форме на отчуждаемый носитель;

- изготавливает два бланка Сертификата ключа подписи (по форме, указанной в Приложении № 13 к настоящим Правилам). Все экземпляры бланка Сертификата ключа подписи на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру изготовления Ключей и Сертификатов ключей подписи (или собственноручной подписью его должным образом уполномоченного лица), а также собственноручной подписью Уполномоченного лица УЦ и печатью УЦ.

6.2.2.8. По окончании выполнения действий, указанных в пункте 6.2.2.7 настоящих Правил, Оператор УЦ выдает:

- Ключи на отчуждаемом Ключевом носителе по Акту формирования и передачи криптографических ключей (по форме, указанной в Приложении №14 к настоящим Правилам). Акт составляется в двух экземплярах по одному для каждой из сторон;
- Сертификат ключа подписи в электронной форме на отчуждаемом носителе электронной информации;
- один экземпляр бланка Сертификата ключа подписи;
- копию Сертификата ключа подписи Уполномоченного лица УЦ в электронном виде на отчуждаемом носителе информации;
- серийные номера лицензий программного обеспечения, СКЗИ, а также ключевые носители по Акту приема - передачи программного обеспечения, СКЗИ и ключевых носителей (Приложение №15 к настоящим Правилам). Акт составляется в двух экземплярах по одному для каждой из сторон.

6.2.2.9. В течение 30 (тридцати) рабочих дней со дня передачи программного обеспечения, СКЗИ и криптографических ключей Участник ЭДО обязан:

- Осуществить инсталляцию и проверку работоспособности программного обеспечения и СКЗИ;
- установить новые Сертификаты ключей подписи в локальные хранилища сертификатов Участника ЭДО;
- произвести сверку параметров выданных Ключей с данными, указанными в Сертификатах ключей подписи;
- предоставить Организатору СЭД подписанный Акт о начале электронного документооборота (по форме, указанной в Приложении №3 к настоящим Правилам).

6.2.2.10. В случае нарушения условий пункта 6.2.2.9 настоящих Правил, а также отсрочки тестовой эксплуатации СЭД Участником ЭДО более чем на 30 (тридцать) дней, Акт о начале электронного документооборота подписывается Организатором ЭДО в одностороннем порядке.

6.2.2.11. По истечении срока действия документа, подтверждающего права Уполномоченного представителя Участника ЭДО на подписание определенного типа информации в СЭД, в случае непредоставления Участником ЭДО документа, подтверждающего новые сроки полномочий Уполномоченного лица Участника ЭДО, Оператор УЦ блокирует криптографический ключ Уполномоченного представителя Участника ЭДО и заносит серийный номер соответствующего ему открытого ключа в список отозванных сертификатов.

6.2.3. Плановая смена Ключей в СЭД

6.2.3.1. Плановая смена Криптографических ключей в СЭД производится один раз в год, поэтому срок действия Криптографических ключей при генерации устанавливается равным одному году.

6.2.3.2. О дате проведения Плановой смены ключей Организатор СЭД уведомляет Участников ЭДО путем направления электронного сообщения не позднее, чем за 10 (Десять) рабочих дней. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО.

6.2.3.3. Старые Криптографические ключи и файлы с ранее действовавшими Открытыми ключами должны сохраняться Участником ЭДО для обеспечения возможности доступа к локальным архивам и проведения процедуры разбора конфликтных ситуаций.

6.2.3.4. Формирование и выдача Участнику ЭДО новых комплектов криптографических ключей осуществляется Организатором СЭД в следующем порядке:

- Участник ЭДО должен направить Организатору СЭД Заявление на получение ключей и сертификатов ключей подписи (по форме, указанной в Приложении №10 к настоящим Правилам) в соответствии с п. 6.2.2.1 настоящих Правил. Новые Криптографические ключи записываются на уже имеющиеся у Участника ЭДО Ключевые носители;
- порядок получения Криптографических ключей Участником ЭДО аналогичен порядку, изложенному в п. 6.2.2 настоящих Правил.

6.2.3.5. В течение 5 (пяти) рабочих дней со дня получения Ключевых носителей и Открытых ключей Участник ЭДО обязан установить новые Сертификаты ключей подписи в локальные хранилища сертификатов Участника ЭДО и произвести сверку параметров новых Ключей с данными, указанными в Сертификатах ключей подписи.

7. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЩИЕ ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ

7.1 Система обеспечения информационной безопасности при взаимодействии Организатора СЭД и Участников ЭДО

7.1.1. С целью защиты информации Организатор СЭД и Участники ЭДО принимают к использованию для осуществления электронной передачи документов в СЭД ЗАО «Райффайзенбанк» СКЗИ КриптоПро CSP, сертифицированное ФСБ. Для выполнения процедуры постановки/снятия/проверки электронно-цифровой подписи и Шифрования/расшифрования Электронных документов используется программное обеспечение КриптоАРМ производства ООО «Цифровые технологии» (далее ПО КриптоАРМ).

7.1.2. Программа для Шифрования и электронной цифровой подписи «КриптоАРМ» предназначена для защиты корпоративной информации, передаваемой по незащищенным каналам связи.

7.1.3. ПО КриптоАРМ обеспечивает следующие функциональные возможности:

Шифрование данных:

- Шифрование данных;
- расшифрование данных.

Электронная цифровая подпись (ЭЦП):

- подпись данных;
- проверка корректности электронной цифровой подписи;

- добавление нескольких подписей к одному документу;
- заверение подписи подписью другого человека;
- два варианта ЭЦП (ЭЦП, отделенная от исходных данных и совмещенная с данными);
- расширенные свойства ЭЦП (время создания подписи, комментарий пользователя и др.).

7.1.4. Организатор ЭДО и Участники ЭДО осуществляют защиту информации, содержащей персональные данные и Конфиденциальную информацию в СЭД.

7.1.5. Соблюдение требований информационной безопасности при организации ЭДО обеспечивает:

- целостность и криптографическую защиту информации;
- защиту информации от несанкционированного доступа.

7.1.6. Система обеспечения информационной безопасности реализуется посредством применения программных средств и организационных мер.

7.1.7. К программным средствам относятся:

- программные средства, используемые для осуществления ЭДО;
- средства аутентификации;
- СКЗИ;
- средства обеспечения безотказной работы, включая антивирусные средства.

7.1.8. К организационным мерам относятся:

- размещение программных средств в помещении с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- допуск только специально обученных и уполномоченных лиц;
- защита от повреждающих внешних воздействий (пожар и т.п.).

7.2. Требования к режиму эксплуатации СКЗИ и Криптографических ключей

7.2.1. Общие требования:

- учет и хранение Ключевых носителей и лицензионных ключей, непосредственная работа с ними поручается руководством Участника ЭДО специально выделенному работнику. Этот работник несет персональную ответственность за сохранность Криптографических ключей и лицензионных ключей;
- все поступающие для использования Криптографические ключи и лицензионные ключи должны браться в организации на поэкземплярный учет (регистрация их выдачи сотрудникам для работы, возврата и уничтожения) в выделенных для этих целей журналах;
- Ключевые носители с записанными на них Криптографическими ключами, лицензионные ключи СКЗИ и эксплуатационная документация должна храниться в хранилищах (металлических шкафах, сейфах, ячейках), оборудованных внутренними замками.

7.2.2. Требования по организационному обеспечению безопасности СКЗИ:

- руководством организации должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ;
- вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством организации с учетом эксплуатационной документации на СКЗИ;
- в организациях должны быть созданы условия, обеспечивающие сохранность

Конфиденциальной информации, обрабатываемой с помощью СКЗИ, а также ключевой информации.

7.2.3. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ:

- размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее именуются Помещения), должны обеспечивать безопасность информации, СКЗИ и Криптографических ключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ неуполномоченными лицами;
- порядок допуска в помещения должен определяться внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации;
- размещение и установка СКЗИ осуществляется в соответствии с требованиями эксплуатационной документации на СКЗИ;
- уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

7.3. Требования по обеспечению безопасности Криптографических ключей.

7.3.1. Криптографические ключи на Ключевых носителях должны храниться в индивидуальных хранилищах (сейфах, металлических шкафах, ячейках) владельцев записанных на них Ключей. В случае хранения Ключевых носителей в совместно используемых хранилищах, они должны храниться в опечатанном виде.

7.3.2. В случае отсутствия у сотрудника, работающего с СКЗИ, индивидуального хранилища Криптографические ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

7.3.3. При нахождении Ключевых носителей вне сейфов, в процессе их использования владельцем записанных на них Ключей, должны быть приняты меры, исключающие возможность несанкционированного доступа к Ключевым носителям.

7.3.4. При использовании Ключевого носителя не допускается:

- снимать несанкционированные копии с Ключевого носителя;
- разглашать содержимое Ключевого носителя;
- передавать Ключевой носитель кому-либо, не являющемуся уполномоченным руководством организации работником;
- выводить Закрытые (секретные) ключи электронно-цифровой подписи, записанные на Ключевом носителе на дисплей, принтер или другие внешние устройства отображения информации;
- вставлять Ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом его работы;
- записывать на Ключевой носитель постороннюю информацию;
- вскрывать оболочку Ключевого носителя.

7.3.5. Закрытые (секретные) ключи электронно-цифровой подписи Владельцев сертификатов ключей подписи записываются при их генерации на отчуждаемые носители ключевой информации.

7.3.6. В качестве отчуждаемых носителей ключевой информации используются только носители, указанные в документации на СКЗИ.

7.3.7. После использования СКЗИ ключевой материал не должен присутствовать в

персональной электронно-вычислительной машине (далее - ПЭВМ).

7.3.8. Вне процесса работы Ключевые носители должны находиться в специально оборудованных металлических шкафах или сейфах.

7.4. Требования к сотрудникам, осуществляющим эксплуатацию и установку СКЗИ.

7.4.1. Руководством организации должны быть назначены сотрудники, ответственные за установку и эксплуатацию СКЗИ.

7.4.2. К работе с СКЗИ допускаются решением руководства организации только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию СКЗИ.

7.4.3. Руководитель организации или уполномоченное им лицо должен иметь представление о возможных угрозах при обработке, передаче и хранении информации, методах и средствах защиты информации.

7.5. Порядок действий при Компрометации Криптографических ключей

7.5.1. Порядок действий Сторон при Компрометации ключей Участника ЭДО

7.5.1.1. К Компрометации криптографических ключей относятся, включая, но не ограничиваясь, следующие случаи:

а. утрата (в том числе хищение) Ключевых носителей;
б. утрата Ключевого носителя с последующим обнаружением;
в. увольнение сотрудника или перевод на другой участок работы сотрудника, имевшего доступ к ключевой информации, с лишением его полномочий на использование ключевой информации;
г. нарушение правил хранения и уничтожения (после окончания срока действия) Закрытого (секретного) ключа;
д. передача ключевой информации по линии связи в открытом виде;
е. возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
ж. нарушение печати на сейфе с Ключевыми носителями;
з. несанкционированное копирование Ключевых носителей;
и. 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.

