Инструкция

по настройке ИТС QUIK

Содержание

1. Технические требования 2
2. Установка комплекта программ с помощью мастера установки Start.bat …..…….. 2
2.1. Установка eToken ….....……..... 3
2.2. Установка КриптоПро .……..... 5
2.3. Установка библиотеки Microsoft CAPICOM …….…... 8
2.4. Установка QUIK ……..……...……..…..10
3. Генерация ключей QUIK 11
4. Настройка QUIK 13
5. Работа с QUIK 17
6. Повышение уровня защищенности QUIK 17
7. Удаление закрытого ключа с eToken 20
8. Изменение пароля (PIN-кода) eToken 22

1. Технические требования.

Рекомендуется ознакомиться с актуальными техническими требованиями рабочего места QUIK на официальном сайте разработчика ARQA Technologies по ссылке:

https://arqatech.com/ru/products/quik/terminals/user-applications/quik-workstation/

2. Установка комплекта программ с помощью мастера установки Start.bat.

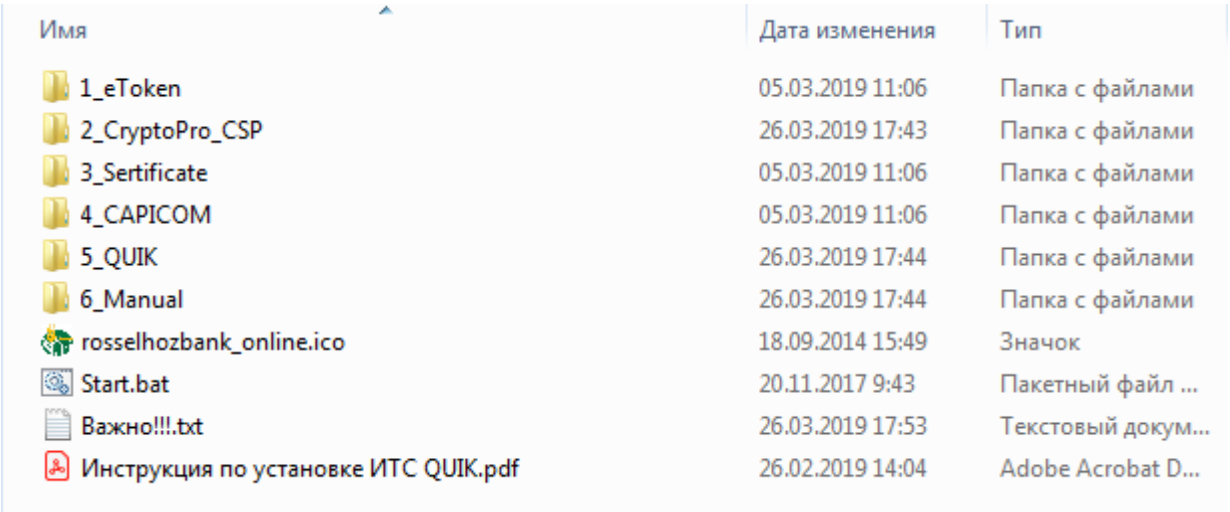
Установка программ происходит автоматически после запуска Start.bat от имени администратора.

Перед началом автоматической установки:

1. Необходимо убедиться, что eToken извлечен из порта USB.

2. Требуется скопировать каталог RSHB_soft с носителя, выданного в отделении Банка в корень диска (к примеру C:\RSHB_soft\).

Для установки необходимо запустить файл из комплекта предоставленного программного обеспечения: **Start.bat** (в каталоге RSHB_soft) от имени **Администратора** (нажать правой кнопкой и выбрать **«Запуск от имени администратора»**).

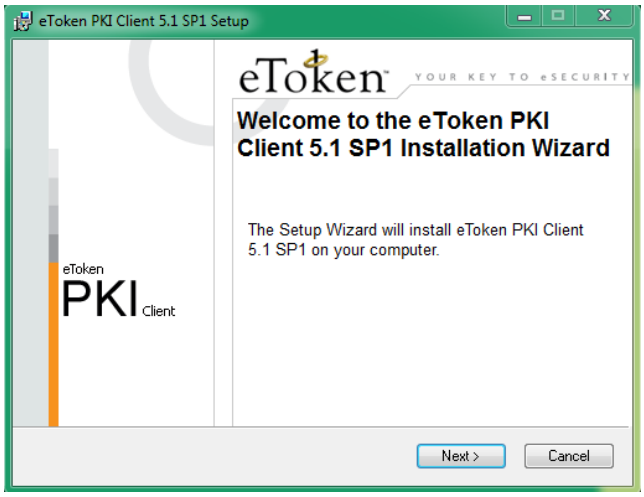


В процессе установки каталог с программой QUIK (RSHB_QUIK) будет установлен в корень диска (к примеру C:\RSHB_QUIK\).

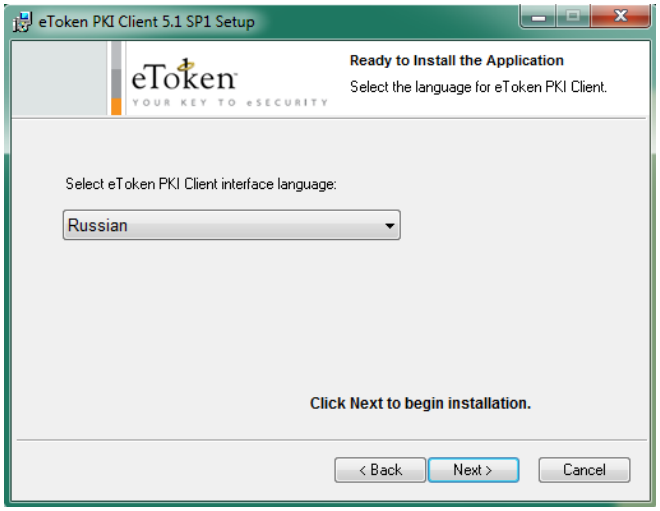
2.1. Установка eToken.

После запуска мастера установки Start.bat автоматически запустится программа установки eToken.

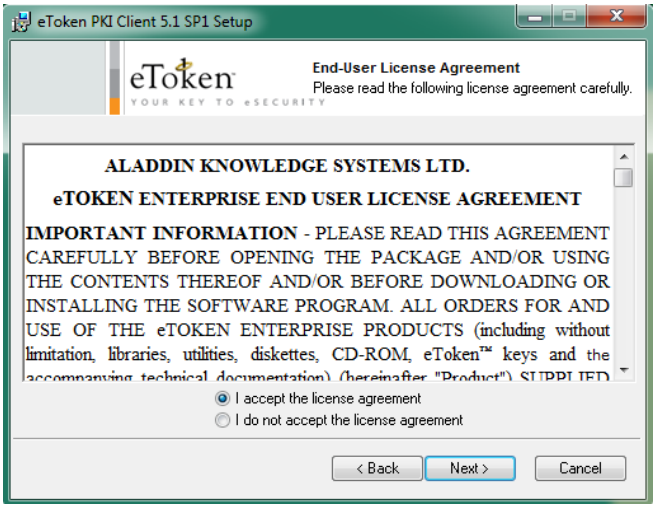
2.1.1. Нажмите кнопку «Next»



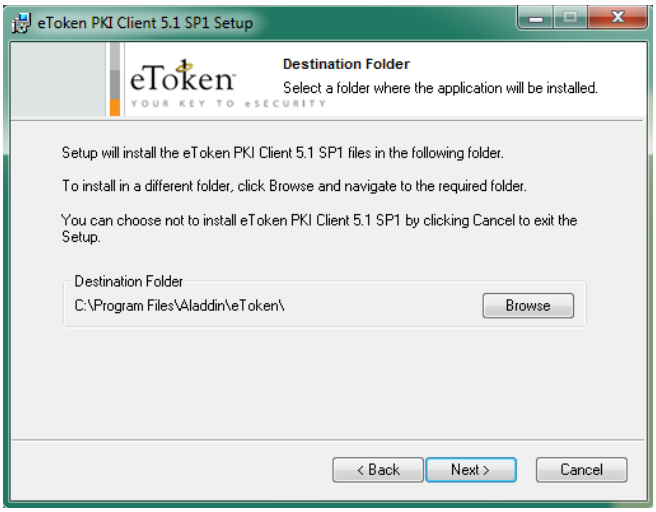
2.1.2. Из списка языков выберите «Russian». Нажмите кнопку «Next»



