Руководство по установке и запуску мобильного приложения QUIK

В настоящей инструкции используются термины и сокращения определенные в ПРАВИЛАХ использования программного обеспечения QUIK и простой электронной подписи при использовании программного обеспечения QUIK.

Основные этапы подключения мобильной версии

1. Для начала использования мобильного приложения QUIK необходимо подключить данную услугу в Банке, заполнив соответствующие поля в заявлении при заключении договора.
2. Сохраните утилиту KeyGen с сайта Банка http://www.sksbank.ru/docs/files/KeyGen.zip
3. Сгенерируйте Открытый ключ ПЭП (pubring.txk) и Закрытый ключ ПЭП (secring.txk) с помощью программы генерации ключей KeyGen (ПЭП – простая электронная подпись). (см. раздел 1)
4. Зарегистрируйте Открытый ключ ПЭП в Личном Кабинете https://lk.sksbank.ru/ (см. раздел 1.7)
5. Установите мобильное приложение на свой смартфон или планшет:

- iQUIK – для смартфонов для iOS
- iQUIK HD – для планшетов на iOS
- QUIK Android – для смартфонов и планшетов на Android

6. Настроите подключение к серверу QUIK Банка в мобильном приложении QUIK (см. раздел 3).
7. В случае возникновения вопросов и проблем при подключении необходимо обращаться в техподдержку по адресу QUIK@SKSBANK.RU или по телефону +7(495) 258 61 03.

1. Генерация ключей в программе KeyGen

Программное обеспечение KeyGen предназначено для создания Открытого и Закрытого ключей ПЭП (далее по тексту – Ключи) в среде Windows.

Ключи используются для надежной взаимной идентификации серверной части программного комплекса QUIK и пользователя клиентской части, а также для защиты информации, передаваемой по каналам связи.

Ключ делится на две части - ***открытую*** (публичную) и ***закрытую*** (секретную), Открытый ключ ПЭП и Закрытый ключ ПЭП соответственно. Секретная часть хранится у стороны, создавшей ключ, и используется для создания Простой электронной подписи. Публичная часть предназначена для передачи другой стороне для возможности проверки подлинности Простой электронной подписи в Электронном документе.

Для взаимной идентификации пользователю QUIK необходимо иметь свой секретный ключ и публичный ключ.

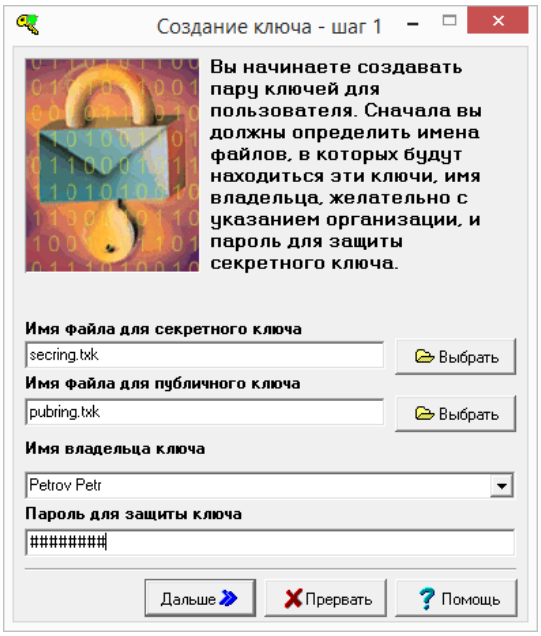
1.1 Создание ключей

При создании ключей рекомендуется использовать сменный носитель, например, USB-флэш-накопитель.

