Порядок получения и использования информационно-торговой системы QUIK с применением Квалифицированной Электронной подписи

[1. Общие положения 1](#_Toc447112187)

[2. Процедура начала работы 1](#_Toc447112188)

[3. Процедура замены Ключей ЭП, Ключей аутентификации, Логина, Пароля, присвоенных Клиенту. 3](#_Toc447112189)

# Общие положения

## Неотъемлемым условием начала и дальнейшего использования Клиентом ИТС QUIK с Квалифицированной ЭП является заключение с Банком Соглашения об использовании квалифицированной электронной подписи и использование Клиентом программного обеспечения средств криптографической защиты информации КРИПТО-ПРО CSP, имеющего действительные на момент использования сертификаты ФСБ России, подтверждающие соответствие программного обеспечения требованиям к средствам электронной подписи, OOO "Крипто-Про".

# 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 Квалифицированной ЭП – с внешним подключаемым программным обеспечением средств криптографической защиты информации КРИПТО-ПРО CSP, имеющим действительные на момент использования сертификаты ФСБ России, подтверждающие соответствие программного обеспечения требованиям к средствам электронной подписи, OOO "Крипто-Про" (далее - ИТС с **Квалифицированной ЭП),** Банк проверяет правильность и полноту заполнения Заявки.

### В случае некорректного или неполного оформления Заявки Банк отказывает в предоставлении услуг, предусмотренных настоящим Порядком.

### В случае корректного оформления Заявки Банк передает Клиенту Дистрибутивный пакет на цифровом носителе Клиента или направляет Дистрибутивный пакет на адрес электронной почты, указанный в Заявлении на обслуживание на финансовых рынках (Приложение №1 или 1А к Регламенту).

## При использовании Квалифицированной ЭП создание и регистрация Ключей ЭП осуществляется в следующем порядке:

### Клиент самостоятельно осуществляет следующие последовательные действия:

#### в отношении Квалифицированной ЭП:

* + - приобретает программное обеспечение средств криптографической защиты информации КРИПТО-ПРО CSP (сертификаты ФСБ России СФ/124-2504, СФ/114-2503 от 12.02.2015) OOO "Крипто-Про", необходимое для использования Ключей ЭП и Квалифицированного сертификата ключа проверки электронной подписи в ИТС QUIK;
    - в соответствии с правилами аккредитованного Минкомсвязи России Удостоверяющего центра получает Ключи ЭП и Квалифицированный сертификат ключа проверки ЭП;
    - передаёт в Банк Квалифицированный сертификат ключа проверки электронной подписи (КСКП) в виде электронного документа на адрес электронной почты [brok@ofc.ru](mailto:brok@ofc.ru) или на адрес электронной почты Уполномоченного лица (Сотрудника) Банка и устанавливает его на Рабочее место Клиента;
    - подписывает два экземпляра Акта признания ключа проверки электронной подписи юридического лица или индивидуального предпринимателя для обмена сообщениями в системе ЭДО ПАО Банк «ФК Открытие» (Приложения №2А к Соглашению об использовании квалифицированной электронной подписи) или Акт признания ключа проверки ЭП физического лица для обмена сообщениями в системе ЭДО ПАО Банк «ФК Открытие» (Приложения №2Б к Соглашению об использовании квалифицированной электронной подписи) (далее – Акт Признания). При этом Клиент контролирует правильность заполнения полей Акта признания;
    - выполняет настройки ИТС QUIK для работы с Квалифицированной ЭП;

#### с Дистрибутивным пакетом:

* + - осуществляет установку Рабочего места Клиента;
    - генерирует (создает) Ключи аутентификации доступа к ИТС QUIK;
    - в процессе генерации Клиент самостоятельно присваивает Логин и Пароль, которые будут использоваться при аутентификации пользователя ИТС QUIK;
    - файл ключа (pubring.txk) направляет на адрес электронной почты [brok@ofc.ru](mailto:brok@ofc.ru) или на адрес электронной почты Уполномоченного лица (Сотрудника) Банка;
    - файл ключа (secring.txk) - хранится на индивидуальном носителе/или компьютере пользователя ИТС QUIK.

### Банк осуществляет следующие последовательные действия:

#### в отношении Квалифицированной ЭП:

* + - проверяет КСКП Клиента на соответствие требованиям, предъявляемым к квалифицированным сертификатам ключа проверки электронной подписи, установленным Федеральным законом №63-ФЗ от 06.04.2011 «Об электронной подписи»;
    - в случае отрицательного результата проверки КСКП Клиента Банк извещает Клиента способами связи, предусмотренными Регламентом, о необходимости повторного выполнения процедуры получения Квалифицированного сертификата ключа проверки ЭП в соответствии с п.2.2.1.1 настоящего Порядка;
    - в случае положительного результата проверки КСКП Клиента Банк:
  1. передает Клиенту для подписи два экземпляра Акта признания;
  2. регистрирует КСКП Клиента в ИТС QUIK после получения подписанного Клиентом экземпляра Акта признания;

#### в отношении Ключей аутентификации:

* + - после получения от Клиента ключа pubring.txk Банк готовит и передает Клиенту для подписания Акт приема-передачи Ключей аутентификации (Приложение №2.1 к Порядку обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK), содержащий сведения:

1. Логин пользователя системы ИТС QUIK;
2. содержание ключа pubring.txk;
3. UID.
   * + регистрирует Ключи аутентификации после получения подписанного Клиентом экземпляра Акта приема-передачи Ключей аутентификации на бумажном носителе.

## Не позднее двух рабочих дней с момента подписания Клиентом Акта признания и Акта приема-передачи Ключей аутентификации Клиент получает возможность совершать операции с использованием ИТС QUIK.

# Процедура замены Ключей ЭП, КЛЮЧей аутентификации, Логина, пароля, присвоенных Клиенту.

## Замена Ключей ЭП осуществляется Клиентом по собственному усмотрению и самостоятельно:

### по инициативе Клиента или по окончании срока действия Ключа ЭП (использование Ключа ЭП, срок действия которого истек, прекращается автоматически).

Клиент не позднее, чем за пять рабочих дней до планируемой даты прекращения использования Ключа ЭП, выполняет процедуры в соответствии с пунктом 2.2.1.1. настоящего Порядка.

### при Компрометации Ключей ЭП и/или Ключей аутентификации, Логина и Пароля Клиент осуществляет действия в соответствии с Разделом 3 Порядка обмена сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK (Приложение №20 к Регламенту).

## Замена Ключей аутентификации, Логина и Пароля осуществляется Клиентом по собственному усмотрению и самостоятельно:

### По инициативе Клиента или по окончании срока действия Ключей аутентификации (если в Акте приема-передачи Ключей аутентификации указан срок действия Ключей аутентификации) Клиент, не позднее чем за пять рабочих дней до планируемой даты прекращения использования Ключей аутентификации, выполняет процедуры в соответствии с пунктом 2.2.1.2. настоящего Порядка.