Приложение №1 к Приказу от 10.10.2016г. №409

УТВЕРЖДАЮ:
Председатель Правления
АО «КОШЕЛЕВ-БАНК»

_____ **О.В. Багаев**

«10» 10 2016г.

Руководство пользователя по формированию ключей доступа в информационно-торговую систему QUIK

Самара 2016

1. Общие положения

1.1. Настоящее Руководство разработано в соответствии с технической и эксплуатационной документацией разработчика программного обеспечения ИТС QUIK, а также согласно Условиям обеспечения технического доступа к информационно-торговой системе QUIK (далее – Условия), нормативным и внутренним регламентирующим документам АО «КОШЕЛЕВ-БАНК» (далее – Банк).

1.2. Данное Руководство описывает порядок действий Пользователя при регистрации в ИТС QUIK, формировании им ключей доступа, а также в случае их компрометации в системе.

1.3. Настоящее Руководство рекомендует соблюдение Пользователем мер по снижению рисков при работе с удаленным рабочем местом ИТС QUIK в соответствии с Приложением №7 к Условиям.

2. Подготовка к работе

2.1. Скачайте с официального сайта Банка www.koshelev-bank.ru программу генерации ключей KeyGen.

2.2. Программа генерации ключей KeyGen предназначена для создания криптографических ключей (ключей доступа) в ИТС QIUK.

2.3. Ключ доступа используется для надежной взаимной идентификации серверной части программного комплекса QUIK и клиентской части пользователя, а также для защиты информации, передаваемой по каналам связи.

2.4. Ключ делится на две части – ***открытую*** (публичную) и ***закрытую*** (секретную), которые также могут называться публичным и секретным ключами соответственно. Секретная часть хранится у создавшего ключ пользователя (владельца ключа доступа), публичная часть предназначена для передачи Банку.

2.5. Каждая часть хранится в файле специального формата. Соблюдайте правила выбора пароля доступа к секретным ключам и обеспечьте надлежащее использование и хранение криптографических ключей в соответствии Приложением №7 к Условиям.

3. KeyGen. Создание ключей доступа в ИТС QUIK

3.1. Распакуйте скаченный с официального сайта Банка архив KeyGen.

Шаг 1. Имя и пароль

3.2. Для создания криптографических ключей запустите программу KeyGen.exe (Рис. 1).

При создании ключей доступа рекомендуется использовать сменный носитель, например, флэш-карту!!!

3.3. С помощью кнопки «Выбрать» укажите пути сохранения файлов криптографических ключей (Рис. 2). Например, съемный диск: \Ключи…\....

3.4. Введите имя владельца ключа доступа (Рис. 3) в формате *Фамилия Имя Отчество* (при наличии) и пароль доступа к секретному ключу (Рис. 4).

Пароль должен иметь длину не менее 8 (восьми) символов, содержать не менее 2 (двух) цифр и 2 (двух) букв, а также буквы верхнего и нижнего регистра!!!

3.5. Для перехода на следующий шаг нажмите кнопку «Дальше». Чтобы остановить процесс создания криптографических ключей, нажмите кнопку «Прервать».