1.2 Имя и пароль

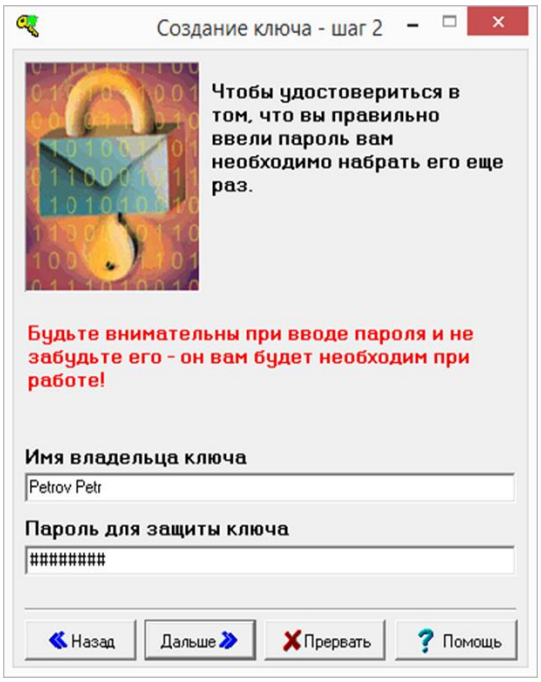
После скачивания архива KeyGen.zip и распаковки для запуска необходимо использовать исполняемый файл KeyGen.exe. Имя владельца ключа используется для регистрации пользователя на сервере и авторизации пользователя при подключении. Пароль, сформированный в соответствии с требованиями Правил (последовательность из строчных и прописных латинских букв и цифр, специальных символов состоящая не менее чем из 6 знаков), защищает секретную часть ключа пользователя от несанкционированного использования.

На первом шаге создания ключа выбираются имена файлов для публичной и секретной части создаваемого ключа, имя его владельца и пароль для защиты секретной части ключа. В двух верхних строках укажите путь для сохранения создаваемых ключей доступа. Кнопки «Выбрать» позволяют выбрать путь и директорию, где будут храниться файлы.



- «Имя файла для секретного ключа» - имя и директория файла с секретным ключом пользователя.
- «Имя файла для публичного ключа» - имя и директория файла с публичным ключом пользователя.
- «Имя владельца ключа» - имя пользователя системы QUIK; необходимо указать с использованием латинских букв.
- «Пароль для защиты ключа» - пароль для защиты секретного ключа, который запрашивается при подключении к серверу QUIK.

Для перехода на следующий шаг нажмите кнопку «Дальше». Остановить создание ключей можно нажатием кнопки «Прервать». Нажатием кнопки «Помощь» можно открыть справку по программе.



1.3 Подтверждение пароля

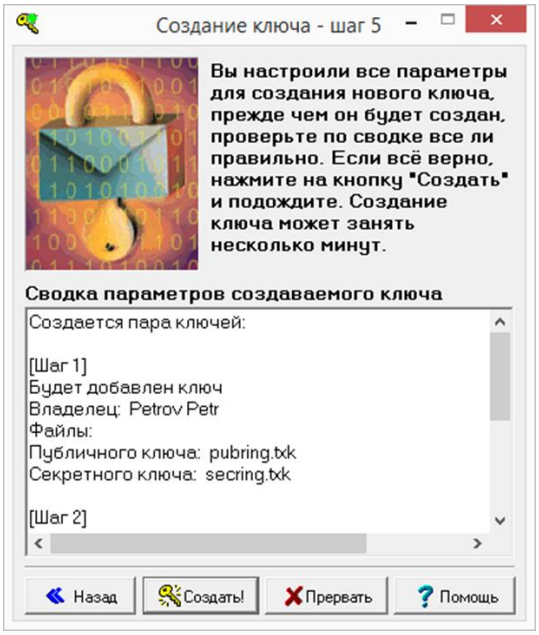
На втором шаге необходимо подтвердить пароль, набрав его снова. При наборе пароля обратите внимание на выбранный язык и регистр шрифта, во избежание неправильного ввода пароля при соединении с сервером.

- «Имя владельца ключа» - справочное поле для проверки правильности введенной информации об имени пользователя. Если необходимо внести изменения, вернитесь на предыдущий шаг создания ключей нажатием кнопки «Назад».

- «Пароль для защиты ключа» - поле для повторного ввода пароля, указанного на предыдущем шаге.

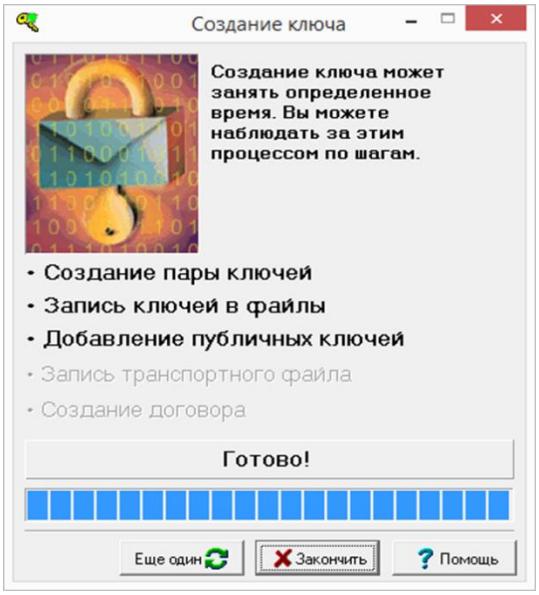
1.4 *Транспортный файл*

Данный пункт пропускаем, так как создание транспортного файла не требуется. Выбираем «Дальше».