7.5.1.2. Случаи с «а» по «г», указанные в пункте 7.5.1.1. Правил, относятся к явной Компрометации ключей. Случаи, с «д» по «и», указанные в пункте 7.5.1.1. Правил, и иные случаи Компрометации относятся к неявной Компрометации ключа и требуют специального рассмотрения Участником ЭДО в каждом конкретном случае.

7.5.1.3. При неявной Компрометации ключа, в случае если Участник ЭДО принимает решение о наличии факта Компрометации ключа, он действует в соответствии с пунктом 7.5.1.4 и пунктом 7.5.1.5 настоящих Правил. В противном случае Участник ЭДО продолжает использование Криптографического ключа.

7.5.1.4. При Компрометации криптографических ключей Участник ЭДО, являющийся

Владельцем сертификатов ключей подписи, прекращает обмен Электронными документами с использованием скомпрометированных ключей.

7.5.1.5. В случае возникновения Компрометации криптографических ключей Участник ЭДО обязан незамедлительно уведомить об этом Оператора УЦ для осуществления отзыва Сертификатов ключей подписи скомпрометированных Ключей. Для этого уполномоченное лицо Участника ЭДО, указанное в Анкете Участника ЭДО, должно связаться с Оператором УЦ и назвать себя, назвать полное наименование организации Участника ЭДО, сообщить пароль и сообщить о факте Компрометации ключей. После этого Участник ЭДО обязан в течение одного рабочего дня предоставить Организатору СЭД письменное Заявление на аннулирование (отзыв) криптографических ключей (по форме, указанной в Приложении №16 к настоящим Правилам), оформленное в двух экземплярах и заверенное собственноручной подписью Владельца сертификата ключа подписи и (или) подписью единоличного исполнительного органа соответствующего Участника ЭДО.

7.5.1.6. Датой и временем Компрометации криптографических ключей считается дата и время получения Организатором СЭД Уведомления о факте Компрометации криптографических ключей.

7.5.1.7. При получении Электронного документа, подписанного отозванным (аннулированным) ключом электронно-цифровой подписи данный электронный документ считается неполученным.

7.5.1.8. Криптографический ключ считается отозванным (аннулированным) с даты занесения серийного номера соответствующего ему Открытого ключа в список отозванных сертификатов.

7.5.1.9. Получив сообщение о факте Компрометации криптографических ключей Участника ЭДО, Уполномоченное лицо УЦ должно убедиться в его достоверности в соответствии с пунктом 7.4.1.2. и незамедлительно заблокировать Ключи Участника ЭДО в СЭД (пометить их как скомпрометированные).

7.5.1.10. Организатор СЭД предоставляет Участнику ЭДО новый Криптографический ключ в соответствии с порядком, указанным в п. 6.2 настоящих Правил после получения от Участника ЭДО всех документов, необходимых для выпуска нового Криптографического ключа. Новый криптографический ключ записывается на уже имеющийся у Участника ЭДО Ключевой носитель.

7.5.1.11. Криптографический ключ записывается на новый Ключевой носитель в случае невозможности использования ранее переданных Участнику ЭДО Ключевых носителей (включая, но не ограничиваясь, случаями утраты ключевого носителя, выхода из строя магнитного носителя).

7.5.1.12. Организатор СЭД предоставляет Участнику ЭДО криптографический ключ, записанный на новый Ключевой носитель, в соответствии с порядком, указанным в п. 6.2 настоящих Правил, после получения от Участника ЭДО всех документов, необходимых для выпуска нового криптографического ключа и получения нового Ключевого носителя.

7.5.2. Порядок действий Сторон при Компрометации ключей Уполномоченного лица УЦ

7.5.2.1 В случае Компрометации криптографических ключей Уполномоченного лица УЦ работа СЭД приостанавливается на срок, необходимый для формирования новых Криптографических ключей Уполномоченного лица УЦ и выдачи Участникам ЭДО новых Криптографических ключей.

7.5.2.2 Оповещение Участников ЭДО производится путем уведомления уполномоченных лиц Участников ЭДО, указанных в Анкетах.

8. СИСТЕМА МЕР УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Виды рисков, связанных с осуществлением ЭДО в рамках СЭД

8.1.1. Правовые риски – риски возникновения конфликтных ситуаций, вызванных правовой неурегулированностью вопросов применения электронно-цифровой подписи и отношений Участников ЭДО.

8.1.2. Организационные риски – риски необеспечения (ненадлежащего обеспечения) ЭДО вследствие неэффективности СЭД.

8.1.3. Технологические риски – риски необеспечения (ненадлежащего обеспечения) порядка осуществления ЭДО вследствие неэффективности и/или неадекватности технологий, порядка и способов осуществления ЭДО.

8.1.4. Операционные риски – риски возникновения нарушений при осуществлении ЭДО вследствие ненадлежащих действий сотрудников, ненадлежащего функционирования используемых СКЗИ и иного аппаратно-программного обеспечения.

8.1.5. Криминальные риски – риски совершения сотрудниками Участников ЭДО, иными лицами, умышленных действий в целях неправомерного получения и использования Конфиденциальной информации, связанной с осуществлением ЭДО, а также нарушения деятельности Участников ЭДО.

8.1.6. Форс-мажорные риски – риски нарушения деятельности Участников ЭДО, целостности СЭД, вследствие возникновения непредотвратимых (форс-мажорных) чрезвычайных ситуаций техногенного, природного и социального характера.

8.2. Меры снижения правовых рисков, связанных с осуществлением ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.2.1. Обеспечение соответствия СКЗИ, используемых при осуществлении ЭДО, требованиям законодательства Российской Федерации (Организатором СЭД).

8.2.2. Обеспечение признания Участниками ЭДО равнозначности ЭЦП и собственноручной подписи (Организатором СЭД).

8.2.3. Установление подлинности электронно-цифровой подписи (Организатором СЭД).

8.2.4. Установление порядка разрешения конфликтов, связанных с использованием ЭДО (Организатором СЭД).

8.3. Меры снижения организационных рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.3.1. Установление прав и обязанностей Участников ЭДО, связанных с осуществлением ЭДО (Организатором СЭД).

8.3.2. Установление функциональных обязанностей подразделений Организатора СЭД, принимающих участие в осуществлении ЭДО (Организатором СЭД).

8.4. Меры снижения технологических рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.4.1. Установление требований к назначению и составу СКЗИ, используемых при осуществлении ЭДО (Организатором СЭД).

8.4.2. Обеспечение использования Участниками ЭДО СКЗИ при осуществлении ЭДО

(Организатором СЭД).

8.4.3. Обеспечение однозначной идентификации Владельца сертификата ключа подписи, уникальности регистрационной информации о Владельце сертификата ключа подписи (Организатором СЭД).

8.4.4. Обеспечение Участниками ЭДО и Организатором СЭД целостности СЭД, регистрации отправленных и полученных Электронных документов, хранению оправленных и полученных Электронных документов.

8.4.5. Установление требований к порядку осуществления ЭДО Участниками ЭДО (Организатором СЭД).

8.4.6. Обеспечение исполнения требований к форматам и реквизитам электронного документа электронного документа (Организатором СЭД).

8.4.7. Определение порядка действий Участников ЭДО (Организатором СЭД) по формированию, Доставке электронного документа, а также его отзыву.

8.4.8. Определение порядка действий Участников ЭДО (Организатором СЭД) по проверке действительности и области действия электронно-цифровой подписи, подлинности, целостности электронного документа и его соответствия установленным форматам.

8.5. Меры снижения операционных рисков ЭДО, применяемые в СЭД

8.5.1. Разделение полномочий и служебных обязанностей сотрудников Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.2. Осуществление контроля за надлежащим исполнением сотрудниками Участников ЭДО и Организатора СЭД своих служебных обязанностей, связанных с осуществлением ЭДО.

8.5.3. Определение порядка выявления ошибок (ошибочных действий), совершенных сотрудниками Участников ЭДО и Организатора СЭД и порядка их устранения.

8.5.4. Установление квалификационных требований к сотрудникам (руководителям подразделений) Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.5. Определение порядка обнаружения и устранения отказов, сбоев, нарушений работы СКЗИ, используемых Участниками ЭДО при осуществлении ЭДО.

8.5.6. Установление требований к техническому сопровождению, замене вышедших из строя СКЗИ Участников ЭДО (Организатором СЭД).

8.6. Меры снижения криминальных рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.6.1. Установление требований (Организатором СЭД) по обеспечению Участниками ЭДО защиты Конфиденциальной информации, связанной с осуществлением ЭДО, от несанкционированного доступа.

8.6.2. Установление требований (Участником ЭДО) по обеспечению Владельцами сертификатов ключей подписи сохранности в тайне Закрытых (секретных) ключей электронно-цифровой подписи.

8.6.3. Определение порядка действий Владельцев сертификатов ключей подписи (Организатором СЭД, Участниками ЭДО) в случае Компрометации Закрытых (секретных) ключей электронно-цифровой подписи.

8.6.4. Определение порядка (Организатором СЭД) расследования случаев неправомерного предоставления и/или использования Конфиденциальной информации, неисполнения (ненадлежащего исполнения) своих служебных обязанностей сотрудниками Участников ЭДО и Организатора СЭД.

8.7. Меры снижения форс-мажорных рисков ЭДО, применяемые в СЭД

8.7.1. Обеспечение Участниками ЭДО и Организатором СЭД целостности ЭДО, защиты Конфиденциальной информации, связанной с осуществлением ЭДО, в случае возникновения чрезвычайных ситуаций.

8.7.2. Определение порядка действий сотрудников Участников ЭДО и Организатора СЭД в случае возникновения чрезвычайных ситуаций.

8.7.3. Применение Участниками ЭДО и Организатором СЭД резервных источников питания, систем бесперебойного питания, средств безаварийного завершения работы.

8.7.4. Применение Участниками ЭДО и Организатором СЭД средств защиты от поражения компьютерными вирусами и вредоносными программами.

8.9. Компенсационные инструменты, применяемые для покрытия убытков от реализации рисков ЭДО.

8.9.1. Собственные средства Участников ЭДО и Организатора СЭД.

8.10. Управление рисками электронного документооборота

8.10.1. Ответственным за управление рисками ЭДО в СЭД является Организатор СЭД.

