Приложение № 3 к Правилам
Открытого акционерного общества
«Всероссийский банк развития регионов»
по использованию Системы QUIK

ПОЛОЖЕНИЕ
об организации обмена ЭД посредством Системы QUIK

1. Общие положения.

1.1. Настоящее Положение устанавливает порядок организации и проведения обмена ЭД между Банком и Клиентом. Обмен ЭД между Сторонами подразумевает передачу (направление/предоставление) одной Стороной и получение другой Стороной ЭД.

1.2. Передача (направление/предоставление) ЭД осуществляется путем их размещения на Сервере Системы QUIK.

1.3. Моментом передачи (направления/предоставления) ЭД одной Стороной и моментом получения этого ЭД другой Стороной является момент его размещения на Сервере Системы QUIK.

1.4. Технологические возможности Системы QUIK позволяют не отделять во времени момент передачи (направления/предоставления) ЭД одной Стороной от момента его непосредственного получения другой Стороной, если Клиентом в это время установлена посредством его интернет-провайдера связь его рабочего места с Сервером Системы QUIK Банка.

1.5. Клиент, осуществляя соединение его рабочего места с Сервером Системы QUIK через своего интернет-провайдера, получает Информацию о ходе биржевых торгов, доступных для торговли средствах и может самостоятельно в режиме реального времени реагировать на изменения ценовых показателей на ценные бумаги, посылая Поручения Банку.

1.6. Рабочее место Клиента состоит из персонального компьютера класса IBM PC/AT, имеющего доступ в сеть Интернет, общесистемного программного обеспечения и программного обеспечения Системы QUIK в составе и в соответствии с требованиями, указанными в Приложении № 4.

1.7. Сервер Системы QUIK принимает ЭД, передаваемые Клиентом через своего интернет-провайдера по сети Интернет и, если ЭД содержит Поручение, производит обмен Информацией со шлюзом ТС, посредством которого происходит взаимодействие с ТС, и размещает Информацию для Клиента.

1.8. Банк размещает для Клиента на Сервере Системы QUIK Отчеты по Сделкам Клиента, совершенные на основании Поручений, поданных Клиентом в виде ЭД.

2. Подготовка к работе с криптографическими ключами. Действия при компрометации ключей.

2.1. Клиент формирует Закрытый и Открытый ключи ЭЦП при помощи программного обеспечения, установленного у Клиента (Приложение № 4). Закрытому ключу ЭЦП соответствует Открытый ключ ЭЦП. При возникновении каких-либо сложностей при формировании (замене) Ключей Клиент может обращаться к Администратору Системы QUIK Банка по телефонам, указанным в данном разделе ниже.

2.2. Для регистрации ключей ЭЦП Клиент предоставляет в Банк по электронной почте по адресу cert@vbrr.ru собственный Открытый ключ ЭЦП в виде электронного файла (запроса на выдачу Сертификата). В тот же день Клиент предоставляет в Банк Открытый ключ ЭЦП также в виде распечатки Акта признания Открытого ключа (Приложение №

10.1, 10.2), подписанный Клиентом и/или Уполномоченным представителем Клиента в 2 (Двух) экземплярах.

2.3. Акты признания заполняются отдельно на каждый криптографический ключ Клиента.

2.4. Банк в течение Рабочего дня, следующего за днем получения от Клиента Открытого ключа ЭЦП в форме, указанной в п.2.2, осуществляет проверку корректности и соответствия Открытого ключа в распечатке Акта признания электронному файлу и, в случае корректности и соответствия, регистрирует Открытый ключ и выдает Клиенту Сертификат, направляя его по адресу электронной почты Клиента.

2.5. Лица, Уполномоченные Клиентом на получение в Банке программного обеспечения, документов и материальных ценностей представляют в Банк надлежащим образом оформленную доверенность, составляемую по форме Приложения № 7.