1.5 *Подтверждение параметров*

На данном шаге предлагается проверить правильность введенных параметров. Для этого в поле вывода пишется сводная информация по выбранным параметрам. Необходимо проверить правильность указания всех параметров в информационном поле «Сводка параметров создаваемого ключа» и начать генерацию ключей нажатием кнопки «Создать». В случае необходимости изменения настроек вернитесь к предыдущим шагам нажатием кнопки «Назад».



1.6 *Завершение*

Программа отображает процесс создания ключа, отмечая производимый шаг.

Нажатие кнопки «Закончить» завершает работу с программой. Процесс генерации ключей завершен.

После завершения создания ключей в каталоге, указанном на Шаге 1 появятся два файла – pubring.txk и secring.txk. В первом файле находятся публичные части ключа пользователя и сервера (SKSBank). Во втором – секретная часть ключа пользователя.

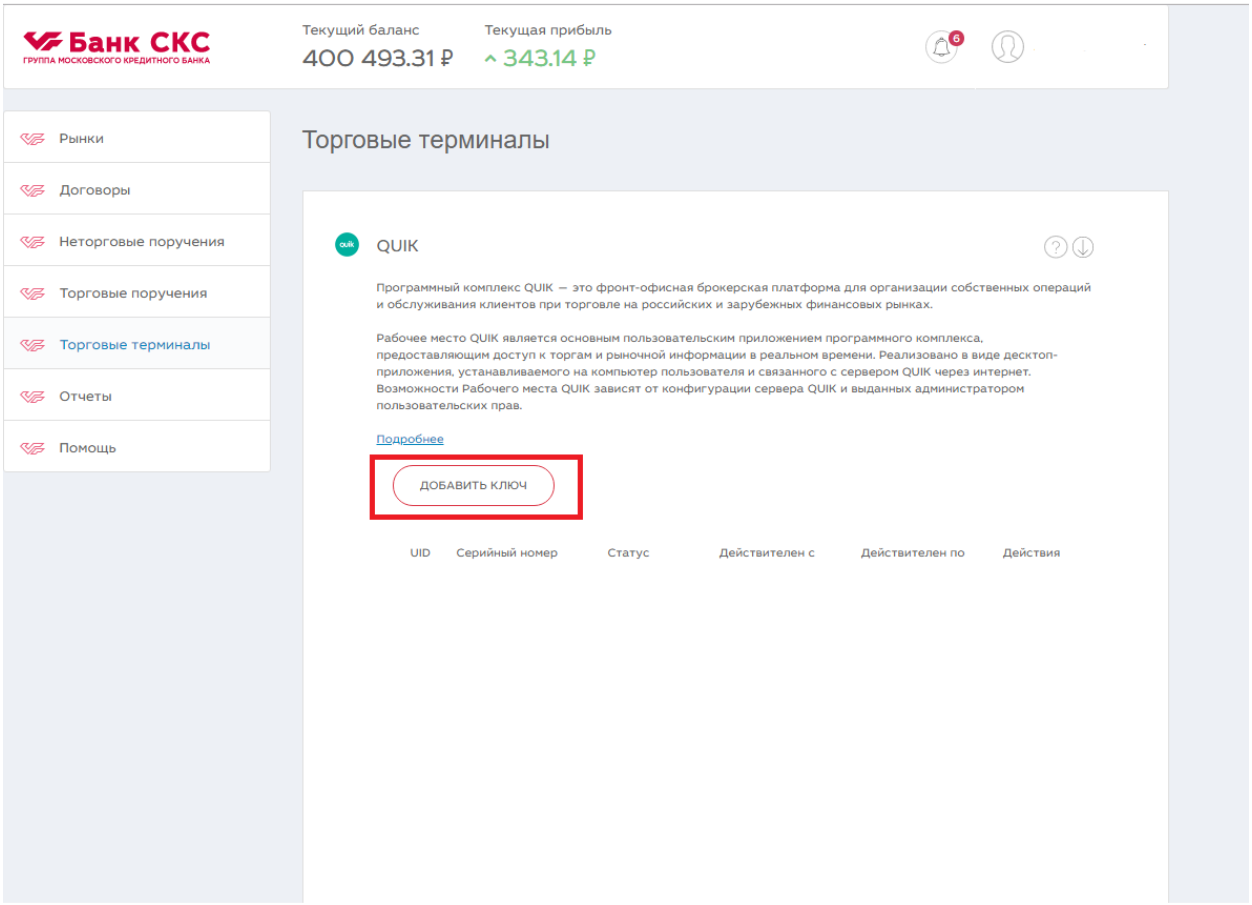
В целях предотвращения несанкционированного доступа к системе QUIK рекомендуется не сохранять в