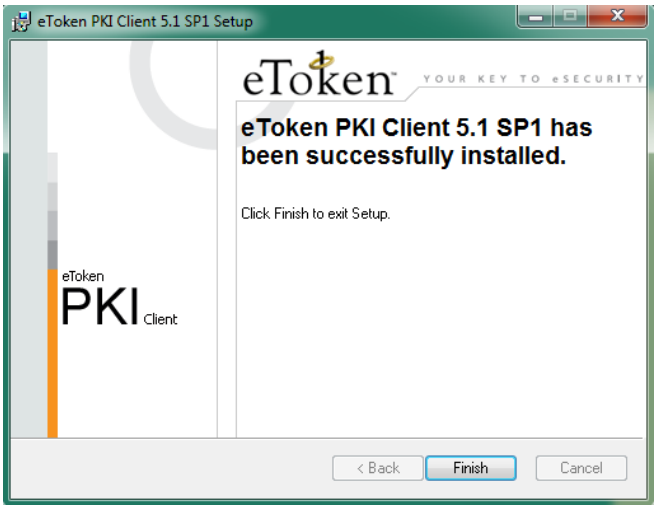
2.1.3. Выберите «I accept the license agreement». Нажмите кнопку «Next»



2.1.4. Нажмите кнопку «Next»



2.1.5. Нажмите кнопку «Finish»

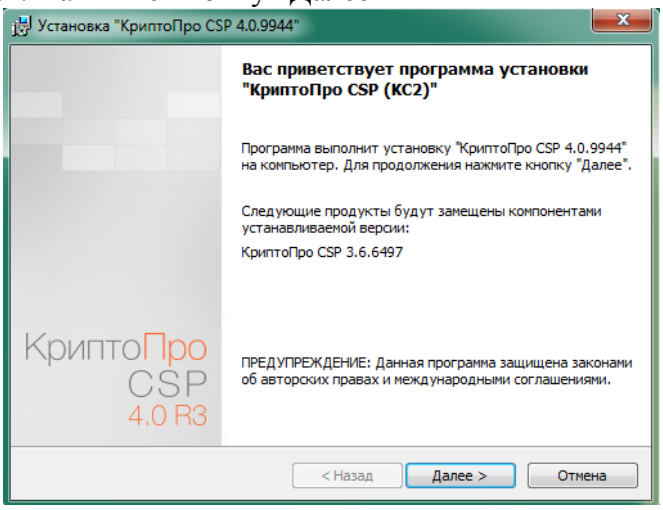


После первого подключения eToken в свободный порт USB автоматически установятся все необходимые драйверы, и устройство будет готово к работе.

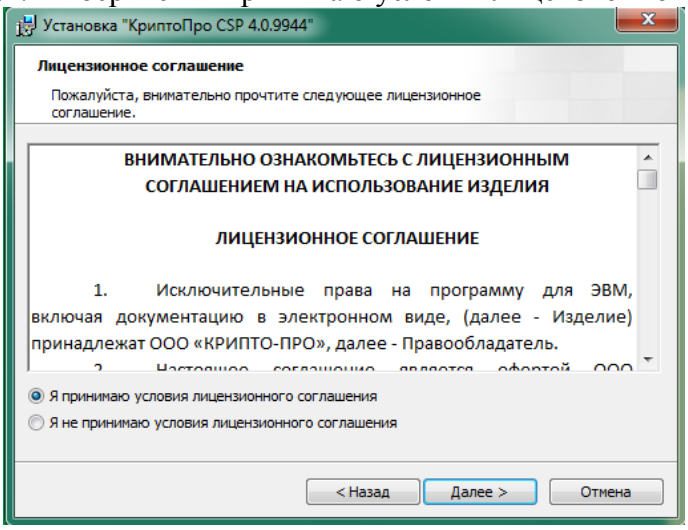
2.2. Установка КриптоПро.

После установки программы eToken, автоматически запустится программа установки КриптоПро.

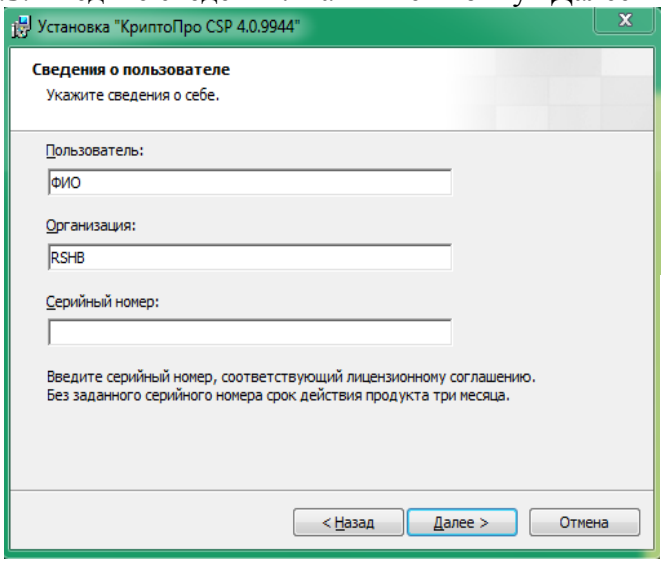
2.2.1. Нажмите кнопку «Далее»



2.2.2. Выберите «Я принимаю условия лицензионного соглашения». Нажмите «Далее»

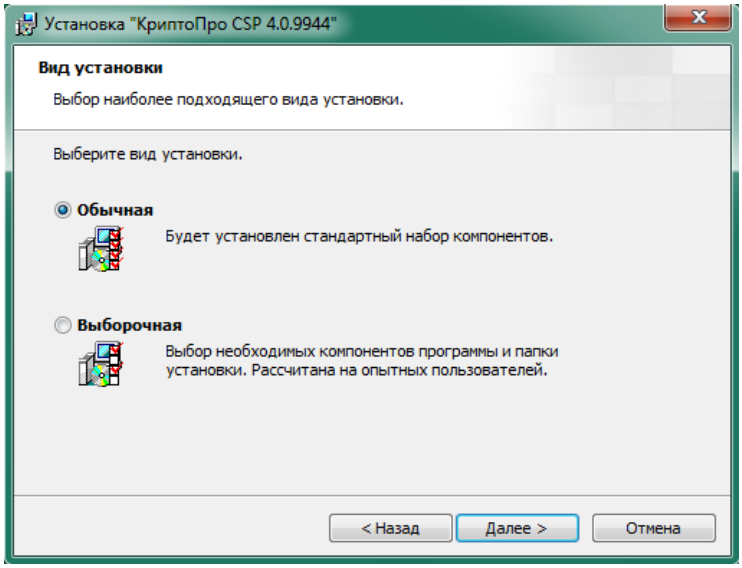


2.2.3. Введите сведения. Нажмите кнопку «Далее»

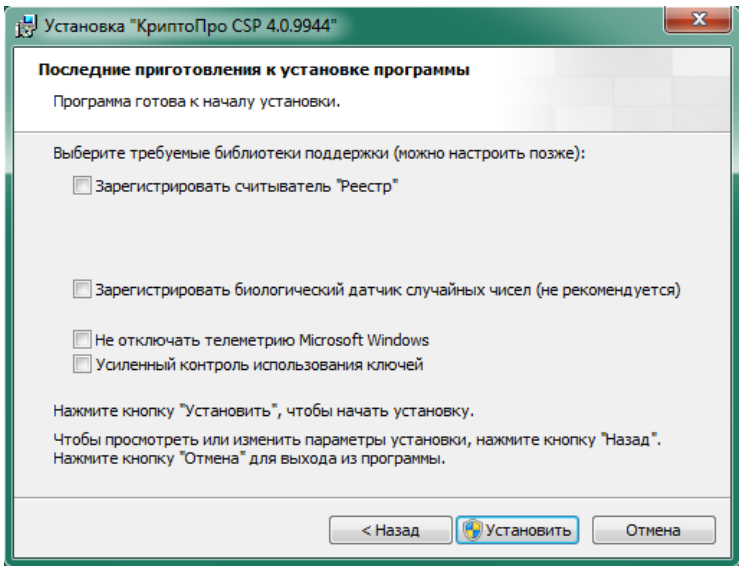


Для получения серийного номера КриптоПро - напишите письмо на электронный адрес QUIK@RSHB.RU тема письма: "Ваше ФИО Запрос с/н КриптоПро"

2.2.4. Нажмите кнопку «Далее»

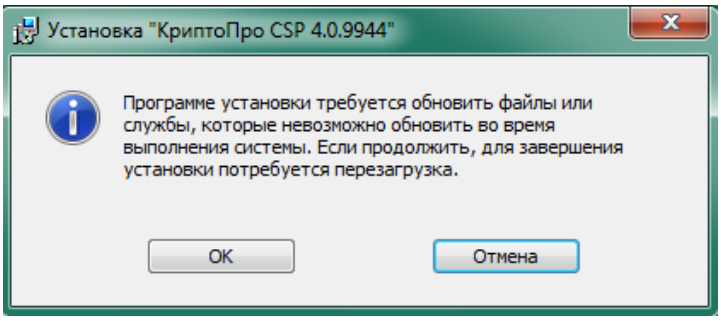


2.2.5. Нажмите кнопку «Установить»

