

Создание ключей

При создании ключей рекомендуется использовать дискету или другой сменный носитель, например, флэш-карту.

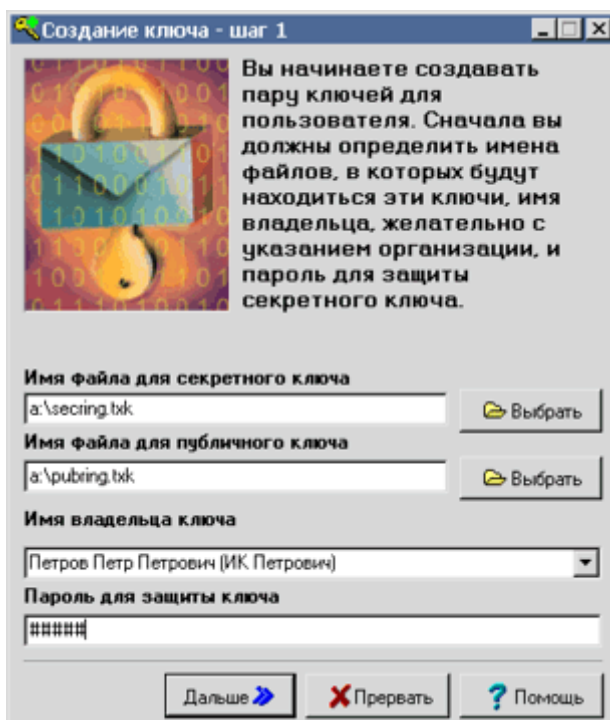
- [Шаг 1. Имя и пароль](#)
- [Шаг 2. Подтверждение пароля](#)
- [Шаг 3. Выбор ключа сервера](#)
- [Шаг 4. Транспортный файл](#)
- [Шаг 5. Подтверждение параметров](#)
- [Шаг 6. Создание ключей](#)
- [Шаг 7. Завершение](#)

Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 1. Имя и пароль

Имя владельца ключа используется для регистрации пользователя на сервере и авторизации пользователя при подключении. Пароль 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.



Создание ключа - шаг 1

Вы начинаете создавать пару ключей для пользователя. Сначала вы должны определить имена файлов, в которых будут находиться эти ключи, имя владельца, желательно с указанием организации, и пароль для защиты секретного ключа.

Имя файла для секретного ключа
a:\secreting.tsk

Имя файла для публичного ключа
a:\pubbring.tsk

Имя владельца ключа
Петров Петр Петрович (ИК Петрович)

Пароль для защиты ключа
#####

- «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.

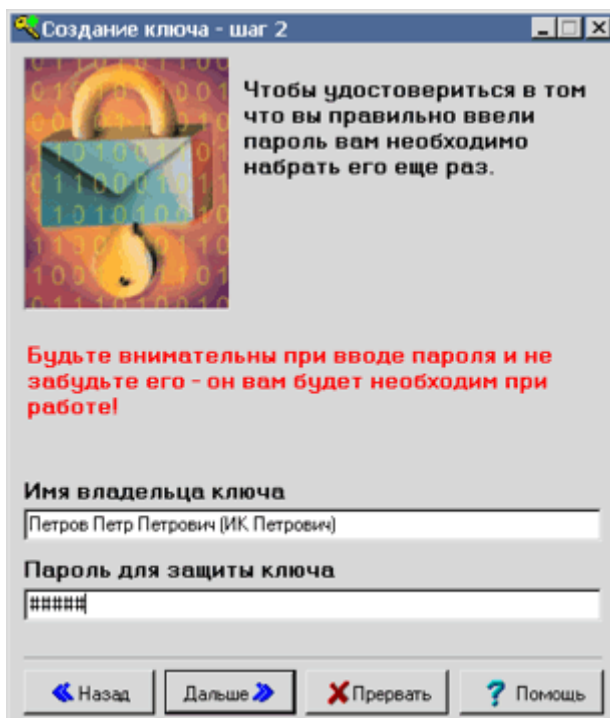
- «Имя владельца ключа» - имя пользователя системы QUIK.
- «Пароль для защиты ключа» - пароль для защиты секретного ключа, который запрашивается при подключении к серверу QUIK. Пароль может состоять из набора произвольных символов, минимальная длина пароля устанавливается параметром **MinPwdLen** секции **Key Management** [файла настроек](#).

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

Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 2. 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.

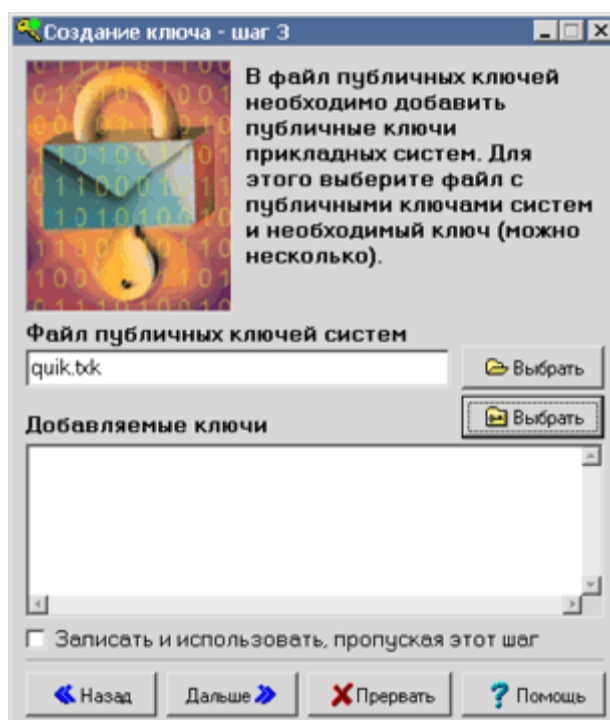


- «Имя владельца ключа» - справочное поле для проверки правильности введенной информации об имени пользователя. Если необходимо внести изменения, вернитесь на предыдущий шаг создания ключей можно нажатием кнопки «Назад».
- «Пароль для защиты ключа» - поле для повторного ввода пароля, указанного на предыдущем шаге.

Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 3. Выбор ключа сервера

На третьем шаге создания ключа выбираются публичные ключи сервера QUIK, добавляемые к создаваемому публичному ключу. Для добавления необходимо сначала выбрать файл публичных ключей прикладных систем, затем в нем указать набор ключей, предназначенных для передачи.



- «Файл публичных ключей систем» - имя и директория файла ключей других прикладных систем.
- «Добавленные ключи» - выбор ключа сервера QUIK.
- «Записать и использовать, пропуская этот шаг» - если флажок включен, то при повторном запуске программа будет пропускать этот шаг и автоматически добавлять записанные ключи из запомненного файла.

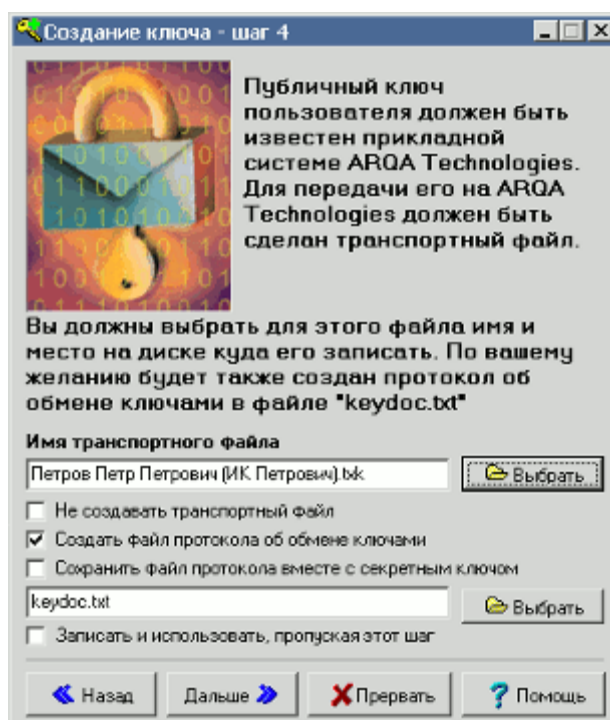
Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 4. Транспортный файл

Публичный ключ пользователя должен быть доступен серверной (центральной) части программного комплекса системы QUIK. Для этого ключ должен быть помещен в так называемый транспортный файл, который передается администратору сервера. На четвертом шаге необходимо выбрать имя для транспортного файла, либо отказаться от его создания.

Замечание:

В случае отказа от создания транспортного файла можно передать публичный ключ.

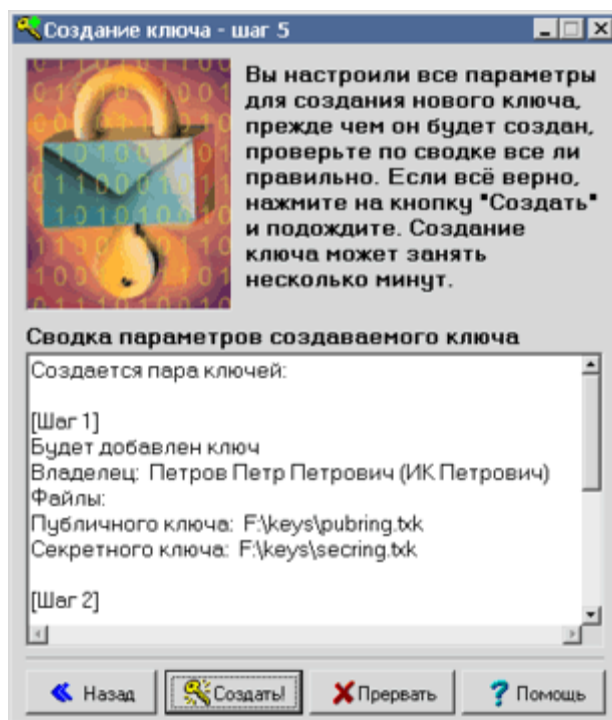


- «Имя транспортного файла» - название транспортного файла с расширением .tkk. Если значение по умолчанию не задано значением параметра **Export** из [файла настроек](#), то начальное значение параметра - «имя пользователя.tkk» в текущем каталоге.
- «Не создавать транспортный файл» - признак отказа от создания такого файла.
- «Создать файл протокола об обмене ключами» - признак создания файла с [протоколом передачи ключей](#).
- «Сохранить файл протокола вместе с секретным ключом» – настройка сохранения файла протокола. Возможные значения:
 - настройка включена – файл протокола сохраняется в каталог с секретным ключом. В поле ввода пути для сохранения файла протокола отображается текущий путь до файла с секретным ключом. Поле недоступно для редактирования;
 - настройка отключена – в поле отображается текущий путь для файла протокола, заданный в `crypto.cfg`. Поле доступно для редактирования.
- «Записать и использовать, пропуская этот шаг» - если флажок включен, то при повторном запуске программа будет пропускать этот шаг, используя запомненные настройки.

Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 5. Подтверждение параметров

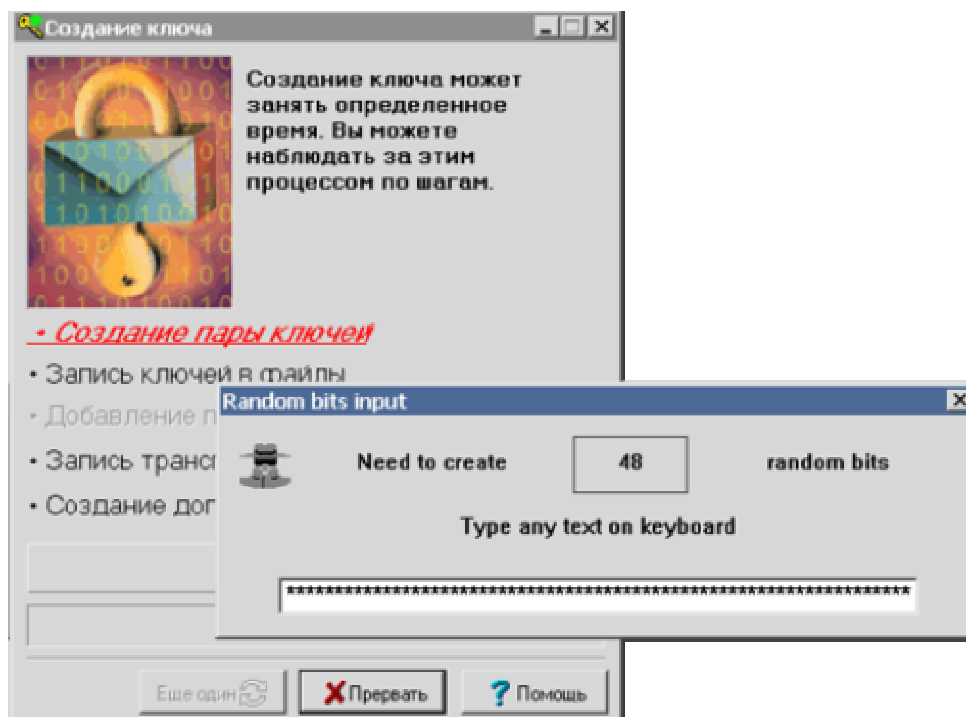
На пятом шаге предлагается проверить правильность введенных параметров. Для этого в поле вывода пишется сводная информация по выбранным параметрам. Необходимо проверить правильность указания всех параметров ключа и начать генерацию ключей нажатием кнопки «Создать». В случае необходимости изменения настроек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



Руководство пользователя KeyGen © ARQA Technologies / www.quik.ru

Шаг 6. Создание ключей

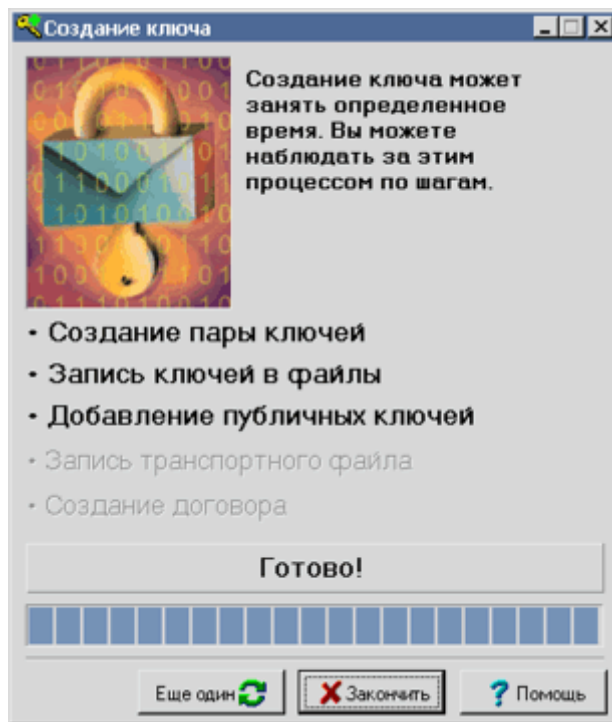
Начинается формирование ключей. В самом начале процесса их создания программе необходимо некоторое количество случайной информации. Поэтому появляется специальное диалоговое окно, в котором нужно набрать произвольный текст.



Для создания случайных чисел программа замеряет время между нажатиями клавиш. Как только необходимое количество случайной информации получено, начинается создание ключа.

Шаг 7. Завершение

Программа отображает процесс создания ключа, отмечая производимый шаг.



Нажатие кнопки «Закончить» завершает работу с программой. Если требуется продолжить создание ключей, нажмите кнопку «Еще один».

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. Во втором – секретная часть ключа пользователя.

В целях предотвращения несанкционированного доступа к системе QUIK рекомендуется хранить эти ключи отдельно от программы, в которой они используются, а также не разглашать никому свой пароль.