настройках программы пароль для доступа к ключу, а также не разглашать никому свой пароль. В случае утери мобильного устройства (телефона/планшета и т.д.) во избежание несанкционированного доступа к своему торговому счету немедленно сообщите в Банк Администратору сервера QUIK о компрометации ключа.

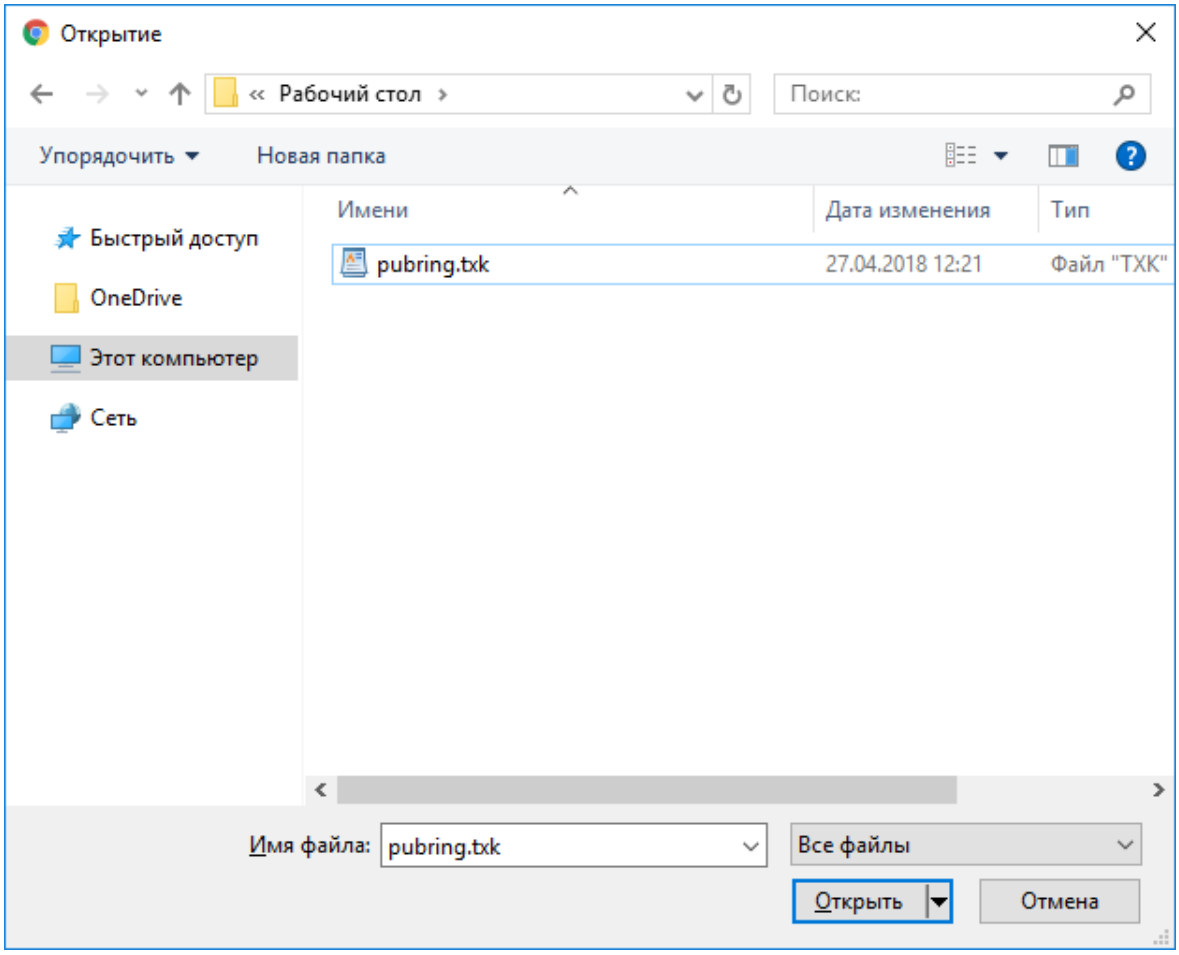
1.7 Регистрация открытого (публичного) ключа в Личном Кабинете