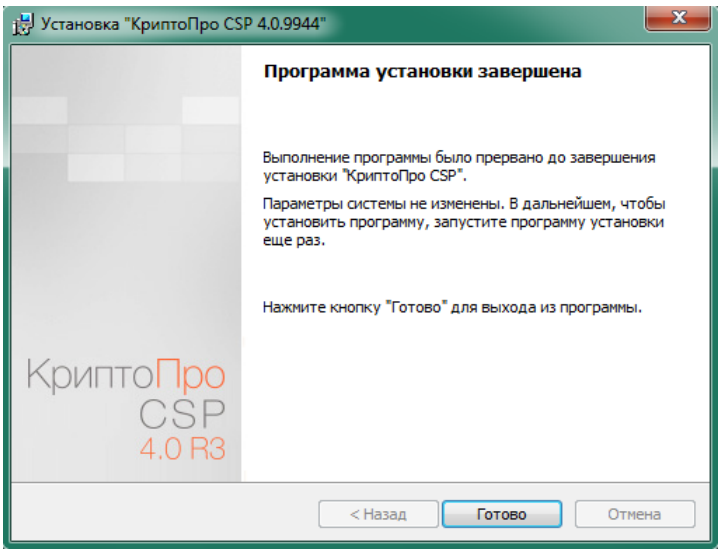


2.2.6. Перезагрузку системы для учета изменений можно произвести после окончания установки всех программ.

Нажмите кнопку «Отмена»



2.2.7. Нажмите кнопку «Готово»



2.3. Установка библиотеки Microsoft CAPICOM.

Если на вашем компьютере установлена **Windows 64xBit** – установка производится путем копирования файлов. Если Start.bat был запущен от **Администратора**, то файлы должны будут скопироваться автоматически.

Если нет, то в Командной строке будет примерно следующий текст:

```
C:\RSHB_soft>copy C:\RSHB_soft\4_CAPICOM\CapicomWin7(64bit)\capicom.dll C:\Windo
ws\syswow64
Отказано в доступе.
Скопировано файлов:          0.

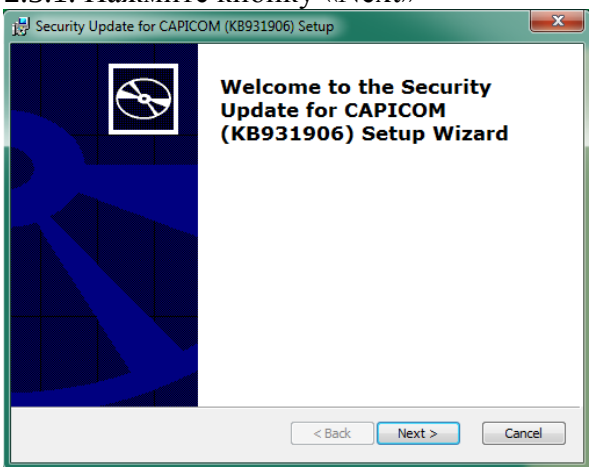
C:\RSHB_soft>copy C:\RSHB_soft\4_CAPICOM\CapicomWin7(64bit)\capicom.inf C:\Windo
ws\syswow64
Отказано в доступе.
Скопировано файлов:          0.
```

В таком случае необходимо вручную скопировать файлы из папки

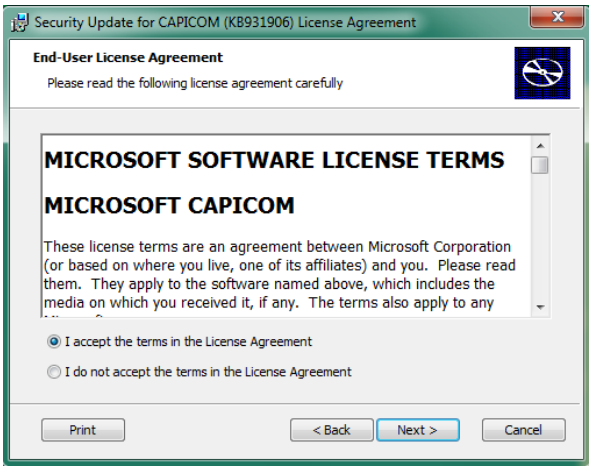
\RSHB_soft\4_CAPICOM\CapicomWin7(64bit) в папку **Windows\syswow64**

Если на Вашем компьютере установлена **Windows 32xBit** – запуск мастера установки Microsoft CAPICOM произойдёт автоматически. Переходите к выполнению пунктов 2.3.1-2.3.6):

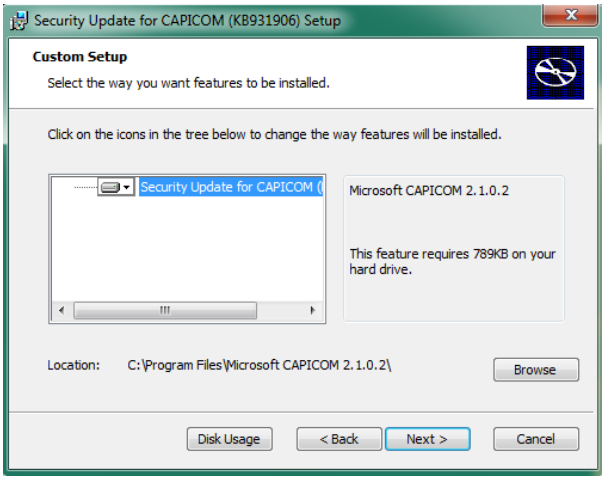
2.3.1. Нажмите кнопку «Next»



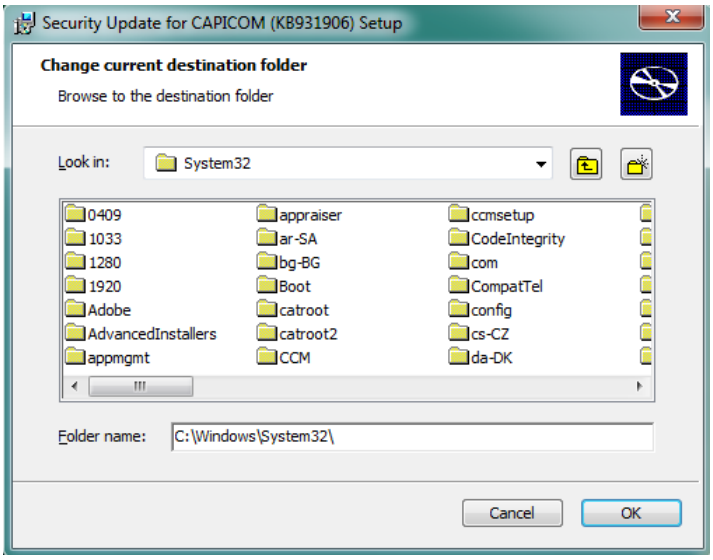
2.3.2. Выберите «I accept the terms in the License Agreement» и нажмите кнопку «Next»



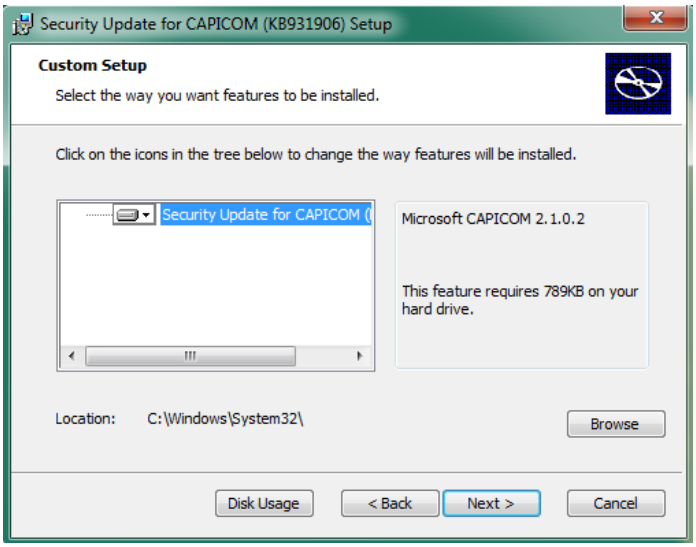
2.3.3. Нажмите кнопку «Browse»