8.10.2. Основными функциями Организатора СЭД в области управления рисками ЭДО являются:

- анализ текущей и планируемой деятельности Организатора СЭД с целью выявления новых рисков ЭДО, установление источников и причин их реализации, оценка последствий реализации выявленных рисков;
- контроль за практическим применением Организатором СЭД мер, препятствующих реализации рисков ЭДО;
- мониторинг событий, способных привести к реализации рисков ЭДО, анализ эффективности применяемых Организатором СЭД способов снижения рисков;
- расследование случаев реализации рисков ЭДО, установление причин несрабатывания, применяемых Организатором СЭД способов снижения рисков;
- оценка эффективности сформированных Организатором СЭД компенсационных инструментов, применяемых при покрытии убытков, в случае реализации рисков ЭДО;
- разработка предложений по повышению эффективности системы мер снижения рисков ЭДО.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ

9.1. Возникновение конфликтов

9.1.1. В случае возникновения конфликтов при использовании Электронных документов в СЭД, в частности, спора между Участниками ЭДО в отношении Авторства электронных документов, подлинности или целостности Электронных документов, подписанных электронно-цифровой подписью, применяется порядок разрешения конфликтов, предусмотренный настоящими Правилами.

9.1.2. При возникновении конфликта Участник ЭДО, оспаривающий подлинность,

целостность или Авторство электронного документа в СЭД, извещает Организатора СЭД об этом событии любым способом, позволяющим однозначно установить Отправителя.

9.2.. Порядок разрешения конфликтных ситуаций, связанных с получением или неполучением Электронного документа, подписанного ЭЦП.

9.2.1. При возникновении между Участниками ЭДО (далее - Стороны) конфликтов и разногласий, связанных с не поступлением Электронного документа подписанного ЭЦП, поступлением документа подписанного ЭЦП с отрицательным результатом проверки Стороны создают комиссию для претензионного урегулирования спорной ситуации. Комиссия создается по инициативе одной из Сторон в течение четырнадцати календарных дней с даты уведомления официальным письмом инициирующей создание данной комиссии стороной вторую сторону о необходимости претензионного урегулирования спорной ситуации.

9.2.2. В состав комиссии должно входить равное количество представителей от каждой из Сторон. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Состав комиссии должен быть зафиксирован в Акте, который является итоговым документом, отражающим результаты работы комиссии. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Срок работы комиссии составляет не более пяти рабочих дней. При необходимости этот срок может быть увеличен до одного месяца.

9.2.3. Стороны способствуют работе комиссии и не допускают отказа от предоставления необходимых документов.

9.2.4. Комиссия определяет корректность или некорректность ЭЦП спорного Электронного документа с помощью процедуры технической экспертизы, которая проводится в соответствии с нижеследующим порядком:

9.2.5. Комиссия получает и устанавливает необходимое для работы программное обеспечение.

9.2.6. Стороны предъявляют комиссии:

- свою электронную архивную копию спорного Электронного документа с ЭЦП;
- свою электронную архивную копию Открытого ключа, предназначенного для проверки ЭЦП спорного Электронного документа;
- свою архивную копию распечатки Сертификата ключа подписи, заверенную обеими Сторонами;
- свой экземпляр Уведомления об отмене действия ключа ЭЦП (при наличии);

9.2.7. В случае не предъявления комиссии одной из Сторон какого-либо из вышеперечисленных документов к рассмотрению принимается экземпляр указанного документа, представленный другой Стороной.

9.2.8. Комиссия устанавливает идентичность значений электронной архивной копии Открытого ключа, с помощью которого проверялась ЭЦП спорного Электронного документа, архивной копии распечатки соответствующего Сертификата ключа подписи.

9.2.9. В случае неидентичности хотя бы одного из значений указанного Открытого ключа электронная цифровая подпись спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершенной.

9.2.10. В случае наличия Заявления на аннулирование (отзыв) криптографических ключей, предназначенного для проверки ЭЦП спорного Электронного документа, комиссия устанавливает идентичность значений Открытого ключа, которые содержатся в электронной архивной копии ключа и в архивной копии Заявления на аннулирование (отзыв) криптографических ключей, а также дату отзыва (аннулирования) Ключа и дату регистрации этого заявления. В случае идентичности указанных значений Открытого ключа и если Электронный документ подписан ЭЦП позже даты отзыва (аннулирования) ключа и даты

регистрации Заявления на аннулирование (отзыв) криптографических ключей, ЭЦП спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершённой.

9.2.11. Комиссия с помощью соответствующего программного обеспечения криптографической защиты производит проверку ЭЦП копии спорного Электронного документа с использованием электронной архивной копии Открытого ключа. После установления комиссией корректности или некорректности ЭЦП спорного Электронного документа процедура технической экспертизы считается завершённой.

9.2.12. По итогам работы комиссии составляется Акт, в котором в обязательном порядке отражаются:

- установленные обстоятельства;
- действия членов комиссии;
- выводы комиссии;
- основания для формирования выводов.

9.2.13. Составленный комиссией Акт утверждается Сторонами и является основанием для принятия Сторонами окончательного решения в рамках претензионного урегулирования спорной ситуации. Акт составляется в необходимом количестве экземпляров по одному для каждой из сторон.

9.2.14. В случае если Стороны в рамках претензионного урегулирования спорной ситуации пришли к взаимоприемлемому соглашению, то они в течение четырнадцати календарных дней с даты окончания работы комиссии составляют соответствующий двусторонний Акт, условия которого являются обязательными для выполнения каждой из Сторон.

9.2.15. В случае если Стороны в рамках претензионного урегулирования спорной ситуации не пришли к взаимоприемлемому соглашению, то заинтересованная Сторона вправе обратиться в суд и в качестве доказательства в судебном споре обязана представить Акт, составленный в соответствии с настоящим Порядком. Представленный в суд Акт имеет равную силу с другими доказательствами, представленными Сторонами.

9.3. Согласительный порядок разрешения конфликтов

9.3.1. Все конфликтные ситуации, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, Стороны будут стремиться разрешить путем переговоров.

9.3.2. В случае, если конфликтная ситуация не урегулирована в процессе переговоров и конфликтная ситуация содержит признаки дисциплинарных нарушений, стороны вправе обратиться в Дисциплинарный Комитет ПАРТАД, для разрешения конфликтной ситуации в соответствии с Кодексом мер дисциплинарного воздействия ПАРТАД.

10. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ ЭДО

10.1. Настоящие Правила прекращают свое действие на основании решения исполнительного органа Организатора СЭД.

10.2. Прекращение действия настоящих Правил и приложений к ним не влияет на юридическую силу и действительность Электронных документов, которыми Организатор СЭД и Участники ЭДО обменивались до прекращения действия настоящих Правил и приложений к ним.

11. ПРИЛОЖЕНИЯ

11.1. Приложение № 1 «Договор о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк»
11.2. Приложение № 2 «Форматы электронных документов, используемые в системе электронного документооборота ЗАО «Райффайзенбанк»
11.3. Приложение № 3 «Акт о начале электронного документооборота»
11.4. Приложение № 4 «Анкета Участника ЭДО»
11.5. Приложение № 5 «Анкета Организатора СЭД»
11.6. Приложение № 6 «Заявка на предоставление программного обеспечения, СКЗИ и ключевых носителей»
11.7. Приложение № 7 «Доверенность (СКЗИ)»
11.8. Приложение № 8 «Заявление на регистрацию Пользователя в Удостоверяющем центре»
11.9. Приложение № 9 «Заявление на получение ключей и сертификатов ключей Пользователя Удостоверяющего центра»
11.10. Приложение №10 «Доверенность на подпись информации в СЭД»
11.11. Приложение № 11 «Область действия сертификатов криптографических ключей пользователя»
11.12. Приложение № 12 «Доверенность (ключи)»
11.13. Приложение № 13 «Сертификат открытого ключа»
11.14. Приложение № 14 «Акт формирования и передачи криптографических ключей»
11.15. Приложение № 15 «Акт приема-передачи программного обеспечения, СКЗИ и криптографических ключей»
11.16. Приложение № 16 «Заявление на аннулирование (отзыв) криптографических ключей»

Приложение №1
к Правилам электронного документооборота Специализированного
депозитария ЗАО «Райффайзенбанк»

ДОГОВОР №
о присоединении к Правилам электронного документооборота

ЗАО «Райффайзенбанк»

г. Москва «__ » _____200_ года

Закрытое акционерное общество «Райффайзенбанк» (далее именуется Организатор СЭД), в лице _____, действующего на основании _____, с одной стороны, и_____ (далее именуется Участник ЭДО), в лице_____, действующего на основании_____, с другой стороны, далее совместно именуемые «Стороны», а по отдельности – «Сторона», заключили настоящий Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Настоящий Договор определяет взаимные права и обязанности Организатора СЭД и Участника ЭДО в связи с осуществлением электронного документооборота в соответствии с Правилами электронного документооборота ЗАО «Райффайзенбанк» (далее именуются Правила).

1.2. В силу настоящего Договора Участник ЭДО присоединяется к системе электронного документооборота ЗАО «Райффайзенбанк» (далее именуется СЭД), организованной и осуществляемой в соответствии с Правилами, и подтверждает наличие юридической силы документов, отправляемых и получаемых по СЭД.

1.3. Участник ЭДО принимает порядок и условия электронного документооборота путем присоединения к Правилам в целом.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Для обеспечения конфиденциальности и подлинности электронных документов Участник ЭДО использует сертифицированные в установленном законодательством порядке средства криптографической защиты информации (далее именуются СКЗИ).

2.2. Стороны признают использование СКЗИ достаточным для обеспечения конфиденциальности и целостности информации, защиты от несанкционированного доступа, Подтверждения подлинности электронно-цифровой подписи и Авторства электронных документов, а также невозможности её фальсификации.

2.3. Особенности взаимодействия Участника ЭДО и Организатора СЭД при обмене электронными документами в СЭД могут быть определены дополнительно в соглашении Сторон.

3. ПРАВА ОРГАНИЗАТОРА СЭД

3.1. Организатор СЭД осуществляет все права, вытекающие из Правил, в том числе, не ограничиваясь:

- в одностороннем порядке вносить изменения в Правила, в том числе путем утверждения новой редакции Правил;
- требовать от Участника ЭДО осуществления электронного документооборота в рамках СЭД в соответствии с Правилами;
- в любой момент потребовать от Участника ЭДО предоставления документов на бумажном носителе, оформленных в соответствии с требованиями действующего законодательства Российской Федерации, соответствующих полученным от Участника ЭДО электронным документам;

- принимать меры, направленные на преодоление чрезвычайных ситуаций, в соответствии с Правилами;
- требовать от Участника ЭДО совершения действий или воздержания от совершения действий в связи с осуществлением мер для преодоления чрезвычайных ситуаций;
- отказать в предоставлении услуг в СЭД в случае неисполнения или ненадлежащего исполнения Участником ЭДО своих обязанностей;
- отказать в предоставлении услуг в СЭД в случае нарушения Участником ЭДО установленного Правилами порядка разрешения конфликтных ситуаций и споров;
- предоставлять копии сертификатов ключей в электронной форме, находящихся в реестре, всем Участникам ЭДО;
- отказать в предоставлении услуг по регистрации с обязательным указанием причины отказа;
- отказать в изготовлении ключей и сертификата ключа с обязательным указанием причины отказа;
- отозвать (аннулировать) сертификат ключа в случае установленного факта Компрометации соответствующего закрытого ключа с обязательным указанием причины;
- осуществлять иные права, предусмотренные Правилами.