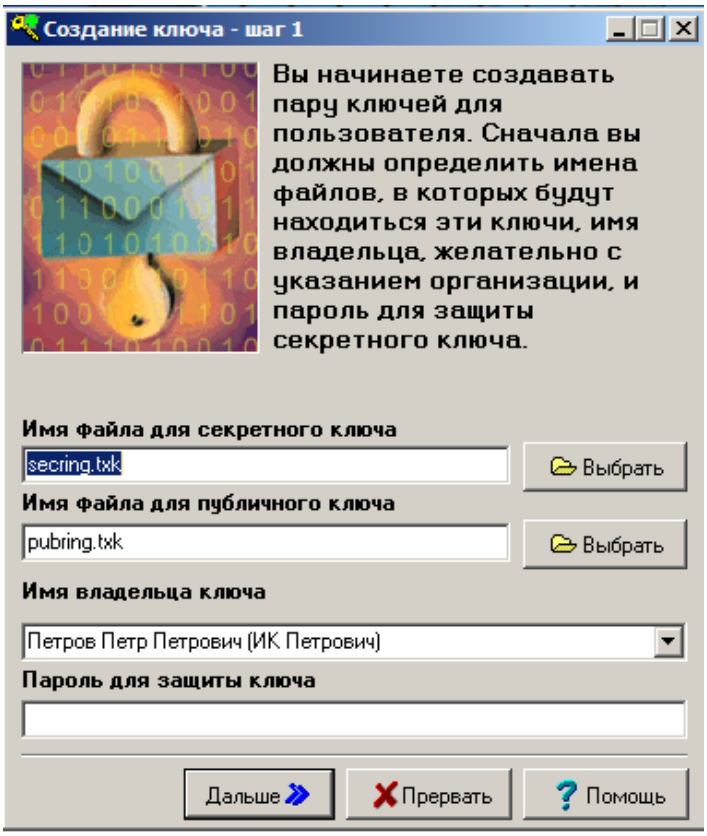

Рис. 1

Рис. 2

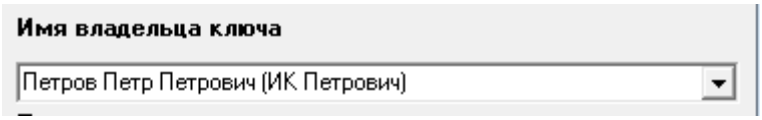

Рис. 3

Рис. 4

Шаг 2. Подтверждение пароля

3.6. На втором шаге подтвердите пароль, набрав его снова (Рис. 5).

При наборе пароля обратите внимание на выбранный язык и регистр шрифта, во избежание неправильного ввода пароля при соединении с сервером!!!

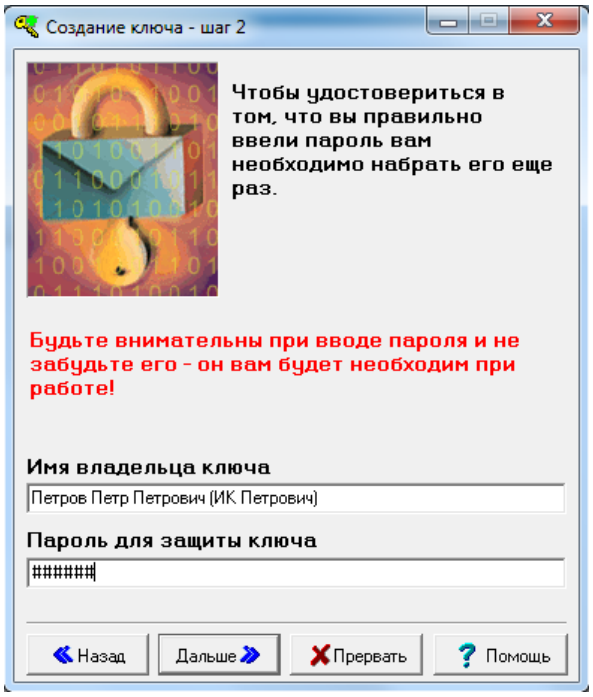

Рис. 5

3.7. После подтверждения пароля перейдите к следующему шагу, нажав кнопку «Дальше».

Шаг 5. Подтверждение параметров

3.8. Проверьте правильность введенных параметров, для этого в поле вывода сводной информации проверьте корректность всех указанных ранее параметров (Рис. 6). В случае необходимости изменения настроек вернитесь к предыдущим шагам нажатием кнопки «Назад». После того, как Вы убедились, что все параметры верны, нажмите кнопку «Создать».