Самостоятельно зарегистрировать новый ключ через Личный Кабинет Вы можете в соответствующем сервисе в разделе «Торговые терминалы».

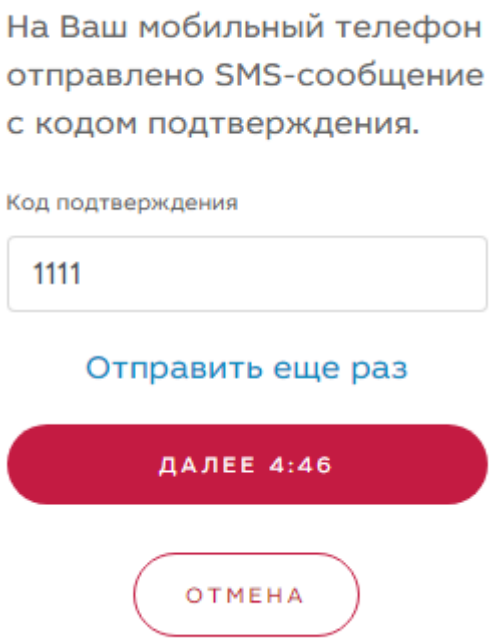
1) Выберите в меню раздел «Торговые терминалы». Далее нажмите кнопку «Добавить ключ».



2) В открывшемся окне выберите файл публичного ключа pubring.txk, сгенерированный с помощь генератора ключей KeyGen и нажмите кнопку «Открыть».



3) Подтвердите действие с помощь SMS-сообщения, которое придет Вам на телефон. В открывшемся окне в поле «Код подтверждения» введите код подтверждения. Нажмите кнопку «Далее»



4) После загрузки публичного ключа следите за статусом регистрации:

UID	Серийный номер	Статус	Действителен с	Действителен по	Действия
	C2554E24856DFE41	Загружен			

5) После изменения статуса на «Активный» Вы можете подключиться к серверу Quik.

UID	Серийный номер	Статус	Действителен с	Действителен по	Действия
	C2554E24856DFE41	Активный	05.04.2018	06.02.2025	Отозвать

Активными могут оставаться только два ключа. В дальнейшем при активации третьего и последующих ключей необходимо сначала отозвать один из двух активных ключей. Все последующие ключи, зарегистрированные без предварительного отзыва активного ключа, будут заблокированы автоматически.

6) Для отзыва действующего активного ключа необходимо в разделе меню «Действие» нажать на соответствующую ссылку «Отозвать» и подтвердить действие с помощью SMS-кода. Отозванный ключ будет иметь статус «Заблокирован».

UID	Серийный номер	Статус	Действителен с	Действителен по	Действия
	C2554E24856DFE41	Заблокирован	05.04.2018	06.02.2025	

РЕГИСТРАЦИЯ ВАС В КАЧЕСТВЕ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ QUIK, ОСУЩЕСТВЛЯЕТСЯ В РАБОЧЕЕ ВРЕМЯ С 9:00 ДО 17:00 ПО МОСКОВСКОМУ ВРЕМЕНИ.

ЕСЛИ ВАМ НЕ УДАЛОСЬ УСТАНОВИТЬ СОЕДИНЕНИЕ С СЕРВЕРОМ QUIK (ПОДКЛЮЧИТЬСЯ К ПРОГРАММЕ), ВАМ НЕОБХОДИМО СВЯЗАТЬСЯ С ТЕХНИЧЕСКОЙ ПОДДЕРЖКОЙ БАНКА ПО АДРЕСУ ЭЛЕКТРОННОЙ ПОЧТЫ QUIK@SKSBANK.RU.