4. ОБЯЗАННОСТИ ОРГАНИЗАТОРА СЭД

4.1. Организатор СЭД обязуется исполнять Правила, в том числе следующие обязанности:

- не позднее, чем за 5 (Пять) рабочих дней до вступления в силу изменений в Правила ЭДО либо Правил ЭДО в новой редакции, извещать Участника ЭДО о таких изменениях в соответствии с требованиями Правил ЭДО;
- после выполнения Участником ЭДО всех действий, необходимых для допуска к осуществлению электронного документооборота в соответствии с Правилами, обеспечить Участнику ЭДО допуск к осуществлению электронного документооборота;
- предоставлять Участнику ЭДО необходимые для осуществления электронного документооборота программное и информационное обеспечение;
- соблюдать конфиденциальность информации, полученной Организатором СЭД от Участника ЭДО в связи с выполнением им своих обязанностей;
- своевременно оповещать Участника ЭДО в случае Компрометации криптографических ключей Организатора СЭД в соответствии с Правилами ЭДО;
- в случае Компрометации криптографических ключей Участника ЭДО заблокировать криптографические ключи Участника ЭДО до завершения внеплановой смены криптографических ключей;
- обеспечивать сохранность и конфиденциальность информации, доверенной ему Участником ЭДО в ходе практической деятельности в рамках настоящего договора, в соответствии с действующим законодательством;
- использовать закрытый ключ Уполномоченного лица УЦ для подписи издаваемых им сертификатов ключей и списков отозванных сертификатов;
- обеспечивать уникальность регистрационной информации, используемой для идентификации владельцев сертификатов ключей подписи;
- обеспечивать секретность изготовленного закрытого ключа;

- обеспечивать уникальность серийных номеров и значений открытых ключей в изготовляемых сертификатах ключей.

5. ПРАВА УЧАСТНИКА ЭДО

5.1. Участник ЭДО в соответствии с Правилами осуществляет следующие права:

- участвовать в СЭД в соответствии с Правилами;
- на основании имеющихся у Организатора СЭД лицензий ФСБ использовать в СЭД сертифицированные ФСБ шифровальные средства без получения собственной лицензии;
- после выполнения всех действий, необходимых для допуска к осуществлению электронного документооборота в соответствии с Правилами, осуществлять электронный документооборот;
- требовать от Организатора СЭД организации работы с криптографическими ключами Участника ЭДО в объеме и в соответствии с порядком, определяемым Правилами;
- осуществлять иные права, предусмотренные Правилами.

6. ОБЯЗАННОСТИ УЧАСТНИКА ЭДО

6.1. Участник ЭДО обязуется исполнять Правила, в том числе своевременно и в полном объеме выполнять следующие обязанности:

- исполнять требования, установленные Правилами;
- использовать необходимые для осуществления электронного документооборота, программное и информационное обеспечение, а также поддерживать их в работоспособном состоянии;
- выполнять все действия, необходимые для получения допуска к осуществлению электронного документооборота в соответствии с Правилами;
- осуществлять регистрацию открытых криптографических ключей, используемых в СЭД, своевременно направлять Организатору СЭД запрос на продление сертификата ключа подписи, своевременно уведомлять Организатора СЭД о Компрометации зарегистрированных ключей;
- осуществлять электронный документооборот в соответствии с Правилами;
- соблюдать организационно-технические требования по обеспечению безопасности информации, установленные в Правилах;
- использовать предоставленные шифровальные средства только в системе электронного документооборота Организатора СЭД без права их продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов исполнительной власти за соблюдением требований и условий осуществления лицензируемой деятельности до окончания срока действия настоящего договора;
- использовать полученные у Организатора СЭД программно-технические средства только для целей осуществления электронного документооборота в рамках СЭД, не передавать без письменного согласия Организатора СЭД данные средства третьим лицам, возвратить их по первому требованию Организатора СЭД, включая резервные копии программных средств;
- не производить декомпиляцию, модификацию программных средств, не совершать относительно указанных программно-технических средств других действий, нарушающих действующее законодательство;
- не совершать действий, способных привести к нарушению целостности СЭД, а

также незамедлительно сообщать Организатору СЭД о ставших известными Участнику ЭДО действиях третьих лиц, направленных на, или способные привести к нарушению целостности СЭД;

- соблюдать конфиденциальность информации, полученной в процессе обмена электронными документами с Организатором СЭД;
- по требованию Организатора СЭД предоставлять документы на бумажном носителе, оформленные в соответствии с требованиями действующего законодательства Российской Федерации, соответствующие представленным Организатору СЭД электронным документам;
- обеспечивать сохранность и целостность программного обеспечения и СКЗИ;
- немедленно извещать Организатора СЭД в случае Компрометации криптографических ключей Участника ЭДО в соответствии с Правилами;
- незамедлительно сообщать Организатору СЭД о ставших известными Участнику ЭДО попытках третьих лиц совершить действия, направленные на нарушение целостности СЭД;
- соблюдать порядок разрешения конфликтных ситуаций и споров, установленный Правилами.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. В случае нарушения условий настоящего договора Стороны несут ответственность, предусмотренную действующим законодательством Российской Федерации.

8.2. Стороны несут ответственность за действия своих сотрудников, а также иных лиц, получивших или имеющих доступ (независимо от того, был ли этот доступ прямо санкционирован Стороной или произошел без ее ведома) к используемым ими аппаратным средствам, программному, информационному обеспечению, криптографическим ключам и иным средствам, обеспечивающим электронный документооборот в соответствии с Правилами, как за свои собственные.

8.3. В случае неисполнения или ненадлежащего исполнения своих обязательств по настоящему договору одной из Сторон, другая Сторона имеет право потребовать от виновной Стороны исполнения принятых на себя обязательств.

9. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

9.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему договору, если исполнение или надлежащее исполнение оказалось невозможным вследствие обстоятельств непреодолимой силы. К таким обстоятельствам относятся: стихийные бедствия, массовые беспорядки, запретительные действия властей и иные обстоятельства, наступление или прекращение действий которых не зависит от действий (бездействия) Сторон.

9.2. О наступлении обстоятельств непреодолимой силы Сторона обязана в двухдневный срок уведомить другую Сторону любым способом (с использование любого вида связи). Сторона, исполнение или надлежащее исполнение обязательств которой оказалось невозможным вследствие непреодолимой силы, не может быть освобождена от ответственности по данному основанию, в случае, если не уведомит об этом другую Сторону в указанный срок.

9.3. Факт наступления форс-мажорных обстоятельств должен быть подтвержден

заинтересованной Стороной путем предоставления соответствующего документа, выданного компетентным органом.

10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

10.1. Все конфликтные ситуации, которые могут возникнуть в связи с применением, нарушением, толкованием настоящего договора, признанием недействительными настоящего договора или его части, Стороны будут стремиться разрешить путем переговоров.

10.2. В случае, если конфликтная ситуация не урегулирована в процессе переговоров и конфликтная ситуация содержит признаки дисциплинарных нарушений, Стороны вправе обратиться в Дисциплинарный Комитет ПАРТАД, для разрешения конфликтной ситуации в соответствии с Кодексом мер дисциплинарного воздействия ПАРТАД.

10.3. Все гражданские споры, которые могут возникнуть в связи с применением, нарушением, толкованием настоящего договора, признанием недействительным настоящего договора или его части, подлежат разрешению в Арбитражном суде г.Москвы.

11. СРОК ДЕЙСТВИЯ ДОГОВОРА

11.1. Настоящий договор заключен сроком на 1 (один) год и вступает в силу со дня его подписания Сторонами.

11.2. Если ни одна из Сторон за 30 (тридцать) календарных дней до истечения срока действия настоящего договора не заявит о намерении его расторгнуть, настоящий договор пролонгируется на срок 1 (один) год на тех же условиях.

11.3. Любая из Сторон по настоящему договору вправе в одностороннем порядке расторгнуть настоящий договор, письменно уведомив другую Сторону.

11.4. Настоящий договор считается расторгнутым на следующий рабочий день после получения одной из Сторон письменного уведомления другой Стороны о расторжении настоящего договора.

12. ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ

12.1. Все дополнения и изменения к настоящему договору действительны в том случае, если они оформлены в письменном виде и подписаны Сторонами.

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Расторжение настоящего договора не влияет на действительность документов, подписанных ЭЦП каждой из Сторон до даты расторжения настоящего договора.

13.2. Настоящий договор составлен в 2 (двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

13.3. Термины, определение которых не приведено в тексте настоящего Договора, определяются в соответствии с Правилами.

14. АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН:

Организатор СЭД: ЗАО «Райффайзенбанк»
Адрес местонахождения: 129090, Москва, ул.Троицкая, д.17, стр.1
Почтовый адрес: 129090, Москва, ул.Троицкая, д.17, стр.1
Банковские реквизиты:
расчетный счет: 47422810200005013925
ИНН: 7744000302, корр. счет № 30101810200000000700 в ОПЕРУ Московского ГТУ Банка России, БИК 044525700.
ОГРН: 1027739326449

Участник ЭДО:
Адрес местонахождения:
Почтовый адрес:
Банковские реквизиты:
ИНН:
ОГРН:

Подписи Сторон:

От Участника ЭДО:

_____/_____/
М.П.

От Организатора СЭД:

_____ /_____/
М.П.

Приложение № 2
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Форматы электронного документооборота.

Структура формализованного электронного документа должна строго соответствовать структуре описанных ниже форматов электронных документов. В случае если какие-либо данные отсутствуют в оригинале документа, соответствующие поля в переданных электронных документах не заполняются.

1. Первичные документы, принимаемые от физических и юридических лиц в отношении паевых инвестиционных фондов.

Вариант 1.

Данные в файле должны соответствовать структуре, описанной в Таблице 1.1, Таблице 1.2., и предоставляться в формате xls (Пример: имя_файла.xls). Записи передаются в виде строк.