2.6. Для начала работ Клиента в Системе QUIK последовательно выполняются действия, указанные таблице:

Работы	**Срок**	**Исполнитель**
1. Передача Клиенту по электронной почте комплекта программного обеспечения Системы QUIK.	В день подписания Заявления Клиентом	Банк
2. Подписание Акта приема-передачи программного обеспечения Системы QUIK (Приложение № 5).	В день подписания Заявления Клиентом	Клиент
3. Установка и настройка комплекта программного обеспечения.	По мере готовности, но не более 2 (Двух) Рабочих дней со дня подписания Заявления	Клиент
4. Формирование Открытого и Закрытого ключей, подписание Акта признания Открытого ключа в 2 (Двух) экземплярах и передача его в Банк. Передача в тот же день по электронной почте в Банк по адресу cert@vbrr.ru запроса на выдачу Сертификата - электронного файла, содержащего Открытый ключ ЭЦП.	По мере готовности, но не более 2 (Двух) Рабочих дней со дня подписания Заявления	Клиент
5. Проверка соответствия Открытого ключа в Акте признания и в электронном файле. Регистрация ключа в Банке. Изготовление Сертификата. Передача файла, содержащего Сертификат, Клиенту по электронной почте.	В Рабочий день, следующий за днем получения от Клиента Открытого ключа ЭЦП по электронной почте и на бумажном носителе	Банк
6. Тестирование Системы QUIK с использованием нулевых Лимитов.	В течение Рабочего дня, следующего за днем передачи Сертификата Клиенту	Банк, Клиент
7. Подписание Акта о начале использования Системы QUIK (Приложение № 6).	Не позднее Рабочего дня, следующего за днем проведения тестирования	Клиент

2.7. В случае компрометации криптографических ключей Клиента:

2.7.1. Клиент немедленно информирует о данном факте Банк, для чего он должен выполнить все указанные ниже действия:

2.7.1.1. Сообщить в Банк о факте компрометации по телефону (495) 662-81-53, (495) 933-03-43 (доб. 2520), либо по бесплатному междугороднему номеру 8 800 700-81-53;

2.7.1.2. заполнить Акт о компрометации криптографических ключей Клиента Системы QUIK (Приложение № 9), подписать и отправить его в Банк по факсу;

2.7.1.3. направить оригинал Акта о компрометации криптографических ключей Клиента Системы QUIK в Банк с курьером, по почте либо представить лично.

2.7.2. В ответ на Сообщение Клиента Банк обязан:

2.7.2.1. после получения факсимильной копии Акта о компрометации криптографических ключей Клиента Системы QUIK приостановить использование указанного в Акте ключа в Системе QUIK не позднее 23:59 текущего дня по московскому времени на срок до 1 (Одной) недели;

2.7.2.2. после получения оригинала Акта о компрометации криптографических ключей Клиента Системы QUIK провести блокировку использования указанного ключа в Системе QUIK не позднее 23:59 текущего дня по московскому времени. После проведения блокировки дальнейшее использование скомпрометированного ключа невозможно.

2.7.3. Для возобновления работ Клиента в Системе QUIK необходимо последовательно выполнить следующие работы:

2.7.3.1. формирование Клиентом Открытого и Закрытого ключей, подписание Акта признания Открытого ключа в 2 (Двух) экземплярах и передача его в Банк в виде оригинала на бумажном носителе вместе с запросом на выдачу Сертификата - электронным файлом, содержащим Открытый ключ ЭЦП, который передается в Банк по следующему адресу электронной почты: cert@vbrr.ru;

2.7.3.2. проверка Банком соответствия Открытого ключа в Акте признания и в электронном файле. Регистрация ключа;

2.7.3.3. передача по электронной почте Сертификата Клиенту.

2.8. Криптографические ключи вводятся в действие с даты и времени, указанного в:

2.8.1. Акте о начале использования Системы QUIK (Приложение № 6);

2.8.2. Акте смены криптографических ключей Системы QUIK (Приложение № 8).

2.9. Криптографические ключи выводятся из действия с даты и времени:

2.9.1. указанного в Акте смены криптографических ключей Системы QUIK (Приложение № 8);

2.9.2. указанного в Акте о компрометации криптографических ключей Клиента Системы QUIK (Приложение № 9);

2.9.3. указанного в Сертификате Открытого ключа Клиента;

2.9.4. либо с даты и времени, определяемыми в соответствии с датой и временем окончания срока действия Соглашения.

3. Хранение и использование СКЗИ и криптографических ключей.

3.1. Банк не хранит закрытых криптографических ключей Клиента и не имеет доступа к ним.

3.2. В целях безопасности Клиент обязан хранить свои закрытые криптографические ключи на съемных носителях Информации в недоступном неуполномоченным лицам месте. Ключевые носители должны извлекаться из хранилища только на время непосредственного использования. Ключевые носители не должны быть доступны для посторонних лиц от момента генерации до момента уничтожения ключей. Всю ответственность за ненадлежащее хранение закрытых ключей несет Клиент.

3.3. Клиент вправе создать необходимое количество резервных копий ключевых носителей при условии соблюдения тех же правил обращения с ними, которые установлены для основных носителей.

3.4. После выведения криптографических ключей Клиента из действия Клиент обязан уничтожить такие ключи.

3.5. Клиент принимает на себя полную ответственность за использование криптографических ключей Клиента и обязуется самостоятельно обеспечить сохранность и конфиденциальность ключей Клиента.

3.6. Клиент осведомлен о рисках, связанных с распространением вредоносного программного обеспечения и обеспечивает защиту рабочего места Клиента в Системе QUIK своими силами. Банк рекомендует использовать следующие меры по подготовке и защите рабочего места Клиента в Системе QUIK, выполняемые в указанной последовательности:

3.6.1. переустановка операционной Системы для исключения присутствия на рабочем месте вредоносного программного обеспечения;

3.6.2. установка необходимого для работы офисного программного обеспечения; при этом должно использоваться только лицензионное программное обеспечение, получаемое из надежных источников;

3.6.3. включение персонального межсетевого экрана, полное блокирование входящего трафика;

3.6.4. установка антивирусного монитора, настройка периодических обновлений антивируса;

3.6.5. настройка режима обновлений операционной системы для своевременной установки обновлений безопасности;

3.6.6. подключение к сети интернет, которое производится только после выполнения указанных выше действий;

3.6.7. ограничение доступа в сеть интернет сайтами Системы QUIK и сайтами обновлений операционной Системы и антивируса;

3.6.8. установка программного обеспечения Системы QUIK;

3.6.9. после установки программного обеспечения Системы QUIK на рабочей станции организационными либо техническими мерами запретить использование на ней (подключение) съемных носителей Информации (дискеты, usb-накопители: flash, hdd, телефоны, фотоаппараты и т.п., CD/DVD диски), кроме тех, на которых хранятся криптографические ключи Системы QUIK.

3.7. После подготовки рабочего места Системы QUIK в целях обеспечения его безопасного использования Клиент должен обеспечить штатное функционирование указанных выше защитных механизмов. Помимо перечисленных выше мер обеспечения Информационной безопасности Клиент вправе использовать любые дополнительные меры, признанные им целесообразными.

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

4. Порядок передачи ЭД в Системе QUIK.

4.1. Для начала работ с Системой Клиент устанавливает соединение с Сервером Системы QUIK Банка через сеть Интернет. После установления соединения Клиент проходит

авторизацию на сервере. Клиент получает возможность создания ЭД в адрес Банка и доступа к размещенной на сервере Информации ТС. Информация размещается на Сервере QUIK Банка в реальном времени по мере поступления такой Информации с шлюза в ТС, находящегося в зоне ответственности ТС.

4.2. В Системе QUIK передача ЭД, представляющих собой Поручения, происходит только в направлении от Клиента в Банк. Такие ЭД передаются по защищенному каналу связи и содержат ЭЦП. От Банка в адрес Клиента направляются ЭД, представляющие собой Отчеты по Сделкам, совершенным в течение дня, и иные документы Информационного характера, также содержащие ЭЦП. Информация от ТС поступает к Клиенту от Банка по защищенному каналу связи, но не содержит ЭЦП. Архив полученных Банком ЭД хранится на сервере Банка и доступен Клиенту по запросу. Архив Отчетов, полученных от Банка, и иных документов Информационного характера, получаемых Клиентом от Банка, должен вестись Клиентом самостоятельно.