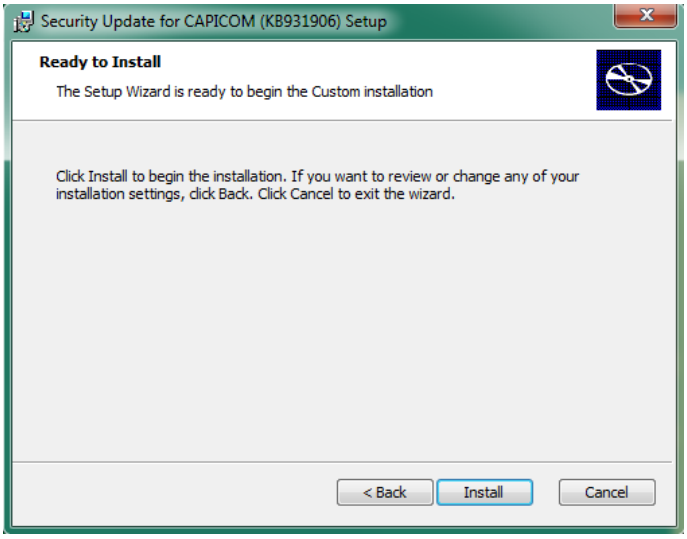
Выберите папку для установки C:\WINDOWS\system32\ и нажмите «OK»



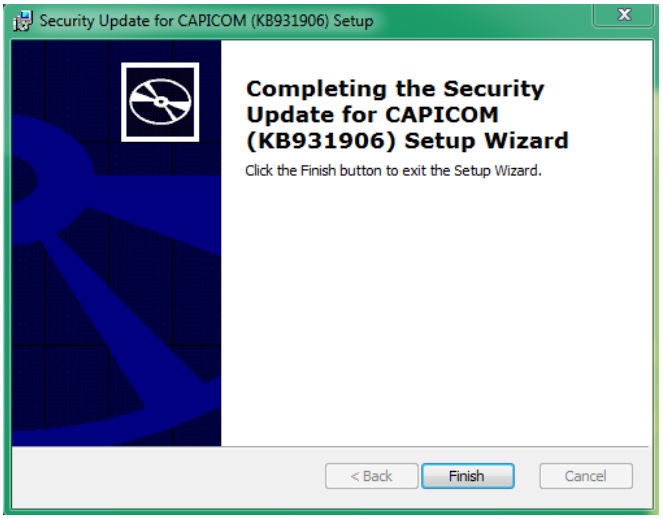
2.3.4. Нажмите кнопку «Next»



2.3.5. Нажмите кнопку «Install»



2.3.6. Нажмите кнопку «Finish»



2.4. Установка QUIK.

После окончания установки комплекта программ через Start.bat, мастер установки автоматически скопирует каталог с QUIK в корень системного диска (например C:\RSHB_QUIK\).

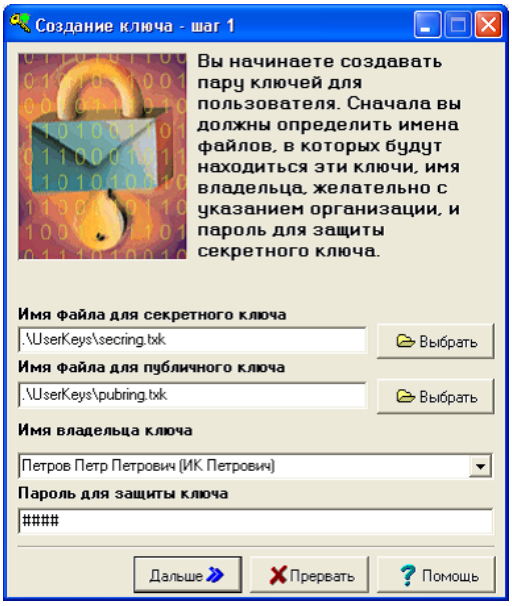
Проверьте наличие данного каталога.

C:\RSHB_QUIK\info.exe – исполняемый файл программы QUIK. Вы можете отправить на рабочий стол ярлык к этому файлу.

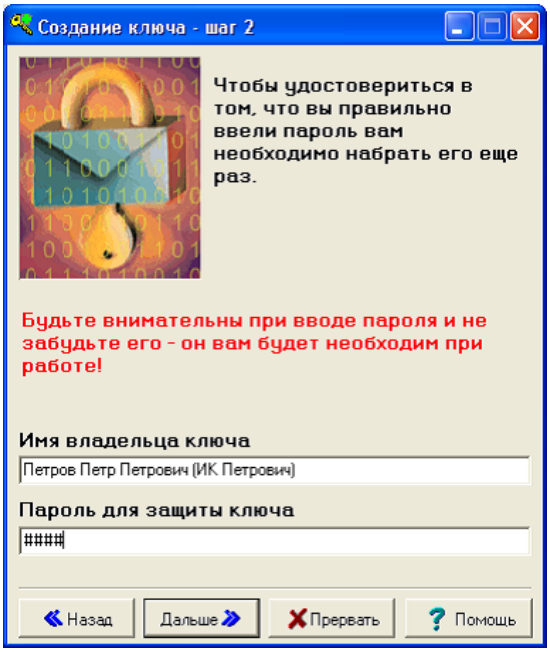
3. Генерация ключей QUIK.

Для генерации ключей доступа к QUIK необходимо перейти в папку программы QUIK (по умолчанию C:\RSHB_QUIK), в ней перейти в папку KeyGen (C:\RSHB_QUIK\KeyGen) и запустить исполняемый файл KeyGen.exe:

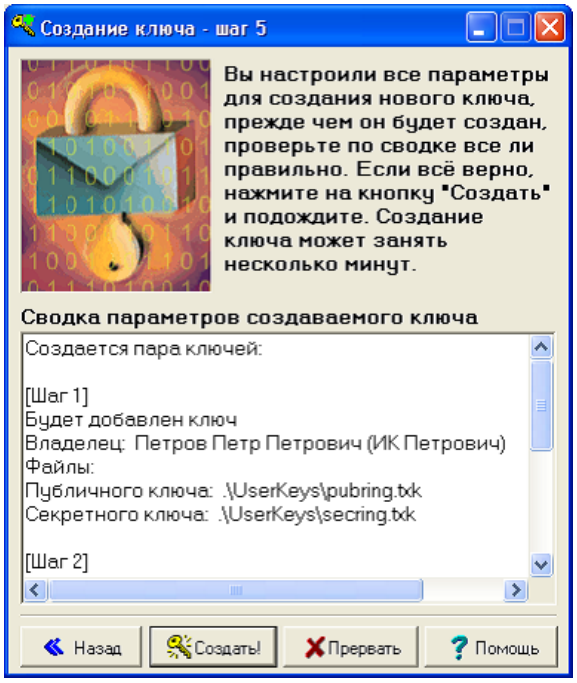
3.1. Заполните имя владельца ключа и пароль для защиты ключа (имя и пароль в дальнейшем будут использоваться для входа в QUIK). Нажмите кнопку «Дальше»



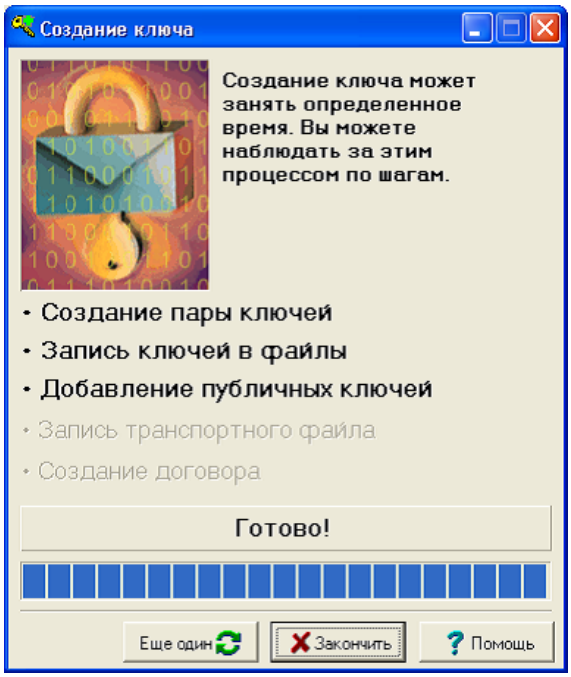
3.2. Следуйте указаниям на экране. Нажмите кнопку «Дальше»



3.3. Нажмите кнопку «Создать» и нажимайте любые клавиши



3.4. Нажмите кнопку «Закончить»



3.5. Сгенерированный файл с именем pubring.txk в каталоге C:\RSHB_QUIK\KeyGen\UserKeys необходимо направить на электронный адрес QUIK@RSHB.RU

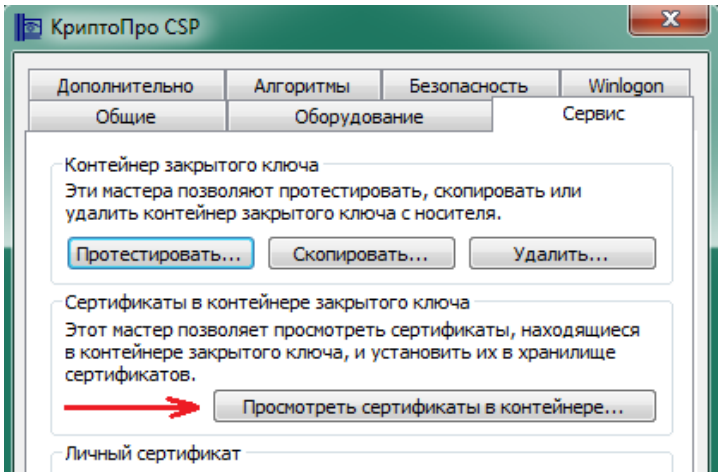
В теме письма укажите «Наименование Вашей организации» или «Ваши Фамилию И.О.»