Таблица 1.1 Анкетные данные

Поле	Формат	Описание
HNUM	integer	Идентификационный номер заявителя
branchname	character (20)	Наименование (код) филиала, принявшего документ
CATEGORY	smallint	Налоговый статус[1]
SURNAME	character (50)	Фамилия
NAME	character (50)	Имя
PATRONYMIC	character (50)	Отчество
DATEOFBIRTH	date	Дата рождения
CITIZENSHIP	character (50)	Гражданство
RESIDENTTYPE	character (1)	Налоговый статус[2]
PASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность
PASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность
ISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность
ISSUEDBY	character (50)	Орган выдачи документа, удостоверяющего личность
LEGALADDRESS	character (150)	Адрес регистрации
MAILINGINDEX	character (6)	Почтовый индекс
MAILINGREGION	varchar (500)	Регион
MAILINGCITY	varchar(100)	Город
MAILINGSTREET	varchar(100)	Улица
MAILINGBUILDING	varchar(50)	Дом
MAILINGFLAT	varchar(5)	Квартира
MAILINGEXTBOX	varchar(100)	Абонентский ящик
PHONE	character (150)	Телефон
PHONECELL	character (150)	Мобильный телефон
TIN	character (12)	ИНН
BANKNAME	character (40)	Наименование банка
BANKLOCATION	character (50)	Город банка

[1] Принимает значения: «1»-физическое лицо; «2»-юридическое лицо.
[2] Принимает значения: "R" - резидент;"N" – нерезидент.

PERSBANKACCOUNT	character (20)	Расчетный счет
BANKBIC	character (9)	БИК банка
BANKTIN	character (10)	ИНН банка
BANKCORRACCOUNT	character (20)	Корреспондентский счет банка
CAPABILITY	varchar(50)	Дееспособность
EMAIL	varchar(100)	Адрес электронной почты
PHONEEMP	varchar(150)	Рабочий телефон
RINUM	smallint	Способ получения информации и выписок из реестра (код)[3]
RINAMERUS	varchar(100)	Способ получения информации и выписок из реестра
DOC_TYPE	varchar (505)	Тип документа, удостоверяющего личность
LASTMODIFIED	timestamp	Дата принятия анкеты
ntuser	character (50)	ФИО лица, принявшего документ
zpSURNAME	character (50)	Фамилия законного представителя
zpNAME	character (50)	Имя законного представителя
zpPATRONYMIC	character (50)	Отчество законного представителя
zpDocType	const	Тип документа, удостоверяющего личность, законного представителя
zpPASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность, законного представителя
zpPASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность, законного представителя
zpISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность, законного представителя
zpISSUEDBY	character (150)	Орган выдачи документа, удостоверяющего личность, законного представителя
zpStatus	smallint	Статус законного представителя[4]
zpDOCUMENTTYPE	smallint	Тип документа - основания законного представителя
zpDOCNUM	varchar (15)	Номер документа-основания законного представителя
zpDOCDATE	date	Дата выдачи документа-основания законного представителя
zpDOCISSUEDBY	character (50)	Орган выдачи документа-основания законного представителя
upFIO	varchar (150)	ФИО уполномоченного представителя
upDocType	varchar (50)	Тип документа, удостоверяющего личность, уполномоченного представителя
upPASSPORTSERIES	varchar (50)	Серия документа, удостоверяющего личность, уполномоченного представителя
upPASSPORTNUMBER	varchar (50)	Номер документа, удостоверяющего личность, уполномоченного представителя
upISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность, уполномоченного представителя
upISSUEDBY	varchar (150)	Орган выдачи документа, удостоверяющего личность, уполномоченного представителя
upDOCNUM	varchar (25)	Номер доверенности
upDOCDATE	date	Дата выдачи доверенности

[3] Принимает значения:
«1» - в месте подачи документов; «2» - у лица, осуществляющего ведение Реестра; «3» - по почте
[4] Принимает значения: «1» - Отец; «2» - Мать; «3» - Усыновитель; «4» - Попечитель; «5» - Опекун

Таблица 1.2 Данные документов

Поле	Формат	Описание
ID	integer	Идентификационный номер документа
RCOD	varchar(32)	Номер документа
RDATE	timestamp	Дата принятия документа
DTNAMERUS	varchar(100)	Тип документа[5]
FNUM	smallint	Идентификационный номер фонда
FNAMERUS	varchar(100)	Наименование фонда
TO_FNUM	integer	Идентификационный номер фонда, на паи которого осуществляется обмен[6]
TO_FNAMERUS	varchar(100)	Наименование фонда, на паи которого осуществляется обмен
BRANCHID	smallint	Идентификационный номер агентского пункта
branchname	character (20)	Наименование агентского пункта
HNUM	integer	Идентификационный номер клиента
HFULLNAME	varchar(100)	Фамилия Имя Отчество заявителя
DATEOFBIRTH	date	Дата рождения
PASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность
PASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность
ISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность
ISSUEDBY	character (150)	Орган выдачи документа, удостоверяющего личность
DOC_TYPE	varchar (505)	Тип документа, удостоверяющего личность
ACCOUNTREGISTRAR	character (20)	Номер лицевого счета
NMNAMERUS	varchar(100)	Способ получения уведомления по операции
RQUANTITY	decimal(16,5)	Количество паев в документе[7]
transactiondate	date	Дата принятия документа
zpSURNAME	character (50)	Фамилия законного представителя
zpNAME	character (50)	Имя законного представителя
zpPATRONYMIC	character (50)	Отчество законного представителя
zpDocType	const	Тип документа, удостоверяющего личность, законного представителя
zpPASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность, законного представителя
zpPASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность, законного представителя
zpISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность, законного представителя
zpISSUEDBY	character (150)	Орган выдачи документа, удостоверяющего личность, законного представителя
zpStatus	smallint	Статус законного представителя[8]
zpDOCUMENTTYPE	smallint	Тип документа - основания законного представителя
zpDOCNUM	varchar (15)	Номер документа-основания законного представителя
zpDOCDATE	date	Дата выдачи документа-основания законного представителя
zpDOCISSUEDBY	character (50)	Орган выдачи документа-основания законного представителя

[5] Принимает значения: "заявка на погашение", "Заявка на многократное приобретение","Анкета", "Изменение реквизитов", "Заявка на обмен паями"

[6] Для заявок на обмен инвестиционных паев

[7] Для заявок на обмен и погашение инвестиционных паев

[8] Принимает значения: «1» - Отец; «2» - Мать; «3» - Усыновитель; «4» - Попечитель; «5» - Опекун

upFIO	varchar (150)	ФИО уполномоченного представителя
upDocType	varchar (50)	Тип документа, удостоверяющего личность, уполномоченного представителя
upPASSPORTSERIES	varchar (50)	Серия документа, удостоверяющего личность, уполномоченного представителя
upPASSPORTNUMBER	varchar (50)	Номер документа, удостоверяющего личность, уполномоченного представителя
upISSUEDDATE	date	Дата выдачи документа, удостоверяющего личность, уполномоченного представителя
upISSUEDBY	varchar (150)	Орган выдачи документа, удостоверяющего личность, уполномоченного представителя
upDOCNUM	varchar (25)	Номер доверенности
upDOCDATE	date	Дата выдачи доверенности
BANKNAME	character (40)	Наименование банка
BANKLOCATION	character (50)	Город банка
PERSBANKACCOUNT	character (20)	Расчетный счет
BANKBIC	character (9)	БИК банка
BANKTIN	character (10)	ИНН банка
BANKCORRACCOUNT	character (20)	Корреспондентский счет банка
ISOPENACC	integer	Заявление на открытие лицевого счета[9]
ACCOUNTREGISTRAR2	character (20)	Лицевой счет в фонде, на паи которого осуществляется обмен[10]
NTUSERFULLNAMERUS	varchar(100)	ФИО сотрудника агентского пункта, принявший документ
FULLNAMERUS	varchar(100)	Полное наименование агентского пункта, принявшего документ
HOLDERFIO	varchar(100)	Фамилия Имя Отчество получателя платежа
PAMOUNTRUR	decimal	Сумма, на которую требуется выдать инвестиционные паи
RESIDENTTYPE	integer	Налоговый статус [11]
POA_PERIOD	varchar (25)	Срок действия документа-основания представителя
POA_NAME	varchar (505)	Наименование документа-основания представителя

Вариант 2.

Данные в файле должны соответствовать структуре описанной в Таблице 2.1, Таблице 2.2. и предоставляться в формате dat (Пример: имя_файла.dat) или в формате xls (Пример: имя_файла.xls). В случае передачи документов в формате dat Записи передаются в виде строк, запись по каждому полю разделяется знаком «;».

Таблица 2.1 Анкетные данные

Поле	Формат	Описание
branchname	char(50)	Наименование агентского пункта, принявшего документ
category	char(50)	Тип зарегистрированного лица[12]
surname	varchar(50)	Фамилия
NAME	varchar(50)	Имя

[9] Принимает значения:
"0", если в заявке не содержится заявление на открытие лицевого счета
"1", если в заявке содержится заявление на открытие лицевого счета
[10] Для заявок на обмен паев
[11] Принимает значения: «R» – резидент; «N» - нерезидент
[12] Принимает значения: "1"-физическое лицо; "2" - юридическое лицо

PATRONYMIC	varchar(50)	Отчество
DATEOFBIRTH	yyyymmdd	Дата рождения
CITIZENSHIP	varchar(50)	Гражданство
RESIDENTTYPE	varchar(1)	Налоговый статус[13]
Doc_type	Char(255)	Наименование документа, удостоверяющего личность
PASSPORTSERIES	varchar(50)	Серия документа, удостоверяющего личность
PASSPORTNUMBER	varchar(50)	Номер документа, удостоверяющего личность
ISSUEDDATE	yyyymmdd	Дата выдачи документа, удостоверяющего личность
ISSUEDBY	varchar(150)	Орган выдачи документа, удостоверяющего личность
LEGALADRESS	varchar(50)	Адрес регистрации
MAILINGINDEX	varchar(6)	Почтовый индекс
MAILINGREGION	varchar(500)	Область
MAILINGCITY	varchar(100)	Город
MAILINGSTREET	varchar(100)	Улица
MAILINGBUILDING	varchar(50)	Дом
MAILINGFLAT	varchar(5)	Квартира
PHONE	varchar(120)	Телефоны[14]
TIN	varchar(12)	ИНН
BANKNAME	varchar(60)	Наименование банка
BANKLOCATION	varchar(50)	Город банка
PERSBANKACCOUNT	varchar(20)	Расчетный счет
BANKBIC	varchar(9)	БИК банка
BANKTIN	varchar(10)	ИНН банка
BANKCORRACCOUNT	varchar(20)	Корреспондентский счет банка
CAPABILITY	varchar(50)	Дееспособность[15]
EMAIL	varchar(100)	Адрес электронной почты
rinum	int	Способ получения информации и выписок из реестра (код)
rinamerus	varchar(100)	Расшифровка способа получения информации и выписок из реестра: "1"- в месте подачи документов, "2" - у лица, осуществляющего ведение Реестра, "3" - по почте
H_id	char(50)	Идентификационный номер клиента
R_id	char(50)	Идентификационный номер заявления на изменение данных анкеты
Branch_id	char(50)	Идентификатор агентского пункта, принявшего заявку/заявление/анкету
rdate	yyyymmdd hh:mm:ss	Дата и время принятия анкеты
UL_FIO	char(255)	ФИО уполномоченного лица
UL_DOCTYPE	char(255)	Наименование (тип) документа, удостоверяющего личность, уполномоченного лица
UL_DOC_SER	char(50)	Серия документа, удостоверяющего личность, уполномоченного лица
UL_DOC_NUM	char(50)	Номер документа, удостоверяющего личность, уполномоченного лица
UL_DOC_DATE	yyyymmdd	Дата выдачи документа, удостоверяющего личность, уполномоченного лица
UL_DOC_ORG	char(2000)	Наименование органа, выдавшего документ, удостоверяющий личность, уполномоченного лица
UL_DOV_NUM	char(255)	Номер доверенности