Если у Вас имеется договор индивидуального инвестиционного счета (далее – ИИС), то отдельный ключ для договора ИИС генерировать не требуется.

2. Установка мобильного приложения QUIK

2.1 iQUIK – для смартфонов iOS ссылка для установки
https://itunes.apple.com/ru/app/iquik/id429888411?mt=8
2.2 iQUIK HD – для планшетов на iOS ссылка для установки

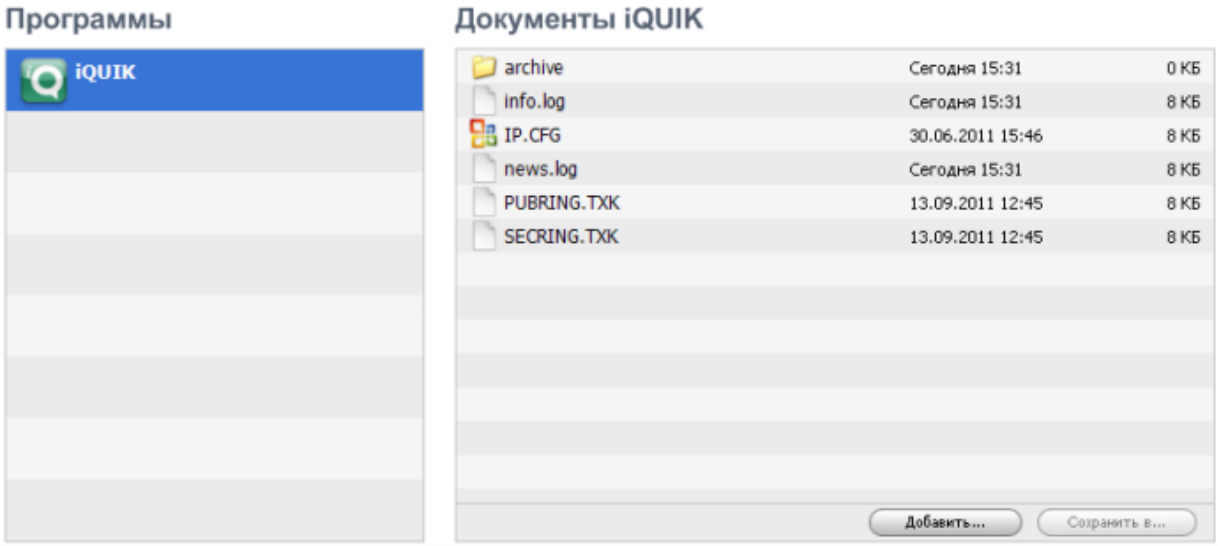
https://itunes.apple.com/ru/app/iquik-hd/id447574997?mt=8

2.3 QUIK Android – для смартфонов и планшетов на Android ссылка для установки
https://play.google.com/store/apps/details?id=air.QUIKAndroid&hl=ru

3. Запуск программы QUIK

3.1. iQUIK.

После установки мобильного приложения QUIK необходимо сохранить ключи на мобильном устройстве с помощью программы iTunes. После копирования из каталога, где ранее были сохранены ключи, необходимо нажать кнопку «Синхронизировать».



После копирования ключей необходимо настроить подключение к серверу QUIK СКС Банка.

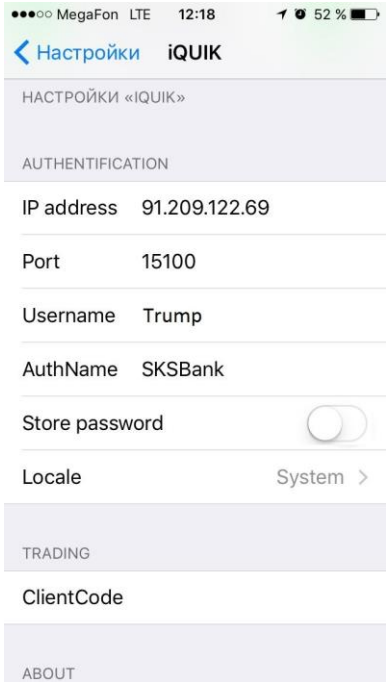
Зайдите в меню «Настройки / iQUIK» и укажите следующие параметры:

Имя соединения: Сервер QUIK СКС Банка

IP : 91.209.122.69

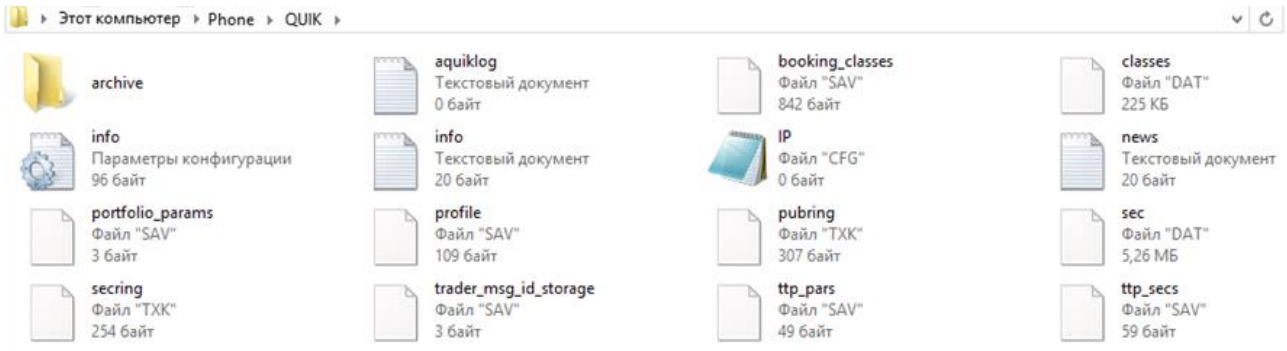
Порт: 15100

Ключ сервера (AuthName): SKSBank



3.2. *QUIK Android.*

После установки мобильного приложения необходимо скопировать ключи в директорию с программой на мобильном устройстве из каталога, где ранее были сохранены ключи.



После копирования ключей необходимо настроить подключение к серверу QUIK СКС Банка при первом запуске QUIK. Выберите пункт «Добавить соединение».

Заполните открывшуюся форму следующими параметрами:

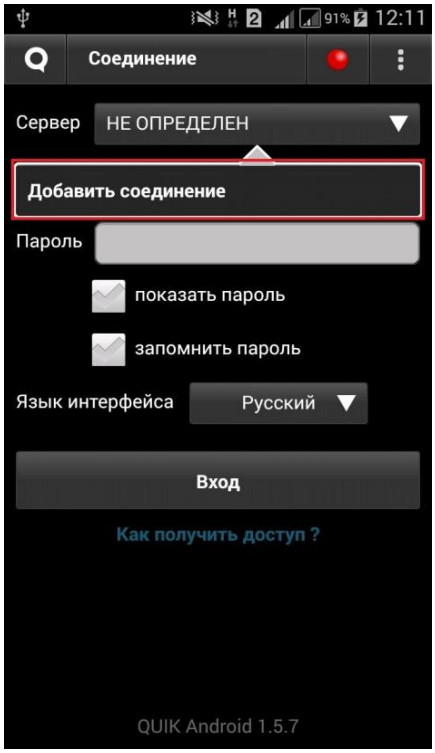
Имя соединения: Сервер QUIK СКС Банка

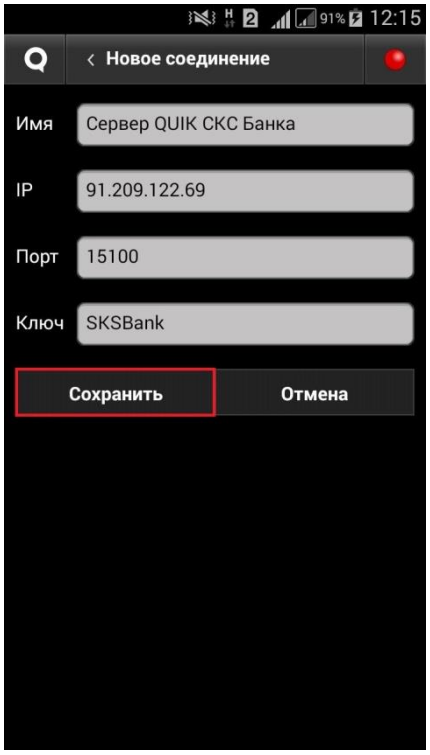
IP : 91.209.122.69

Порт: 15100

Ключ: SKSBank

Далее нажмите кнопку «Сохранить».





Статус подключения мобильного QUIK можно проверить с помощью индикатора подключения к серверу QUIK: