Порядок получения и замены Простой Электронной подписи для использования информационно-торговой системы QUIK

[1. Общие положения 1](#_Toc459990672)

[2. Процедура начала работы 2](#_Toc459990673)

[3. Использование пароля доступа 3](#_Toc459990674)

[4. Правила идентификации Клиента, подписывающего Поручение простой ЭП 3](#_Toc459990675)

[5. Процедура разрешения споров и разногласий 4](#_Toc459990676)

[6. Процедура замены ключей ЭП 5](#_Toc459990677)

# Общие положения

## Банк имеет право отказать Клиенту в получении и использовании Простой ЭП по своему усмотрению без объяснения причин.

## Термины и определения

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| Двухфакторная аутентификация | Процедура проверки Клиента посредством ввода Пароля доступа, полученного в виде SMS-сообщения. Является вторым этапом идентификации Клиента (после ввода Логина и Пароля) при входе в ИТС QUIK. |
| Закрытый ключ (secring) | Уникальная последовательность символов, известная только Клиенту и предназначенная для дешифрования потока передаваемых в ИТС QUIK данных Клиентом.  Дешифрование кода без знания Закрытого ключа неосуществимо. |
| Логин | Имя Клиента или последовательность символов, установленная Клиентом, которая служит средством аутентификации Клиента при подключении к ИТС QUIK, и является подстроками открытой части ключа в файле pubring.txk и закрытой части ключа в файле secring.txk. |
| Открытый ключ (pubring) | Уникальная последовательность символов, соответствующая Закрытому ключу (secring), доступная обеим Сторонам и предназначенная для шифрования передаваемых данных и аутентификации Клиента. |
| Пароль доступа | Пароль, действующий только для одного сеанса аутентификации, являющийся одноразовым. Действие такого пароля ограничено определенным промежутком времени, заданным Банком. |

# Процедура начала работы

## При получении Банком от Клиента Заявки на использование ИТС QUIK (Приложение №1 к Порядку обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK) (далее - Заявка) с указанием (выбором) в Заявке использования ИТС QUIK с интегрированной библиотекой Криптографических ключей ЗАО «АРКА Текнолоджиз» Банк проверяет правильность и полноту заполнения Заявки.

### В случае некорректного или неполного оформления Заявки Банк отказывает в предоставлении услуг, предусмотренных Приложением №20 к Регламенту.

### В случае корректного оформления Заявки Банк передает Клиенту Дистрибутивный пакет на цифровом носителе или направляет Дистрибутивный пакет на электронную почту, указанную в Заявлении на обслуживание на финансовых рынках (Приложение №1 или 1А к Регламенту).

## Клиент самостоятельно в соответствии инструкцией, встроенной в Дистрибутивный пакет, последовательно осуществляет следующие действия:

* осуществляет установку Рабочего места Клиента;
* присваивает Логин и Пароль, которые впоследствии будут использоваться при аутентификации Клиента;
* создает средствами ИТС QUIK Криптографические ключи (Ключи).

В результате у Клиента должны сформироваться два файла:

1. файл с содержанием Закрытого ключа (secring.txk), который хранится на индивидуальном носителе или компьютере Клиента;
2. файл с содержанием Открытого ключа (pubring.txk), который направляется Клиентом на электронную почту [brok@ofc.ru](mailto:brok@ofc.ru) или на электронную почту Уполномоченного лица (Сотрудника) Банка для размещения на сервере Банка.

## После получения от Клиента файла с содержанием Открытого ключа (pubring.txk) Банк готовит и передает Клиенту для подписания Акт приема-передачи Открытого ключа (pubring) Простой ЭП и номера сотового телефона для получения Пароля доступа (далее - Акт) (Приложение №4.1 к Порядку обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK), содержащий сведения:

* Логин, присвоенный Клиентом;
* содержимое Открытого ключа (pubring);
* UID;
* номер сотового телефона для направления Пароля доступа.

## Открытый ключ (pubring.txk) считается зарегистрированным Банком с момента подписания Клиентом и передачи в Банк Акта на бумажном носителе.