[13] Принимает значения: - "R" - резидент; "N" - нерезидент
[14] Домашний, мобильный, рабочий - через запятую
[15] Принимает значения: "p" - полная;"o" - частичная;"n" - недееспособен

UL_DOV_DATE	yyyymmdd	Дата выдачи доверенности
PREDST_FIO	char(255)	Фамилия, имя, отчетсво законного представителя
PREDST_DOCTYPE	char(255)	Наименование (тип) документа, удостоверяющего личность, законного представителя
PREDST_DOC_SER	char(50)	Серия документа, удостоверяющего личность, законного представителя
PREDST_DOC_NUM	char(50)	Номер документа, удостоверяющего личность, законного представителя
PREDST_DOC_DATE	yyyymmdd	Дата выдачи документа, удостоверяющего личность, законного представителя
PREDST_DOC_ORG	char(2000)	Наименование органа, выдавшего документ, удостоверяющий личность, законного представителя
POLN_DOC_P	yyyymmdd	Срок действия доверенности

Таблица 2.2 Данные документов

Поле	Формат	Описание
rcod	char	Номер документа
rdate	yyyymmdd hh:mm:ss	Дата и время принятия документа
dtnamerus	char(100)	Тип документа[16]
fnum	int(2)	Цифровой код фонда
fnamerus	char(50)	Наименование фонда
to_fnum	int(2)	Цифровой код фонда, на паи которого осуществляется обмен
to_fnamerus	char(50)	Наименование фонда, на паи которого осуществляется обмен
branchname	char(50)	Наименование агентского пункта, принявшего документы
hfullname	char(100)	Полное наименование лица/Фамилия, имя, отчетсво
bdate	yyyymmdd	Дата рождения
passport_ser	char(50)	Серия документа, удостоверяющего личность
passport_num	char(50)	Номер документа, удостоверяющего личность
nmnamerus	char(100)	Способ получения информации и выписок из реестра
rquantity	num(16,5)	Количество паев[17]
transaction_date	yyyymmdd	Дата формирования документа
H_id	char(50)	Идентификационный номер клиента
R_id	char(50)	Идентификационный номер документа
Branch_id	char(50)	Идентификатор филиала, принявшего документ
Account_in	char(50)	Номер счета в фонде (для заявки на приобретение паев/для зачисления паев при заявке на обмен паев[18]/для заявления на изменение реквизитов/для запроса на предоставление информации и выписки из реестра)
Account_out	char(50)	Номер счета в фонде для заявки на погашение паев или для списания паев по заявке на обмен паев
Doc_type	char(255)	Наименование документа, удостоверяющего личность
Dos_issue	yyyymmdd	Дата выдачи документа, удостоверяющего личность

[16] допустимые значения: «Заявка на многократное приобретение паев», «Заявка на обмен паев», «Заявка на погашение паев», «Анкета зарегистрированного физ. лица», «Заявление на изменение способа получения информации из реестра», «Заявление на изменение данных Анкеты», «Запрос о предоставлении выписки/информации из Реестра»

[17] Для заявок на обмен и погашение инвестиционных паев

[18] В случае наличия в заявке на приобретение/обмен паев заявления на открытие лицевого счета, в поле должна содержаться отметка о таком заявлении

Doc_org	char(2000)	Наименование органа, выдавшего документ, удостоверяющий личность
BANKNAME	varchar(60)	Наименование банка
BANKLOCATION	varchar(50)	Город банка
PERSBANKACCOUNT	varchar(20)	Номер расчетного счета
BANKBIC	varchar(9)	БИК банка
BANKTIN	varchar(10)	ИНН банка
BANKCORRACCOUNT	varchar(20)	Корреспондентский счет банка
UL_FIO	char(255)	Фамилия, имя, отчество уполномоченного лица
UL_DOCTYPE	char(255)	Наименование (тип) документа, удостоверяющего личность, уполномоченного лица
UL_DOC_SER	char(50)	Серия документа, удостоверяющего личность, уполномоченного лица
UL_DOC_NUM	char(50)	Номер документа, удостоверяющего личность, уполномоченного лица
UL_DOC_DATE	yyyymmdd	Дата выдачи документа, удостоверяющего личность, уполномоченного лица
UL_DOC_ORG	char(2000)	Наименование органа, выдавшего документ, удостоверяющий личность, уполномоченного лица
UL_DOV_NUM	char(255)	Номер документа-основания
UL_DOV_DATE	yyyymmdd	Дата выдачи документа-основания
PREDST_FIO	char(255)	Фамилия, имя, отчество законного представителя
PREDST_DOCTYPE	char(255)	Наименование (тип) документа, удостоверяющего личность, законного представителя
PREDST_DOC_SER	char(50)	Серия документа, удостоверяющего личность, законного представителя
PREDST_DOC_NUM	char(50)	Номер документа, удостоверяющего личность, законного представителя
PREDST_DOC_DATE	yyyymmdd	Дата выдачи документа, удостоверяющего личность, законного представителя
PREDST_DOC_ORG	char(2000)	Наименование органа, выдавшего документ, удостоверяющий личность, законного представителя
DOC_CH_TYPE	char(2000)	Тип изменяемых реквизитов (для заявления на изменение данных анкеты зарегистрированного лица)
REQ_DOC_TYPE	char(255)	Вид запрашиваемого документа(для запроса о предоставлении выписки/информации из Реестра)
REQ_DATE_B	yyyymmdd	Дата начала периода (для запроса о предоставлении выписки/информации из Реестра)
REQ_DATE_E	yyyymmdd	Дата окончания периода (для запроса о предоставлении выписки/информации из Реестра)
REQ_PAI_NUM	Char(30)	Количество паев на лицевом счете (для запроса о предоставлении выписки/информации из Реестра)
PDI_AUTHOR	varchar(256)	ФИО сотрудника агентского пункта, принявший документ
POLN_DOC_TYPE	varchar(256)	Наименование документа-основания представителя
POLN_DOC_P	yyyymmdd	Срок действия доверенности
PROPERTY_TYPE	varchar(256)	Вид собственности
PURCHASE_SUM	num	Сумма, на которую требуется выдать инвестиционные паи
TAX_STATUS	varchar(256)	Налоговый статус[19]

[19] Принимает значения: "R" - резидент;"N" – нерезидент

2. Информация из реестра владельцев инвестиционных паев.

Данные в файле должны соответствовать структуре, описанной в Таблице 1 или Таблице 2, и предоставляться в формате xls (Пример: имя_файла.xls) или в формате csv (Пример: имя_файла.csv) соответственно. Записи передаются в виде строк.
Данные по уведомлениям об операциях в реестре инвестиционных паев должны соответствовать структуре, описанной в Таблице 3.

Таблица 1

Данные в файле должны быть представлены на 3 листах:

- **Лист UnitValues (Стоимость одного инвестиционного пая паевого инвестиционного фонда на дату):**

Поле	Формат	Описание
FNUM	smallint	Идентификационный номер фонда
DAY	timestamp	Дата, на которую предоставляется информация (Дата)
VALUE	decimal (16,5)	Стоимость одного инвестиционного пая на Дату

- **Лист HolderUnitAmount (Количество инвестиционных паев на лицевом счете на дату):**

Поле	Формат	Описание
HNUM	integer	Идентификационный номер клиента
FNUM	smallint	Идентификационный номер Фонда
DAY	timestamp	Дата, на которую предоставляется информация
QUANTITY	decimal(16,5)	Количество инвестиционных паев на лицевом счете, открытом в Фонде

- **Лист Extract (Записи по лицевым счетам, произведенные в реестре владельцев инвестиционных паев, на дату)**

Поле	Формат	Описание
Application number	varchar(32)	Номер документа, на основании которого совершена запись в реестре владельцев инвестиционных паев
Application date	timestamp	Дата документа, на основании которого совершена запись в реестре владельцев инвестиционных паев
Sum +	decimal(16,5)	Сумма денежных средств, внесенная в Фонд[20]
Sum -	decimal(16,5)	Сумма денежных средств, списанная из Фонда[21]
Date of money receipt	timestamp	Дата внесения денежных средств на счет Фонда или списания денежных средств со счета Фонда[22] (Дата)
Net Unit value	decimal(16,5)	Стоимость одного инвестиционного пая на Дату
Date of unit issue	timestamp	Дата списания или зачисления инвестиционных паев на лицевой счет в реестре владельцев инвестиционных паев[23]
Number of units +	decimal(16,5)	Количество зачисленных на лицевой счет инвестиционных паев
Number of units -	decimal(16,5)	Количество списанных с лицевого счета инвестиционных паев

[20] Для заявок на приобретение и обмен инвестиционных паев
[21] Для заявок на погашение и обмен инвестиционных паев
[22] В зависимости от типа заявки
[23] В зависимости от типа заявки

All Units	decimal(16,5)	Количество инвестиционных паев на лицевом счете, открытом в Фонде, на Дату
Налог	decimal(16,5)	Сумма уплачиваемого налога[24]

Таблица 2

Информация из Реестра владельцев инвестиционных паев представляется в двух файлах:

Файл 1.

Поле	Формат	Описание
DAY	timestamp	Дата, на которую предоставляется информация из реестра владельцев инвестиционных паев (Дата)
Fund	character (50)	Код фонда, в который подана заявка
Doctype	int(2)	Тип документа (заявки)[25]
SURNAME, NAME, PATRONYMIC	character (150)	ФИО клиента
PASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность
PASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность
Number of units	decimal(16,5)	Количество инвестиционных паев по заявке
Net Unit value	decimal(16,5)	Стоимость одного инвестиционного пая на Дату
Sum	decimal(16,5)	Сумма денежных средств по заявке
Discount_sum	decimal(16,5)	Сумма скидки
Application number	varchar(32)	Номер документа (заявки)
To_Fund	character (50)	Код фонда, на паи которого осуществляется обмен или паи которого списываются по обмену

Файл 2.