4. Настройка QUIK.

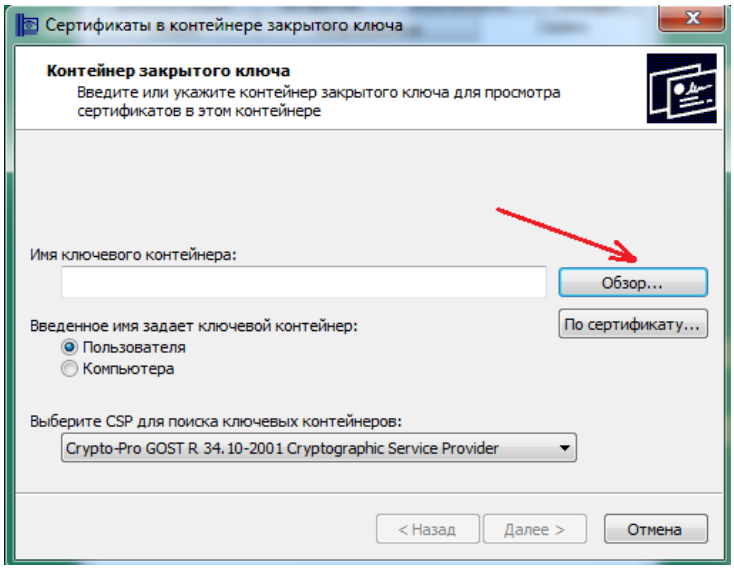
Для проставления ЭП (электронной подписи) под заявками необходимо указать используемый ключ ЭП.

4.1. Запустите:
Панель управления -> КриптоПро CSP
или
Пуск -> Все программы -> Крипто-Про -> КриптоПро CSP

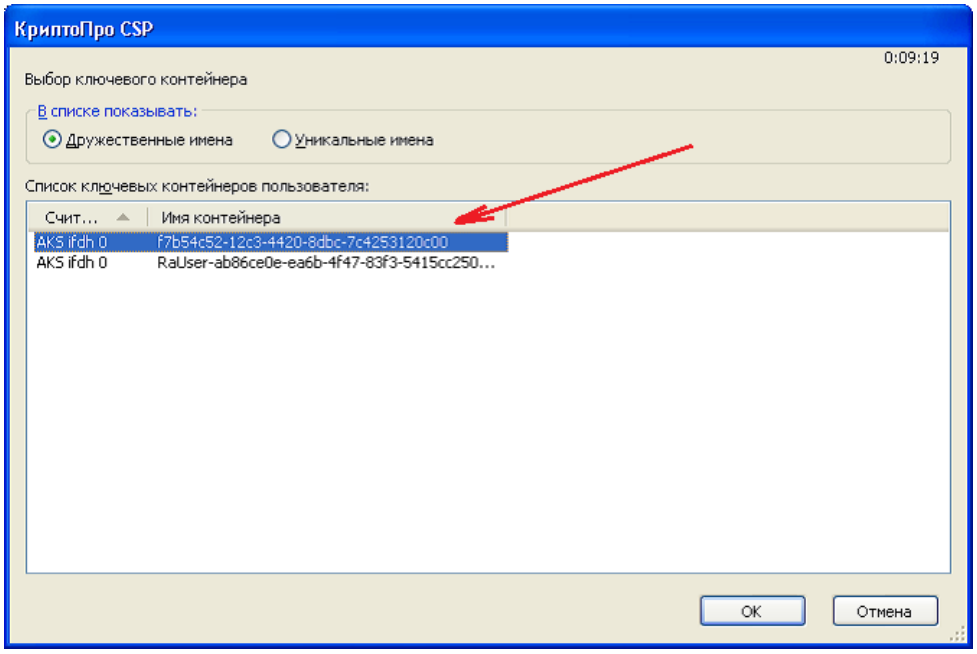
4.2. Перейдите на вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере…»



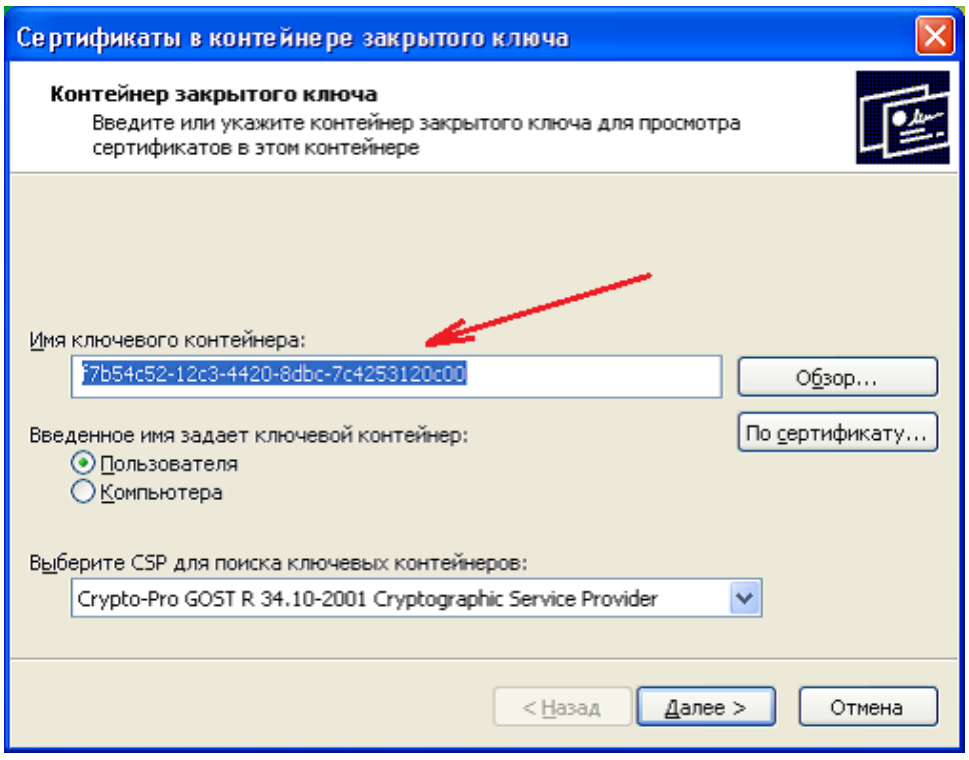
4.3. Нажмите кнопку «Обзор…» (чтобы выбрать по имени контейнера)



4.4. Выберите контейнер и нажмите «ОК»



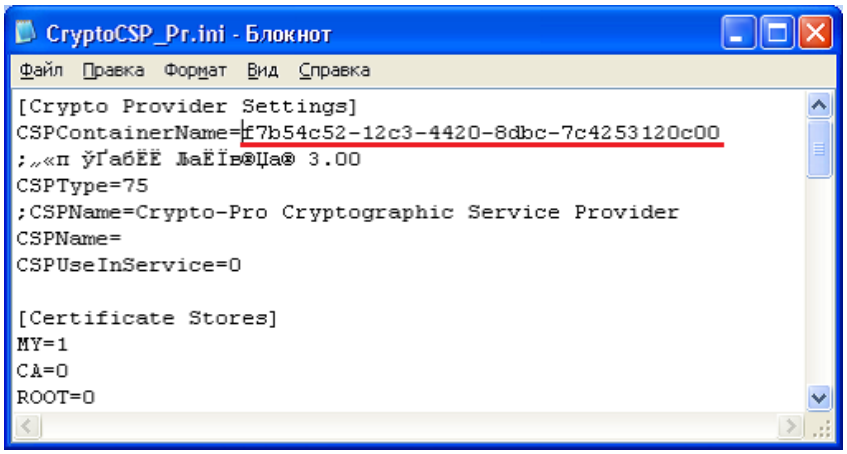
4.5. Выделите Имя ключевого контейнера и скопируйте его (нажав правую клавишу мыши и выбрав «Копировать» или нажав комбинацию клавиш Ctrl+C).



Если необходимо посмотреть сведения о выбранном контейнере нажмите «Далее». В появившемся окне будут отображены данные о владельце сертификата и сроках действия сертификата.
Нажмите «Назад», если был выбран не тот контейнер и выберите другой.

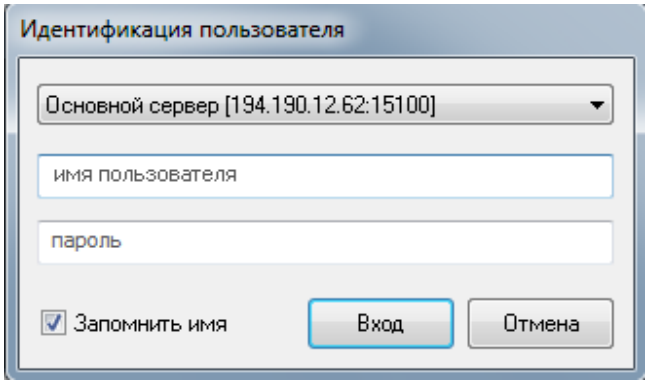
4.6. В папке с установленным QUIK (например C:\RSHB_QUIK) откройте в блокноте файл CryptoCSP_Pr.ini.

В строке CSPContainerName= вставьте скопированное имя контейнера.
Пример:
CSPContainerName=f7b54c52-12c3-4420-8dbc-7c4253120c00
Сохраните и закройте файл CryptoCSP_Pr.ini.



4.7. Запустите QUIK через ярлык на рабочем столе или через исполняемый файл info.exe, который по умолчанию находится в папке C:\RSHB_QUIK\info.exe

Введите имя и пароль, использованные при генерации ключей доступа к QUIK
(3. Генерация ключей QUIK).



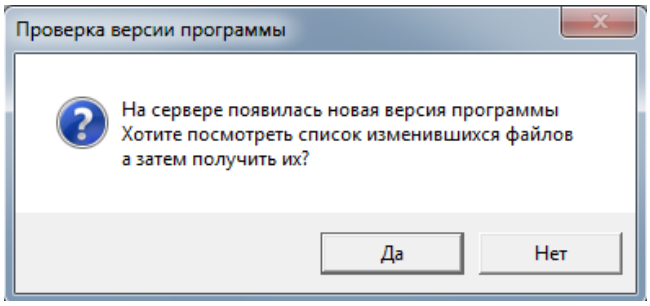
Обращаем Ваше внимание!

Для работы с установленной программой QUIK необходимо сформировать запрос и выпустить постоянный сертификат на сайте Удостоверяющего центра РСХБ используя полученный в отделении Банка eToken с временным сертификатом.

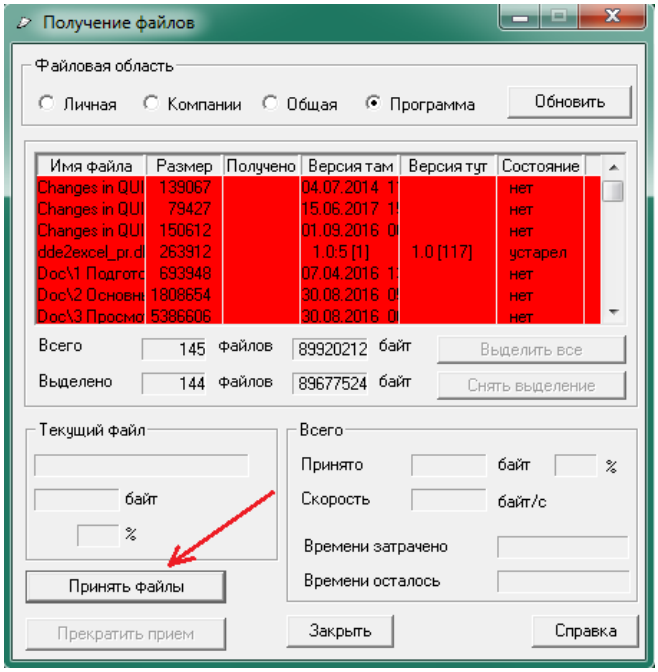
Ссылка на Инструкцию по работе с сайтом Удостоверяющего центра АО «Россельхозбанк» (УЦ РСХБ):

https://www.rshb.ru/download-file/350279/

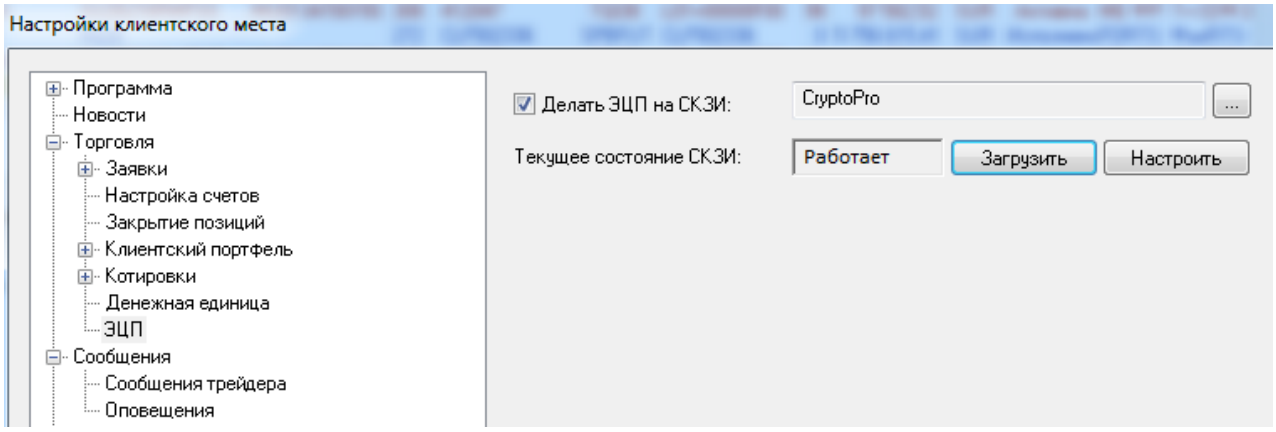
4.8. После выполнения входа в программу QUIK с использованием постоянного сертификата, выполните предложенное обновление версии программы:



Нажмите кнопку «Принять файлы»



4.9. Для проверки работы ЭЦП (электронно-цифровой подписи) необходимо в QUIK зайти в меню «Система» – «Настройки» – «Основные настройки» - вкладка «Торговля» - раздел «ЭЦП». Проверьте, что стоит галочка на «Делать ЭЦП на СКЗИ» - «CryptoPro» и значение «Текущее состояние СКЗИ» - «Работает».



5. Работа с QUIK.

Для ознакомления с основными правилами работы с программой воспользуйтесь справкой по ИТС QUIK, вызываемой непосредственно в программе (клавиша F1).

Актуальную документацию по Рабочему месту QUIK также можно найти на официальном сайте разработчика ARQA Technologies.

6. Повышение уровня защищенности QUIK.

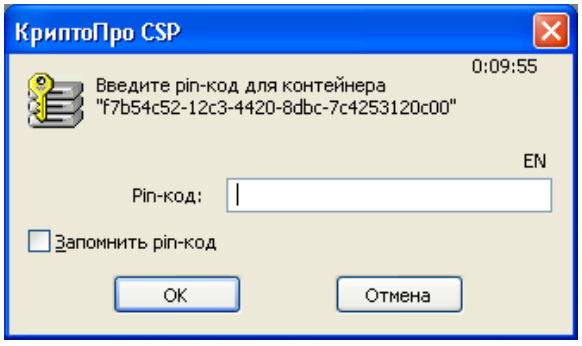
В настройках ИТС QUIK предусматривается только начальная инициализация ЭП (электронной подписи). Наличие носителя eToken с ключами ЭП проверяется только при запуске QUIK. Если после запуска QUIK извлечь из порта USB ключевой носитель eToken с ключами ЭП, то QUIK будет по-прежнему принимать ввод транзакций (поставить/изменить/снять заявку).
Для того чтобы программа QUIK проверяла наличие ключевого носителя eToken с ключами ЭП при каждом вводе транзакций (поставить/изменить/снять заявку) необходимо внести некоторые изменения в настройки:

6.1. В папке с установленной программой QUIK необходимо открыть файл CryptoCSP_Pr.ini (для открытия лучше использовать стандартную программу Блокнот).
В секции [Crypto Provider Settings] добавить ключ CachKeyAndCertificates со значением 0.
Пример:

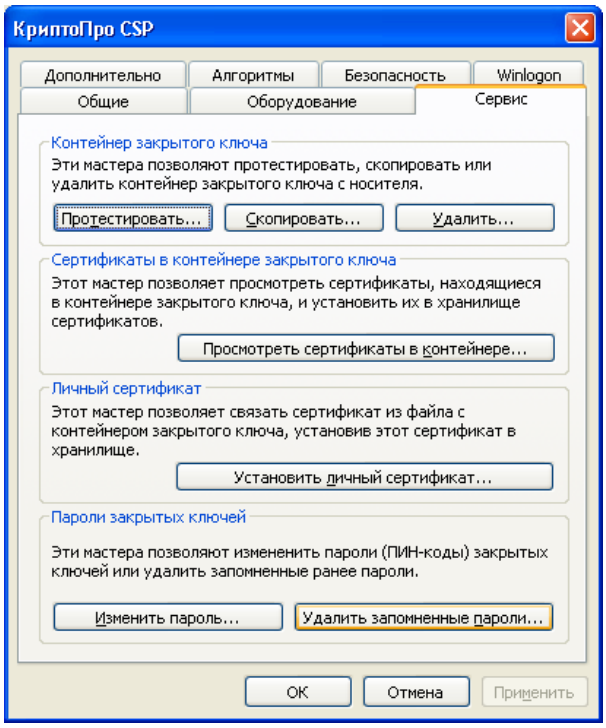
[Crypto Provider Settings]
CSPContainerName=f7b54c52-12c3-4420-8dbc-7c4253120c00
CSPType=75
CSPName=
CSPUseInService=0
CachKeyAndCertificates=0

После внесения изменений сохраните и закройте файл.
В результате данных изменений будет проводиться проверка наличия ключевого носителя eToken с ключами ЭП при каждом вводе транзакций.
Если извлечь носитель eToken из порта USB, то система отвергнет попытку ввода транзакции.

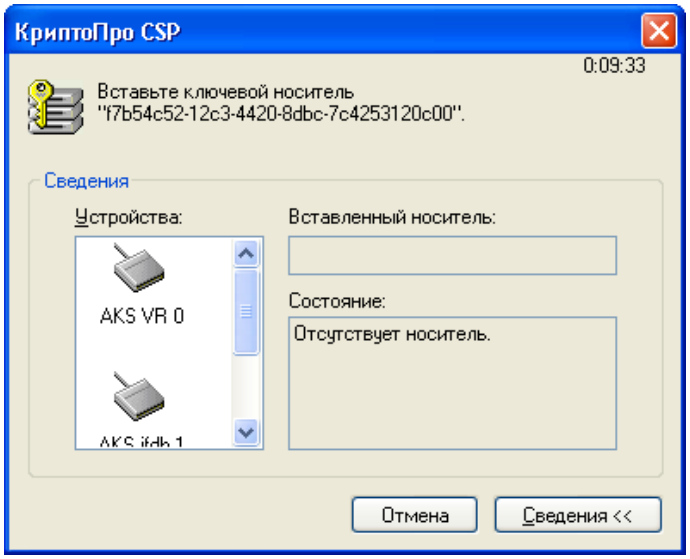
6.2. Каждый раз при вводе транзакции будет появляться запрос на ввод Pin-кода.
Для ускорения процедуры ввода можно ввести Pin-код и поставить галочку у «Запомнить pin-код» и нажать «OK». Теперь система будет проверять только наличие носителя eToken в порте USB.



Для удаления запомненных паролей необходимо запустить КриптоПро CSP, перейти на вкладку «Сервис» и нажать на «Удалить запомненные пароли…» (в секции Пароли закрытых ключей).

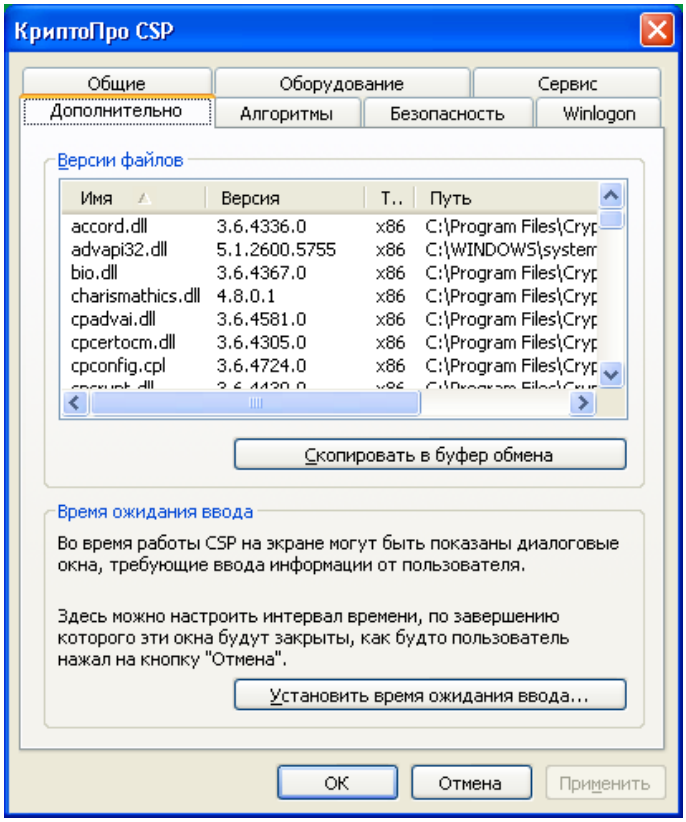


6.3. После описанных в п. 6.1. настроек ИТС QUIK (запуск с ключом CachKeyAndCertificates=0) будет проводиться проверка наличия ключевого носителя eToken с ключами ЭП перед каждой отправкой транзакции на сервер QUIK. Однако при извлеченном носителе eToken можно набрать параметры транзакции (например, заявки на покупку) и нажать «Да» для отправки на сервер QUIK. После этого появится окно с предложением вставить ключевой носитель и таймером отсчета времени ожидания:

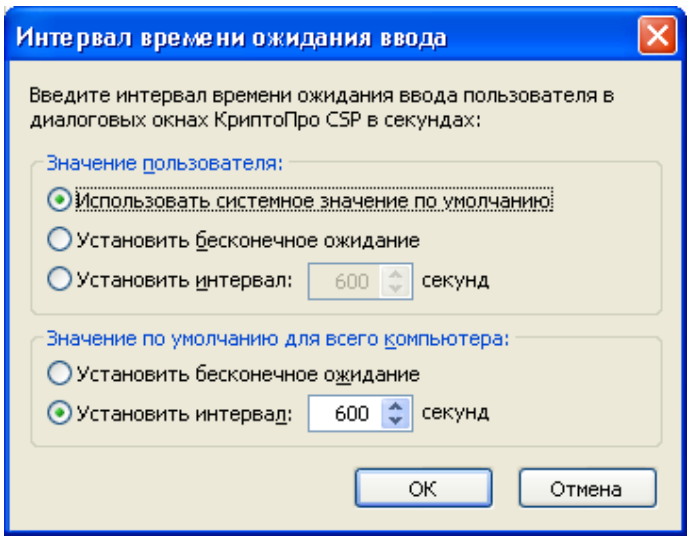


По умолчанию время ожидания вставления ключевого носителя eToken составляет 600 секунд. Для уменьшения риска несанкционированного ввода транзакции рекомендуется уменьшить время ожидания до 20 - 30 секунд, что позволит исключить вероятность набора параметров транзакции и оставлении в режиме ожидания вставления носителя

eToken лицом, не уполномоченным на совершение такой операции. Установка времени ожидания 20 - 30 секунд гарантирует, что набравший параметры транзакции и владелец носителя eToken являются одним лицом.
Для изменения времени ожидания запустите КриптоПро CSP, перейдите на вкладку «Дополнительно» и нажмите кнопку «Установить время ожидания ввода…»



В появившемся окне измените интервал времени ожидания ввода.

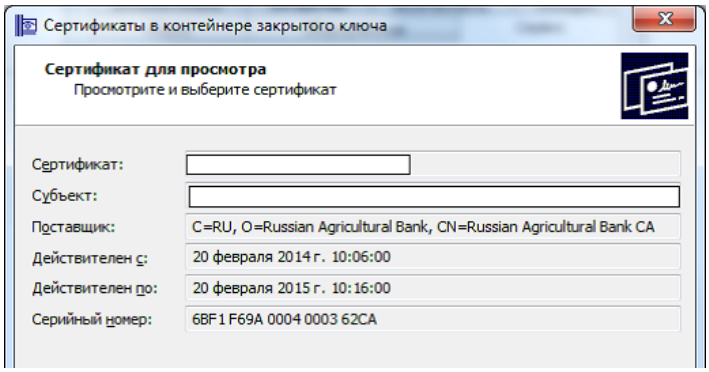


7. Удаление закрытого ключа с eToken.

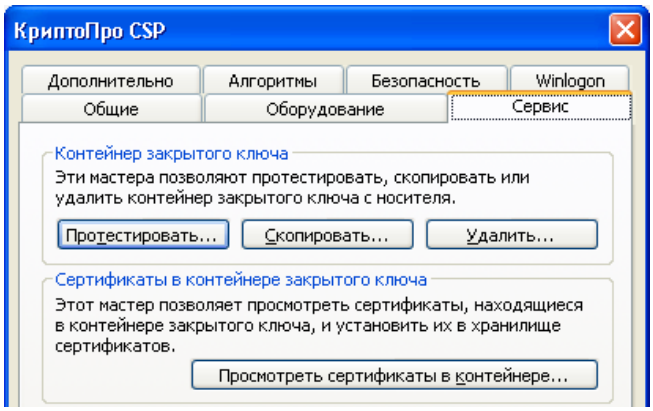
Данный раздел выполняется при необходимости удалить ключ с истекшим сроком действия или скомпрометированный ключ.

Настоятельно рекомендуется перед удалением контейнера закрытого ключа записать название контейнера, подлежащего удалению.

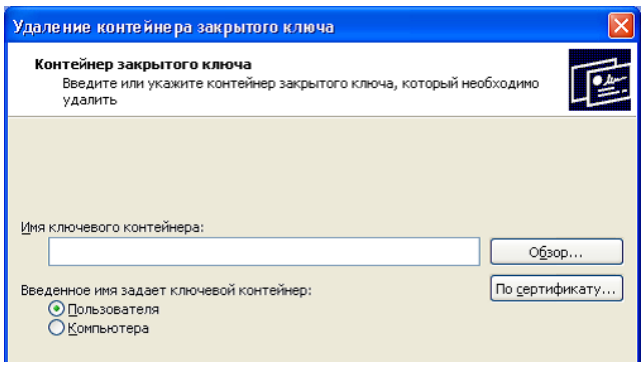
Для получения сведений о контейнере (который предполагается удалить) необходимо запустить КриптоПро CSP, перейти на вкладку «Сервис» и нажать на «Просмотреть сертификаты в контейнере…», в открывшемся окне нажать «Обзор…». Для просмотра сведений о контейнере выбрать имя контейнера и нажать «ОК», в открывшемся окне нажать «Готово».
В окне просмотра сведений будет отображено имя владельца, даты начала и окончания действия сертификата и другая информация.



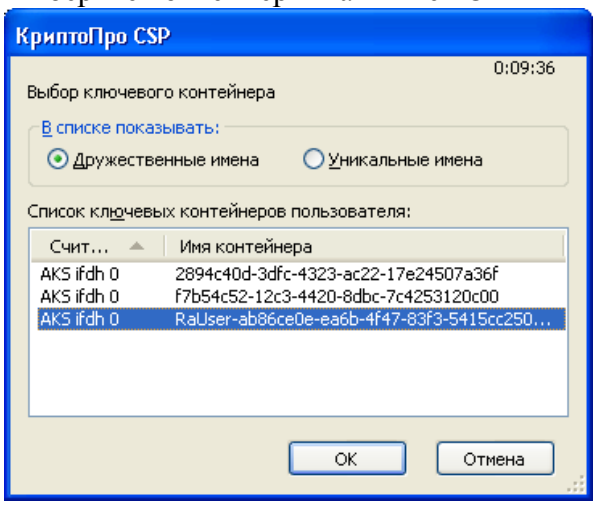
После просмотра нажмите «Отмена».
Для удаления контейнера закрытого ключа с eToken (при необходимости удалить ключ с истекшим сроком действия, скомпрометированный или т.п.) необходимо запустить КриптоПро CSP, перейти на вкладку «Сервис» и нажать на «Удалить…» (в секции Контейнер закрытого ключа).



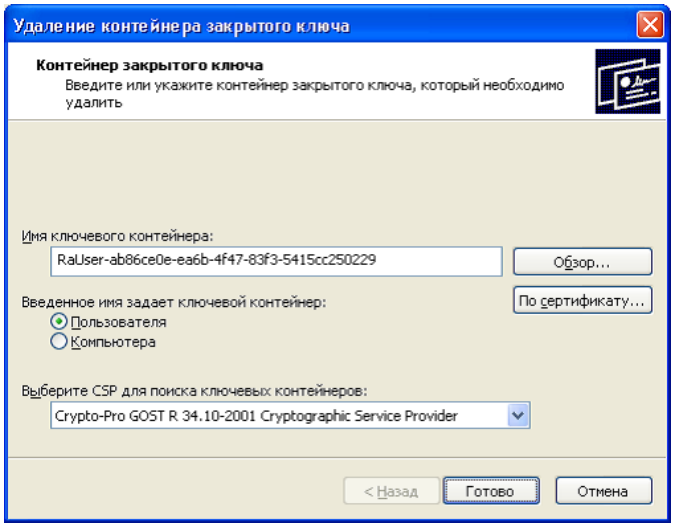
Нажмите «Обзор…»



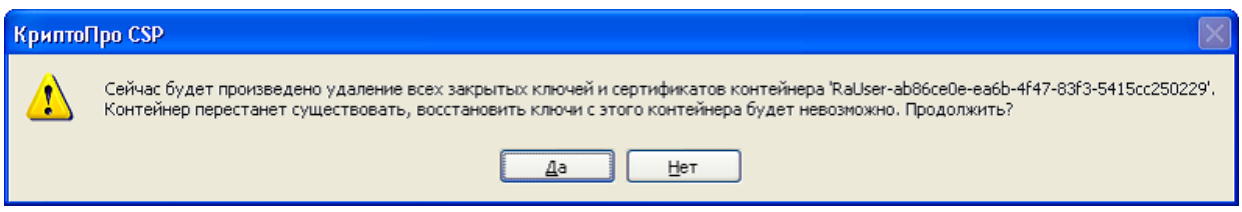
Выберите контейнер и нажмите «ОК»



Нажмите «Готово»



Для удаления нажмите «Да».
Для отмены нажмите «Нет».



8. Изменение пароля (PIN-кода) eToken.

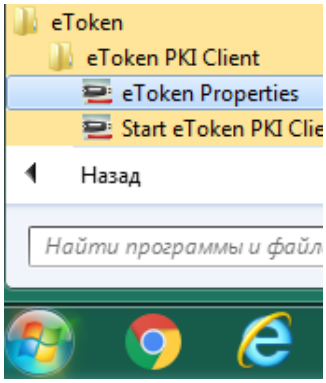
После установки настоятельно рекомендуется изменить PIN-код eToken (см. Руководство пользователя eToken PKI Client 5.1 SP1).

Новый пароль следует вводить на английской раскладке клавиатуры.
Длина пароля должна быть не более 10 символов.

Для изменения пароля (PIN-кода) eToken откройте «eToken Properties», дважды щелкнув на значок на панели задач:



или Пуск -> Все программы -> eToken -> eToken PKI Client -> eToken Properties:



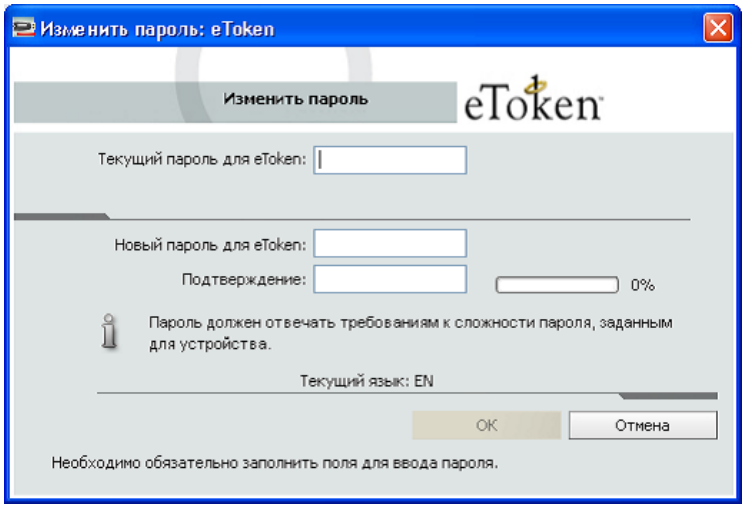
Нажмите «Изменить пароль eToken»



В открывшемся окне ввести данные о текущем пароле и новом пароле.

После нажатия «ОК» вступает в силу новый пароль.

В случае если пароль будет забыт, восстановить его невозможно. Вход на eToken и использование ЭП будет невозможно.



Повторно обращаем Ваше внимание!

Для работы с установленной программой QUIK необходимо сформировать запрос и выпустить постоянный сертификат на сайте Удостоверяющего центра РСХБ используя полученный в отделении Банка eToken с временным сертификатом.

Ссылка на Инструкцию по работе с сайтом Удостоверяющего центра АО «Россельхозбанк» (УЦ РСХБ):

https://www.rshb.ru/download-file/350279/