## Не позднее двух рабочих дней с момента получения Банком подписанного Акта Клиент получает возможность подавать Поручения с использованием ИТС QUIK.

## Клиент после регистрации Банком Открытого ключа (pubring.txk) осуществляет подключение к ИТС QUIK с использованием присвоенного Логина и Пароля, а также Пароля доступа, полученного через Двухфакторную аутентификацию.

# использование пароля доступа

## Механизм Двухфакторной аутентификации позволяет снизить вероятность возникновения попыток Несанкционированного доступа, происходящих по причине утери, либо кражи Ключей доступа к системе ИТС QUIK Клиента злоумышленниками.

## Клиент при каждом подключении к ИТС QUIK, наряду с обычными параметрами (Логин и Пароль для защиты Закрытого ключа (secring.txk)), вводит дополнительную информацию (Пароль доступа).

## Пароль доступа сообщается Банком Клиенту через сотовый канал связи, а именно передача Пароля доступа производится с помощью SMS-сообщений, отправляемых Банком на номер сотового телефона, указанный Клиентом в Акте. При возникновении любых технических проблем (в т.ч. если при подключении к ИТС QUIK не поступило SMS-сообщение с Паролем доступа) или сбоев Клиент обязан максимально быстро связаться с Банком по телефону или электронной почте brok@ofc.ru для выяснения причин возникновения технических проблем или сбоев, а также для принятия Клиентом решения в отношении переданных Банку, но не исполненных Поручений Клиента, если таковые имеются, а также подачи новых Поручений.

## В случае смены номера сотового телефона Клиент сообщает Банку способами связи, предусмотренными Регламентом, новый номер сотового телефона, предназначенного для получения Пароля доступа. Банк оформляет, а Клиент подписывает новый Акт с указанием нового номера сотового телефона.

## До момента получения Банком подписанного Клиентом нового Акта Банк направляет Пароли доступа на заявленный ранее в Акте номер сотового телефона.

## Утрата, либо кража мобильного телефона и/или SIM-карты с номером телефона, указанного в Акте, признаются Компрометацией Ключей ЭП. В таком случае Клиент осуществляет действия в соответствии с разделом 3 Порядка обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK (Приложения №20) к Регламенту.

# правила ИДЕНТИФИКАЦИИ Клиента, подписывающего Поручение простой эП

## Клиент, использующий Простую ЭП, однозначно идентифицируется Банком при:

## соответствии данных Клиента, указанных при оформлении Акта, данным Клиента, имеющимся в Банке в рамках Соглашения;

## соответствии данных Открытого ключа (pubring.txk) и UID Клиента, указанных в оформленном клиентом Акте, файлу с содержанием Открытого ключа (pubring.txk), переданному Клиентом для привязки к Рабочему месту Клиента на сервере Банка (проверка при регистрации в ИТС QUIK нового ключа Клиента);

## соответствии Закрытого ключа (secring.txk), запрашивающего доступ на сервер Банка с Рабочего места Клиента, Открытому ключу (pubring.txk), размещенному на сервере Банка и соответствующему Рабочему месту Клиента (проверка при аутентификации Клиента для установления связи с Банком).

## соответствии Пароля доступа, полученного Клиентом в SMS-сообщении, Паролю доступа, введенному при входе в ИТС QUIK.

## Соединение с сервером ИТС QUIK c Рабочего места Клиента происходит только после ввода Клиентом:

### Логина и Пароля (при этом Пароль известен только Клиенту), и

### Двухфакторной аутентификации - дополнительного ввода Пароля доступа, полученного SMS-сообщением.

### Для Банка данное соединение однозначно считается установленным Клиентом.

## Все Поручения в ТС или Сообщения после подключения к ИТС QUIK Клиента, использующего Простую ЭП, в случае присутствия данного Поручения в ТС или Сообщения в отчете по транзакциям, сформированном по UID, на который зарегистрирован его Открытый ключ (pubring.txk), Стороны признают поданными/направленными Клиентом.