Поле	Формат	Описание
DAY	timestamp	Дата, на которую предоставляется информация из реестра владельцев инвестиционных паев (Дата)
ACCOUNTREGISTRAR	character (20)	Номер лицевого счета, открытого в реестре владельцев инвестиционных паев в Дату
SURNAME, NAME, PATRONYMIC	character (150)	ФИО клиента
PASSPORTSERIES	character (50)	Серия документа, удостоверяющего личность
PASSPORTNUMBER	character (50)	Номер документа, удостоверяющего личность

[24] Для заявок на погашение инвестиционных паев. В случае отсутствия налога указывается «0»

[25] Принимает значение: «01» - заявка на приобретение инвестиционных паев; «02» - заявка на погашение инвестиционных паев; «03» - заявка на обмен инвестиционных паев (приобретение паев по обмену); «04» - заявка на обмен инвестиционных паев (погашение паев по обмену)

Таблица 3

Поле	Формат	Описание
id	numeric(18,0)	Идентификационный номер уведомления
fond	varchar(255)	название паевого инвестиционного фонда
doc_no	varchar(100)	номер уведомления
doc_date	datetime	дата уведомления
op_name	varchar(100)	название операции
op_date	datetime	дата операции
op_time	datetime	время операции
pays_qty	decimal(18,8)	количество инвестиционных паев фонда, в отношении которых осуществлена операция
pay_date	datetime	дата ценообразования
pay_price	decimal(18,4)	расчетная стоимость инвестиционного пая (руб)
docs_str	varchar(255)	Документы, на основании которых совершена операция
docs_str2	varchar(255)	Документы, на основании которых совершена операция
partner_name_in	varchar(150)	Наименование зарегистрированного лица (Заполняется при приходной операции)
partner_doc	varchar(100)	Документ (Заполняется при приходной операции)
partner_reg	varchar(100)	Рег. Орган (Заполняется при приходной операции)
partner_no	varchar(100)	Лицевой счет № (Заполняется при приходной операции)
partner_type_acc	varchar(100)	Вид счета (Заполняется при приходной операции)
get	int	Отметка о выдаче уведомления
partner_name_out	varchar(150)	Наименование зарегистрированного лица (Заполняется при расходной операции)
partner_doc_out	varchar(100)	Документ (Заполняется при расходной операции)
partner_reg_out	varchar(100)	Рег. Орган (Заполняется при расходной операции)
partner_no_out	varchar(100)	Лицевой счет № (Заполняется при расходной операции)
partner_type_acc_out	varchar(100)	Вид счета (Заполняется при расходной операции)
hnum	varchar(50)	Идентификационный номер зарегистрированного лица
op_type	tinyint	при передаче увеодмления об отказе указывается "1"; в остальных случаях указывается "0"
refuse_reason	varchar(255)	основание отказа
sotrud_name	varchar(80)	подписант
bankname	varchar(255)	Реквизиты Специализированного регистратора
bankname2	varchar(255)	Реквизиты Специализированного регистратора
fj	int	зарегистрированное лицо: если юридическое лицо, заполняется как "1", если физическое лицо, заполняется как "0"
ank_partner_name	varchar(255)	Наименование зарегистрированного лица (Заполняется при операции изменения данных)
ank_country	varchar(80	Гражданство (Заполняется при операции изменения данных)
ank_status	varchar(80	Налоговый статус (Заполняется при операции изменения данных)
ank_birthday	varchar(40	Дата рождения (Заполняется при операции изменения данных)
ank_passport	varchar(255)	Документ (Заполняется при операции изменения данных)
ank_regist	varchar(255)	Свидетельство о регистрации (Заполняется при операции изменения данных)
ank_inn	varchar(40	ИНН (Заполняется при операции изменения данных)
ank_address	varchar(255)	Адрес регистрации (Заполняется при операции изменения данных)
ank_postaddress	varchar(255)	Почтовый адерс (Заполняется при операции изменения данных)
ank_phone	varchar(40	Телефон (Заполняется при операции изменения данных)
ank_email	varchar(80	Адрес электронной почты (Заполняется при операции изменения данных)
ank_receive_letter	varchar(40	Способ получения информации из рестра (Заполняется при операции изменения данных)
ank_bank	varchar(255)	Банковские реквизиты (Заполняется при операции изменения данных)

ank_signator	varchar(255)	Данные уполномоченного лица (Заполняется при операции изменения данных)
ank_partner_name_short	varchar(255)	Сокращенное наименование (Заполняется при операции изменения данных)
ank_opf	varchar(255)	Сокращенное наименование (Заполняется при операции изменения данных)
ank_kpp	varchar(40	КПП
ank_ogrn	varchar(80	ОГРН
ank_factaddress	varchar(255)	Фактический адрес
ank_director	varchar(255)	Руководитель

Приложение № 3
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

АКТ
о начале электронного документооборота

г. Москва
200___ года

«___» _____

ЗАО «Райффайзенбанк» (адрес местонахождения: 129090, Москва, ул.Троицкая, д.17, стр.1, ОГРН: 1027739326449), именуемое в дальнейшем **Организатор СЭД**, в лице _____, действующего на основании _____, с одной стороны, и _____ (адрес местонахождения: _____, ОГРН: _____), именуемое в дальнейшем **Участник ЭДО,** в лице _____, действующего на основании_____ с другой стороны, в дальнейшем именуемые **Сторонами**, заключили настоящий Акт о начале электронного документооборота (далее – Акт) о нижеследующем:

Стороны пришли к соглашению осуществлять электронный документооборот в соответствии с Договором о присоединении к Правилам электронного документооборота ЗАО «Райффайзенбанк» №_____ от «____» _____ 200__ г.

Стороны установили дату перехода к обмену электронными документами с «_____» _____ 200__ года.

Настоящий Акт составлен в 2-х экземплярах, имеющих одинаковую юридическую силу: один экземпляр хранится у Организатора СЭД, другой – у Участника ЭДО.

От Организатора СЭД:

_____ /_____
М.П.

От Участника ЭДО:

_____ /_____
М.П.

Приложение № 4
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Анкета Участника ЭДО

ДАТА ПЕРЕДАЧИ АНКЕТЫ ОРГАНИЗАТОРУ СЭД	**«___» _____ 200_ ГОДА**
Полное наименование Участника ЭДО	
Почтовый адрес Участника ЭДО, на котором произведена установка СКЗИ	
Электронный адрес Участника ЭДО	
Фамилия, имя, отчество ответственного лица, личный рабочий адрес электронной почты Интернет и номер рабочего телефона (заполняется на каждого ответственного исполнителя)	
Фамилия, имя, отчество администратора программного обеспечения, личный рабочий адрес электронной почты Интернет и номер рабочего телефона.	

От Участника ЭДО:

_____ /_____/
М.П.

Приложение № 5
к Правилам электронного документооборота
Специализированного депозитария ЗАО «Райффайзенбанк»

Анкета Организатора СЭД

Дата передачи Анкеты Участнику ЭДО	« » 200 года
Полное наименование Организатора СЭД	Закрытое акционерное общество «Райффайзенбанк»
Почтовый адрес Организатора СЭД	129090, Москва, ул.Троицкая, д.17, стр.1
Электронный адрес Организатора СЭД	
Фамилия, имя, отчество ответственного лица, личный рабочий адрес электронной почты Интернет и номер рабочего телефона (заполняется на каждого ответственного исполнителя)	
Фамилия, имя, отчество Оператора Удостоверяющего Центра, личный рабочий адрес электронной почты Интернет и номер рабочего телефона	

От Организатора СЭД:

_____/_____/
М.П.

Приложение №6
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Заявка

на предоставление программного обеспечения, СКЗИ и ключевых носителей от

_____
(наименование организации)

Для обеспечения работы в системе электронного документооборота ЗАО «Райффайзенбанк» в соответствии с Договором о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк» №_____ от «__»_____ 200__года, просим Вас предоставить программное обеспечение и средства криптографической защиты информации (СКЗИ):

Наименование	Количество
Программное обеспечение «КриптоАРМ» версия 4.4	
Программное обеспечение СКЗИ «КриптоПро CSP» версия 3.0	
Ключевой носитель	

Контактное лицо по техническим вопросам

ДОЛЖНОСТЬ	Ф. И. О.	ТЕЛЕФОН	E-MAIL

От Участника ЭДО:

_____ /_____/
М.П.

Приложение № 7
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

(БЛАНК УЧАСТНИКА ЭДО)

ДОВЕРЕННОСТЬ

город Москва
Дата (прописью)

_____
(полное наименование юридического лица – Участника)

_____
(местонахождение)

именуемое в дальнейшем «Доверитель», в лице _____
_____,
(должность, фамилия, имя, отчество)

действующего на основании _____, доверяет
_____
(должность, фамилия, имя, отчество)

паспорт серии _____, № _____, выдан _____,

проживающего по адресу _____,

получать программное обеспечение, СКЗИ и ключевые носители, подписывать акт приема-передачи программного обеспечения, СКЗИ и ключевых носителей.

Настоящая доверенность действительна до «__» _____ 20___года.

Полномочия по данной доверенности не могут быть переданы другим лицам.

Подпись _____ удостоверяю.

[Генеральный директор] _____/_____
М.П.

Приложение №8
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Заявление на регистрацию Пользователя
в Удостоверяющем центре ЗАО «Райффайзенбанк»

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта

_____
кем и когда выдан)

прошу зарегистрировать меня в Реестре Удостоверяющего центра ЗАО «Райффайзенбанк»:

CN = Общее имя = _____ Фамилия, Имя, Отчество
OU = Подразделение = _____ наименование подразделения
O = Организация = _____ наименование организации
L = Город = _____ наименование населенного пункта
C = Страна/Регион = RU
E = Электронная почта = _____ адрес электронной почты

От Участника ЭДО:

Заявитель _____ /Фамилия И.О./

Генеральный директор _____ /Фамилия И.О./

«____» _____ 20____ г.

Заявление на регистрацию Пользователя
в Удостоверяющем центре получил
«__»_____200_г.
Оператор Удостоверяющего Центра

_____ / _____
(подпись) (ФИО)

Приложение №9
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

(БЛАНК УЧАСТНИКА ЭДО)

ДОВЕРЕННОСТЬ

город Москва
Дата (прописью)

_____
(полное наименование юридического лица – Участника)

_____
(местонахождение)

именуемое в дальнейшем «Доверитель», в лице _____
_____,
(должность, фамилия, имя, отчество)

действующего на основании _____, доверяет
_____
(должность, фамилия, имя, отчество)

паспорт серии _____, № _____, выдан _____,

проживающего по адресу _____,
выполнять от лица _____
(Наименование организации)

следующие действия:

- передавать заявление на регистрацию пользователя _____;
(ФИО)

передавать заявление на получение ключей и сертификатов ключей подписи
_____;
(ФИО)

передавать заявление на аннулирование (отзыв) криптографических ключей
_____;
(ФИО)

получать от Удостоверяющего центра ключи подписи и сертификат ключа подписи, выданный на имя _____;
(ФИО)

расписываться в соответствующих документах Удостоверяющего центра для исполнения поручений, определенных настоящей Доверенностью.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.
Настоящая доверенность действительна до «__» _____ 20___года.