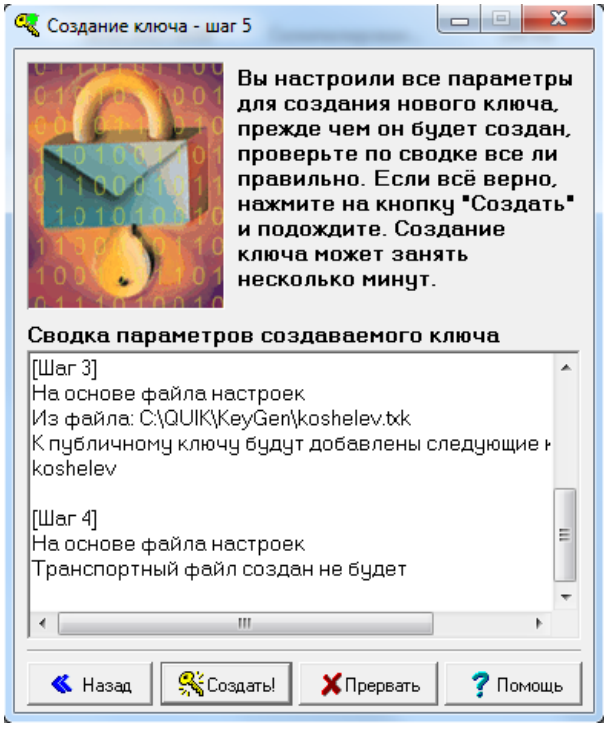

Рис. 6

Шаг 6. Создание ключей

3.9. После нажатия кнопки «Создать» появится диалоговое окно (Рис. 7), в котором нужно набирать произвольный текст, для запуска процесса создания криптографических ключей. Для создания случайных чисел программа замеряет время между нажатием клавиш. Как

только необходимое количество случайно информации будет введено, начнется процесс создание ключа доступа (Рис. 8).

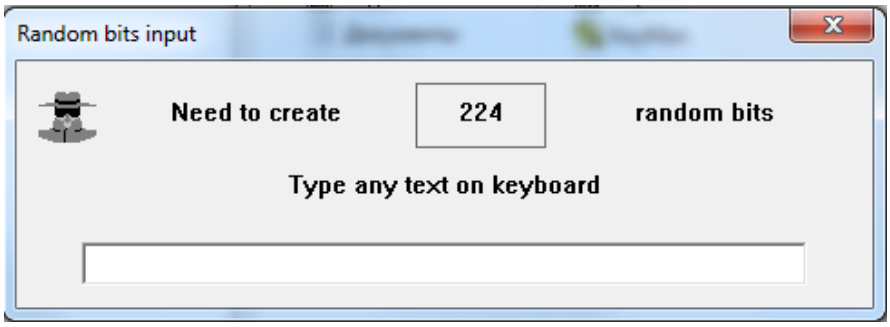

Рис. 7

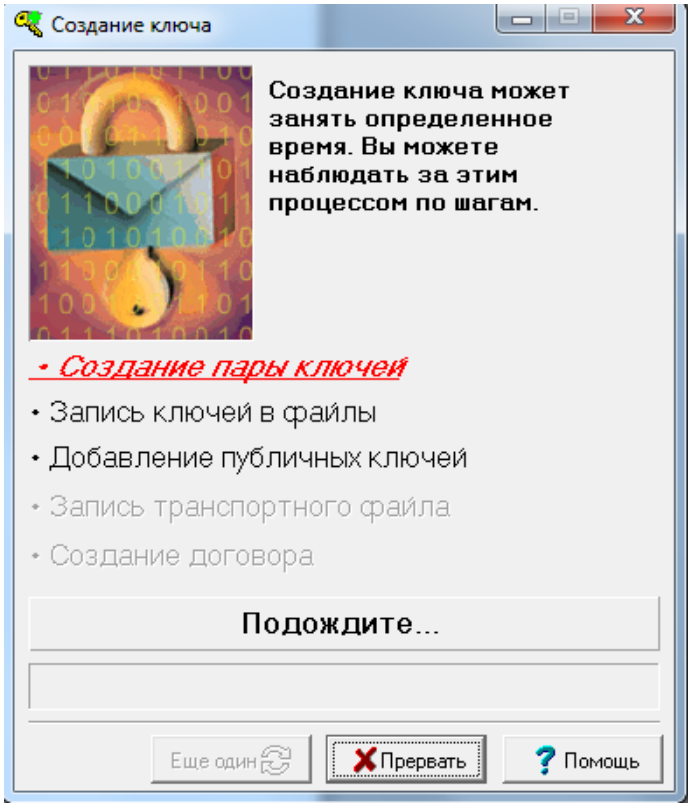

Рис. 8

Шаг 7. Завершение

3.10. Программа отображает процесс создания ключа, отмечая производимый шаг. После того как появится сообщение о готовности ключа доступа «Готово!», нажатием кнопки «Закончить» завершить работу с программой (Рис. 9).

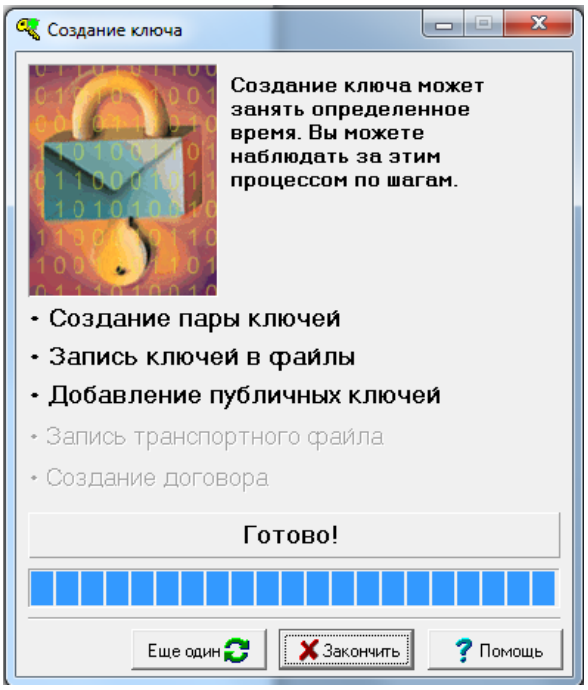

Рис. 9

3.11. После завершения создания криптографических ключей в каталоге, указанном на Шаге 1 п.3.3 настоящего Руководства, появятся 2 (два) файла – pubring.txk (публичная часть ключа пользователя) и secring.txk (секретная часть ключа пользователя):

– **публичная** (открытая) часть, файл pubring.txk – уникальная последовательность символов, соответствующая секретному (закрытому) ключу, предназначенная для шифрования потока данных. Файл pubring.txk передается в Банк для регистрации в системе. Функционирует только при наличии секретной части.

– **секретная** (закрытая) часть, файл secring.txk – уникальная последовательность символов, известная только владельцу ключа доступа и предназначенная для шифрования потока данных. Не подлежит передаче посторонним лицам, в том числе **НЕ** передается в Банк. Требует соблюдения условий безопасного хранения.

В целях предотвращения несанкционированного доступа к ИТС QUIK храните ключ доступа на съемном носителе. Не передавайте носитель ключа третьим лицам! Не сообщайте третьим лицам пароль от секретного ключа! Подключайте носитель ключа доступа к Устройству доступа только на время работы в системе. В случае утери (хищения) или повреждения носителя ключа немедленно свяжитесь с Банком!!!

3.12. Генерация ключей доступа в ИТС QUIK завершена!

4. Регистрация ключа доступа в системе

4.1. Для регистрации ключа доступа необходимо предоставить в Банк следующие документы:

– Комплект документов в рамках Условий предоставления брокерских услуг клиентам;

– Договор присоединения (Приложение №3 к Условиям);

– Заявление о предоставлении доступа к ИТС QUIK (Приложение № 1 к Условиям - для физических лиц, Приложение № 2 к Условиям – для юридических лиц);

– Акт приема-передачи публичного (открытого) ключа (Приложение №4 к Условиям).

4.2. Отправить в Банк файл pubring.txk, сгенерированный на шаге 7, на адрес электронной почты keys@k-bnk.ru (Рис. 10), при этом:

– письмо должно быть направлено с адреса электронной почты, указанного в Анкете Клиента;

– в теме письма должен быть указан 5-тизначный Код Клиента;

– во вложении к письму должен быть приложен файл pubring.txk.