4.3. Все ЭД Клиента, поступающие в Банк, а также ЭД, предоставляемые Банком Клиенту, должны содержать корректную ЭЦП Уполномоченного представителя, полученную на действующем ключе ЭЦП. Это позволяет обеспечить целостность данных документов, так как любое изменение в документе после его подписания сделает ЭЦП некорректной, а также подтверждение факта создания документа уполномоченным лицом (авторства).

4.4. Основанием для принятия к исполнению Банком переданного Клиентом по Системе QUIK ЭД является его передача на Сервер QUIK Банка, наличие корректной ЭЦП у данного документа, полученной на действующем в момент подписания ключе ЭЦП, а также соответствие этого ЭД требованиям к оформлению таких документов.

4.5. Исполнение Поручения заключается в формальной проверке возможности формирования заявки Банка на основании Поручения Клиента, формирование и передача такой заявки в ТС, либо уведомление Клиента о невозможности исполнения Поручения.

5. Порядок разрешения споров.

5.1. Порядок разрешения споров между Банком и Клиентом, не связанных с технической стороной исполнения ЭД Системы QUIK, определяется в соответствии с Регламентом (п. 6 «Порядок и разрешение споров») и действующим законодательством. Споры между Банком и Клиентом, связанных с технической стороной исполнения ЭД Системы QUIK, рассматриваются Сторонами в порядке, предусмотренном разделом 13 Правил с учетом особенностей, изложенных в настоящем разделе ниже.

5.2. Стороны признают, что используемые средства защиты информации достаточны для защиты информации от несанкционированного доступа, подтверждения подлинности ЭД, а также разрешения споров по ним.

5.3. Все споры, которые могут возникнуть по поводу технической стороны исполнения ЭД Системы QUIK, могут быть сведены к разногласиям относительно подлинности ЭД. Таким образом, любой такой спор может быть разрешен путем предъявления подлинного ЭД или фиксирования факта невозможности предъявления такого документа.

5.4. Суть спора заключается в том, что Сторона, инициирующая спор, выражает сомнение в наличии у другой Стороны подлинного ЭД по предмету спора. Спор решается в пользу инициатора спора, если другая Сторона не может предъявить такой ЭД и не в пользу инициатора спора, если другая Сторона предъявляет такой документ.

5.5. При возникновении спора относительно подлинности ЭД Сторона, инициирующая спор, направляет другой Стороне в письменном виде претензию, в которой излагает существо требований, а также правовые и фактические основания требований.

5.6. С целью разрешения спора рассматриваются документы, в том числе ЭД, относящиеся к предмету разногласий, и выполняется процедура установления подлинности ЭД, являющегося предметом разбирательства.

5.7. Математические свойства алгоритма ЭЦП свидетельствуют о невозможности подделки ЭЦП любым лицом, не обладающим секретным криптографическим ключом ЭЦП. Стороны признают, что процедура разрешения спора в отношении подлинности ЭД заключается в доказывании подписания конкретного ЭД на конкретном, действовавшем на момент выработки ЭЦП, ключе ЭЦП.

5.8. При разрешении споров Стороны используют эталонный компьютер, эталонное программное обеспечение, Акты признания и Сертификаты криптографических ключей.

5.9. Эталонное программное обеспечение состоит из операционной Системы, программного обеспечения Системы QUIK и программного обеспечения СКЗИ, применяемого в QUIK.

5.10. Эталонное оборудование и программное обеспечение предоставляется Банком.

5.11. При разрешении спора Клиент вправе пользоваться средствами разработчика СКЗИ; в этом случае оплата услуг разработчика производится Клиентом с последующим отнесением расходов на неправую сторону.

5.12. Банк предоставляет подтверждения получения и исполнения ЭД в виде протоколов работы Системы QUIK. Сторона, отстаивающая подлинность ЭД, предоставляет другой стороне спорный ЭД; документы, подтверждающие статус ключа ЭЦП, использованного при проверке спорного ЭД, а также Сертификат данного ключа.

5.13. Стороны предоставляют Сертификаты ключей, а также акты и иные документы, подтверждающие статус использованного при проверке спорного ЭД ключа ЭЦП.