Подпись _____ удостоверяю.

Генеральный директор _____/_____
М.П.

Приложение №10
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Заявление на получение ключей и сертификатов ключей подписи
Пользователя Удостоверяющего центра ЗАО «Райффайзенбанк»

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта

_____
кем и когда выдан)

прошу сформировать для меня ключи подписи и изготовить на мое имя сертификат ключа подписи в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CN = Общее имя = _____ Фамилия, Имя, Отчество
OU = Подразделение = _____ наименование подразделения
O = Организация = _____ наименование организации
L = Город = _____ наименование населенного пункта
C = Страна/Регион = RU
E = Электронная почта = _____ адрес электронной почты

Области использования сертификата (идентификаторы OID), определяющие отношения, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение	

От Участника ЭДО:

Пользователь Удостоверяющего центра _____ /Фамилия И.О./

Генеральный директор _____ /Фамилия И.О./

«____» _____ 20____ г.

Заявление на получение ключей и сертификатов ключей подписи
Пользователя Удостоверяющего центра получил
«__»_____200_г.
Оператор Удостоверяющего Центра

_____ / _____
(подпись) (ФИО)

Приложение № 11
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

(БЛАНК УЧАСТНИКА ЭДО)

ДОВЕРЕННОСТЬ

г. _____
Дата (прописью)

_____
(полное наименование юридического лица – Участника ЭДО)

_____
(местонахождение)

именуемое в дальнейшем «Доверитель», в лице _____
_____,
(должность, фамилия, имя, отчество)

действующего на основании _____, доверяет
_____
(должность, фамилия, имя, отчество)

паспорт серии _____, № _____, выдан _____,

проживающего по адресу _____,

подписывать с применением электронной цифровой подписи от имени
_____
(полное наименование юридического лица – Участника ЭДО)

документы в соответствии со следующими областями применения:

1. _____;
2. _____.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.
Настоящая доверенность действительна до «__» _____ 20___года.

Подпись _____ удостоверяю.

Генеральный директор _____/_____
М.П.

Приложение №12
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Область использования сертификатов криптографических ключей пользователя.

Соответствие типов заверяемых ЭЦП в рамках системы электронного документооборота ЗАО «Райффайзенбанк» электронных документов идентификаторам, определяющим отношения, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

Область применения ЭЦП	Тип электронного документа
1.2.643.4.1.1.1	Система Электронного документооборота между Банком и Управляющими компаниями ПИФ
1.2.643.4.1.1.1.1	Первичные документы, принятые от физических и юридических лиц в отношении паевых инвестиционных фондов, а также сопровождающие документы
1.2.643.4.1.1.1.2	Документы, касающиеся осуществления операций, связанных с хранением и учетом прав на ценные бумаги и имущества паевого инвестиционного фонда
1.2.643.4.1.1.1.3	Документы, содержащие расчет показателей в отношении паевого инвестиционного фонда
1.2.643.4.1.1.1.4	Документы, подтверждающие согласие на списание денежных средств с банковского счета и на совершение сделок с имуществом паевого инвестиционного фонда
1.2.643.4.1.1.1.5	Документы, содержащие сведения о нарушениях, выявленных при осуществлении специализированным депозитарием контрольных функций
1.2.643.4.1.1.1.6	Отчеты специализированного депозитария
1.2.643.4.1.1.1.7	Информация из реестра владельцев инвестиционных паев
1.2.643.4.1.1.1.8	Счета за вознаграждения управляющей компании и Агента
1.2.643.4.1.1.1.9	Документы в отношении комиссий депозитария
1.2.643.4.1.1.1.10	Документы, подаваемые управляющей компанией, в отношении операций по счетам депо, в т.ч. документы для открытия/закрытия счета депо
1.2.643.4.1.1.1.11	Отчеты и справки депозитария
1.2.643.4.1.1.1.12	Ежемесячная, ежеквартальная и годовая отчетность, предоставляемая в Федеральную службу по финансовым рынкам РФ
1.2.643.4.1.1.1.13	Документы, связанные с совершением сделок, договоров и иных распорядительных действий, относящиеся к компетенции единоличного исполнительного органа
1.2.643.4.1.1.1.14	Поручения в отношении корпоративных действий
1.2.643.4.1.1.1.15	Информационные документы в отношении корпоративных действий
1.2.643.4.1.1.1.16	Журналы учета входящих документов
1.2.643.4.1.1.1.17	Информация об изменениях документов паевых инвестиционных фондов и порядка выдачи, погашения и обмена паев паевых инвестиционных фондов
1.2.643.4.1.1.1.18	Выписки с банковского счета с подтверждающими документами (платежные или иные документы), платежные документы на списание денежных средств с банковского счета
1.2.643.4.1.1.1.19	Отчеты брокера об операциях с портфелем ценных бумаг паевого инвестиционного фонда (или справка об их отсутствии)

Приложение № 13
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Корпоративный Удостоверяющий Центр ЗАО "Райффайзенбанк"

Сертификат открытого ключа

Сведения о сертификате:
Кому выдан:

Фамилия Имя Отчество

Область действия сертификата:
Область использования сертификата №1
Действителен с 24 декабря 2008 г. 10:42:00 UTC по 24 декабря 2009 г. 10:51:00 UTC
Кем выдан:
RaiffeisenBank Root CA

Версия: 3 (0x2)
Серийный номер: 6198 C4D0 0000 0000 0010
Издатель сертификата: CN = RaiffeisenBank Root CA, O = ZAO RaiffeisenBank, L = Moscow, C = RU
Срок действия:
Действителен с: 24 декабря 2008 г. 10:42:00 UTC
Действителен по: 24 декабря 2009 г. 10:51:00 UTC
Владелец сертификата: CN = Фамилия Имя Отчество, OU = Подразделение, O = Организация, L = Москва, C = RU, E = address@raiffeisen.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 7D65 D4FC 31D2 B9A8 0FAA 7F17 8E67 2025 2CA3 CB87 7B20 185F 5C22 440E 3027 E460 B68E 9B20 CDB5 B27D 83A8 5822 CDD8 C540 DA63 35AF D42B 2142 1A81 4EA6 5448 CC29
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Key Usage
Значение: Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
2. Расширение 2.5.29.37
Название: Enhanced Key Usage
Значение: Область использования сертификата №1 (1.1.1.1.1.1.1)
3. Расширение 2.5.29.14
Название: Subject Key Identifier
Значение: 1d e9 b2 f3 b8 8b f6 39 37 66 3f 02 4e 2d a8 c2 c6 35 a8 13
4. Расширение 2.5.29.35
Название: Authority Key Identifier
Значение: KeyID=58 98 7c 17 f7 d3 67 b7 4c 28 65 78 5c ba 53 dc 0d dd 29 46
5. Расширение 2.5.29.31
Название: CRL Distribution Points
Значение: [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki.raiffeisen.ru/pki/cdp/9949e612e6a748ddf4e168951a231cbafcc3344e.crl
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 05 00
Значение: B98F BF30 3A50 2F85 CB0A 41C7 B516 57E7 F231 F2D1 1283 094C A221 1862 6915 3431 8BE4 B96E 6DDC A3A8 7254 2E15 D85A 29D2 8C88 5508 7D67 19A2 9329 3305 E24C F928

Подпись владельца сертификата: _____/_____

"____" _____ 20__ г.

Подпись уполномоченного лица Удостоверяющего Центра: _____/_____

"____" _____ 20__ г.
М. П.

Средство криптографической защиты информации "КриптоПро CSP"

119071, Москва, ул. Ленинский проспект, д.15А
Управление информационной безопасности.

Приложение № 14
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

АКТ

формирования и передачи криптографических ключей

г. Москва «___» _____ 200__ года

ЗАО «Райффайзенбанк» (адрес местонахождения: 129090, Москва, ул.Троицкая, д.17, стр.1, ОГРН: 1027739326449), именуемое в дальнейшем Организатор СЭД, в лице Оператора УЦ _____, действующего на основании _____, с одной стороны, и _____(адрес местонахождения: _____ ОГРН: _____), именуемое в дальнейшем Участник ЭДО, в лице _____, действующего на основании _____, с другой стороны, составили настоящий Акт о нижеследующем:

В соответствии с:

- Правилами электронного документооборота ЗАО «Райффайзенбанк»;
- комплектом эксплуатационной документации на СКЗИ «КриптоПРО»;

сформированы, упакованы и переданы Участнику индивидуальные криптографические ключи, записанные на ключевые носители:

Идентификационные данные сформированных ключей:

№ п/п	Серийный номер № криптографического ключа (по реестру Удостоверяющего центра)	Экземпляр	Статус ключей (действующие или резервные)

Секретные ключи шифрования и подписи сформированы в количестве, указанном в приведенной выше таблице. Каждый конверт с ключевым носителем содержит идентификационные данные лиц, уполномоченных для работы со СКЗИ, указанные в Заявке на предоставление СКЗИ и формирование криптографических ключей.

Участником ЭДО приняты все меры по обеспечению их сохранности и конфиденциальности ключей.

Настоящий Акт составлен в 2 (двух) экземплярах.

От Организатора СЭД: _____/_____ М.П.

От Участника ЭДО: _____/_____ М.П.6

Приложение № 15
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

АКТ

приема - передачи программного обеспечения, СКЗИ и ключевых носителей

г. Москва «___» _____ 200__ года

В соответствии с Договором о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк» № _____ от «___» _____ 200_ года ЗАО «Райффайзенбанк» (адрес местонахождения: 129090, Москва, ул.Троицкая, д.17, стр.1, ОГРН: 1027739326449), именуемое в дальнейшем Организатор СЭД, в лице _____, действующего на основании _____, передал, а _____ (адрес местонахождения: _____ ОГРН: _____), именуемое в дальнейшем Участник ЭДО, в лице _____, действующего на основании _____, для целей использования в системе электронного документооборота ЗАО «Райффайзенбанк» принял:

- программное обеспечение *(далее именуется ПО)* «КриптоПРО»:

Серийный номер ПО «КриптоАРМ» версия 4.4	
Серийный номер СКЗИ «КриптоПРО CSP» версия 3.0	

- ключевые носители e-Token PRO в количестве ____ шт.

Настоящий Акт составлен в 2 (двух) экземплярах.

От Организатора СЭД:	От Участника ЭДО:
_____/_____	_____/_____
М.П.	М.П.

Приложение № 16
к Правилам электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк»

Заявление на аннулирование (отзыв) криптографических ключей.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата*)

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра:

_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

Серийный номер криптографического ключа _____

Подпись владельца сертификата ключа подписи –
Пользователя Удостверяющего центра _____ / _____

Генеральный директор _____ / _____
(подпись) (ФИО)

М.П.

Заявление на аннулирование (отзыв)
криптографических ключей получил
«__»_____200_г.
Оператор Удостоверяющего Центра

_____ / _____
(подпись) (ФИО)