# ПРОЦЕДУРА РАЗРЕШЕНИЯ СПОРОВ И РАЗНОГЛАСИЙ

## В целях разрешения споров и разногласий Стороны образуют согласительную комиссию в количестве двух человек (по одному представителю от каждой из Сторон), которая производит все операции по подготовке и проведению проверки спорного Электронного документа (ЭД). Представителями Банка и Клиента могут быть назначены как представители Сторон, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.

## Проверка спорного Электронного документа (ЭД) проводится на оборудовании и программном обеспечении Банка в помещении Банка. Для проведения процедуры проверки на свободном от программного обеспечения компьютере устанавливается операционная система и программное обеспечение, необходимое для осуществления проверки:

### Клиент предоставляет на внешнем электронном носителе экземпляр Открытого ключа (pubring.txk), соответствующего Рабочему месту Клиента на момент отправки ЭД, используемого при передаче спорного ЭД и соответствующий Акт.

### Банк предоставляет отчет по транзакциям с сервера Банка, содержащий номер Рабочего места Клиента и спорный ЭД, контрольный экземпляр Открытого ключа (pubring.txk), зарегистрированного на сервере ИТС QUIK, соответствующий данному Рабочему месту на момент получения Банком спорного ЭД и другую информацию, зафиксированные в ИТС QUIK и подтверждающие соответствие контрольного экземпляра Открытого ключа Рабочему месту Клиента, и аутентификацию Клиента в сессии, в рамках которой был передан спорный Электронный документ с использованием контрольного экземпляра Открытого ключа.

### Согласительной комиссией проводится проверка соответствия экземпляра Открытого ключа (pubring.txk) и Акта, представленных Клиентом, и контрольного экземпляра Открытого ключа (pubring.txk), представленного Банком. На основании отчета о транзакциях и другой информации с сервера ИТС QUIK проверяется соответствие номера рабочего места в Электронном документе, полученном Банком и сессии, в рамках которой был получен документ, контрольному экземпляру Открытого ключа и номеру Рабочего места Клиента в Акте.

### Результатом деятельности согласительной комиссии является определение Стороны, несущей ответственность по фактам, вызвавшим спорную ситуацию. Результаты работы согласительной комиссии оформляются решением. В решении должны быть указаны обстоятельства возникновения спорной ситуации, Сторона, по вине которой возникла спорная ситуация, а также распределение обязанностей (при необходимости - порядок распределения между Сторонами материальных расходов), связанных с исполнением решения комиссии.

## В случае возникновения у любой из Сторон сомнений в полноте и/или целостности (отсутствие, искажение, присутствие ошибочной) информации, зафиксированной ИТС QUIK, Стороны могут привлечь в качестве независимого эксперта разработчика(ов) ИТС QUIK. При этом оплата услуг независимого эксперта, если необходимо, осуществляется за счет Стороны, выступившей инициатором приглашения эксперта, либо иным образом – при наличии согласия Сторон.

## При несогласии одной из Сторон с решением согласительной комиссии, либо отказе одной из Сторон исполнять решение комиссии, спор решается в порядке, установленном Регламентом.

# Процедура замены ключей ЭП

## Замена Ключа ЭП и пароля осуществляется Клиентом самостоятельно средствами Дистрибутивного пакета в следующих случаях:

### по инициативе Клиента;

### по окончании срока действия Ключа ЭП (использование Ключа ЭП, срок действия которого истек, прекращается автоматически);

### при Компрометации Ключей ЭП.

## При замене Ключей ЭП по инициативе Клиента или по окончании срока действия Ключа ЭП Клиент, не позднее чем за пять рабочих дней до планируемой даты прекращения использования Ключа ЭП, выполняет процедуры в соответствии с пунктом 2.4.1. настоящего Порядка.

## При замене Ключей ЭП в случае Компрометации Ключей ЭП Клиент осуществляет действия в соответствии с разделом 3 Порядка обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK (Приложения №20) к Регламенту.