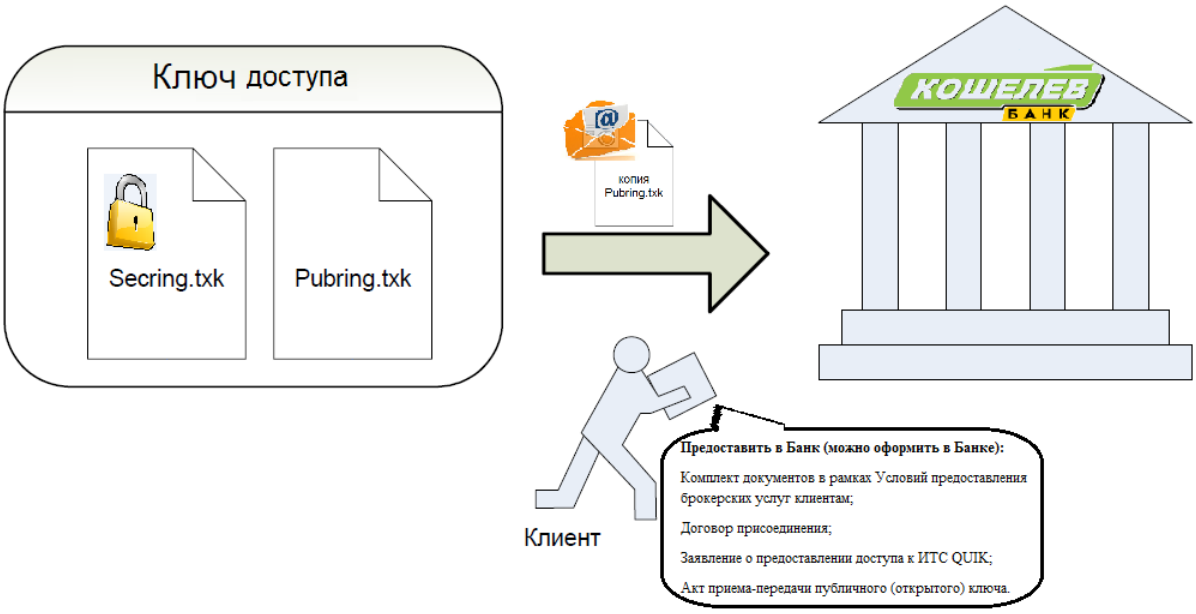

Рис. 10

Банк регистрирует ключи доступа Клиента не позднее рабочего дня, следующего за днем предоставления документов, указанных в п. 4.1 настоящего Руководства, отправки в Банк публичного ключа в соответствии с п. 4.2 Руководства и выполнения Клиентом его обязанностей, предусмотренных Условиями и иными сопутствующими договорными отношениями с Банком!!!

5. Смена ключа доступа в системе

5.1. Клиент/Уполномоченный представитель Клиента (при наличии доверенности) может в любой момент времени произвести замену ключей доступа.

Рекомендованный срок плановой смены ключей доступа 1 (один) год с момента изготовления предыдущей пары криптографических ключей!!!

5.2. Замена ключей доступа должна быть произведена в случае их компрометации. К событиям, на основании которых Клиент принимает решение о компрометации ключа, относятся следующие:

– утрата/хищение носителя ключа доступа;
– утрата носителя ключа доступа с последующим обнаружением;
– временный доступ неуполномоченных лиц к информации, содержащейся на носителе ключа доступа;
– иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к криптографическим ключам третьих лиц.

В случае принятия решения о компрометации ключа Клиент обязан позвонить и уведомить об этом Банк, а также произвести все необходимые мероприятия по блокировке ключа доступа в соответствии с разделом 6 Условий.

5.3. Формирование новых ключей доступа осуществляются аналогично п.3 настоящего Руководства.

Создание новых ключей доступа должно производиться на носитель, не содержащий файлы заменяемых ключей. Удостоверьтесь, что создаете файлы в пустую папку!!!

5.4. По факту регистрации нового ключа доступа Клиенту/Уполномоченному представителю Клиента предоставляется доступ в ИТС QUIK в соответствии с новыми ключами и блокируется доступ с использованием старых, за исключением случая компрометации ключа.