eToken. Руководство пользователя

Версия 3.66

02.04.2008

Aladdin
SECURITY SOLUTIONS
www.aladdin.ru

Содержание

Введение

eToken: общие сведения

eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП. eToken выпускается в форм-факторах USB-ключа или смарт-карты.

USB-ключ eToken напрямую подсоединяется к компьютеру через порт USB (Universal Serial Bus) и не требует устройства для чтения смарт-карт.

eToken обладает защищённой энергонезависимой памятью и используется в качестве портативного хранилища секретных данных (ключей шифрования, имён пользователя, паролей, учётных записей, сертификатов и пр.).

PIN-код

Для получения доступа к защищённым данным, хранящимся в памяти eToken, требуется ввести PIN-код (Personal Identification Number, eToken password), являющийся аналогом пароля.

PIN-код должен содержать минимум четыре символа. Для увеличения стойкости PIN-кода используйте последовательность из восьми или более символов, включающую буквы, цифры и специальные символы. Русские буквы и пробелы в PIN-код включать не рекомендуется.

Предустановленный PIN-код: 1234567890 (используется по умолчанию в новых USB-ключах и смарт-картах).

Для замены PIN-кода необходимо знание текущего PIN-кода.

Важно! Если пользователь забыл PIN-код, то применять eToken в дальнейшем он не сможет.

Модели eToken

eToken PRO

eToken PRO — смарт-карта или USB-ключ с аппаратной поддержкой шифрования по алгоритму RSA. Кроме PIN-кода пользователя, в eToken PRO предусмотрен пароль администратора. С помощью него,

например, можно сменить забытый PIN-код. Пароль администратора также можно менять. Для защиты от подбора PIN-кода в eToken PRO установлено предельное число попыток неправильного ввода PIN-кода подряд, по истечении которого PIN-код блокируется.

eToken NG-OTP

eToken NG-OTP — комбинирующее устройство, совмещающее возможности eToken PRO и генератора одноразовых паролей (One Time Password – OTP). eToken NG-OTP выпускается в виде USB-ключа с жидкокристаллическим дисплеем, встроенным источником питания и кнопкой генерирования одноразового пароля.

eToken NG-FLASH

eToken NG-FLASH — комбинирующее устройство, совмещающее возможности eToken PRO и устройства хранения информации (Flash-памяти).

Объем Flash-памяти — до GB.

Программное обеспечение для eToken

Общие сведения

eToken Run Time Environment 3.66

eToken Run Time Environment (eToken RTE) — это среда функционирования устройств eToken, включающая все необходимые драйвера и утилиту eToken Properties (Свойства eToken). С помощью утилиты eToken Properties вы можете:

- осуществлять настройки параметров eToken и его драйверов;
- просматривать общую информацию относительно eToken;
- импортировать, просматривать и удалять сертификаты и ключевые контейнеры RSA.

eToken Run Time Environment 3.66 Russian User Interface

По умолчанию в eToken Run Time Environment 3.66 предусмотрен интерфейс на английском языке. При установке пакета eToken Run Time Environment 3.66 Russian User Interface (eToken RTE 3.66 RUI) язык интерфейса eToken RTE 3.66 изменяется на русский.

Установка и удаление

Необходимые полномочия

Для установки и удаления программного обеспечения для eToken необходимы полномочия локального администратора.

Порядок установки и удаления

Важно: eToken нельзя подключать до установки eToken RTE.

Устанавливайте программное обеспечение в следующем порядке:

1. eToken RTE 3.66.
2. eToken RTE 3.66 RUI.

Удаляйте программное обеспечение в обратном порядке.

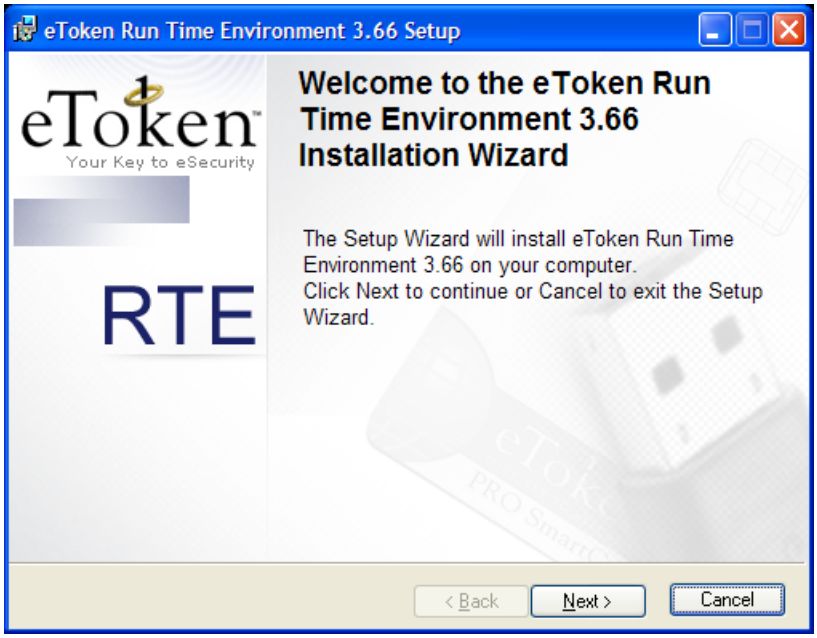
Установка и удаление на локальном компьютере

eToken RTE 3.66

Установка

Для того чтобы установить eToken Run Time Environment 3.66, выполните следующую последовательность действий.

1. Запустите программу установки eToken Run Time Environment 3.66.
2. В окне приветствия программы установки eToken Run Time Environment 3.66 нажмите **Next (**Далее).

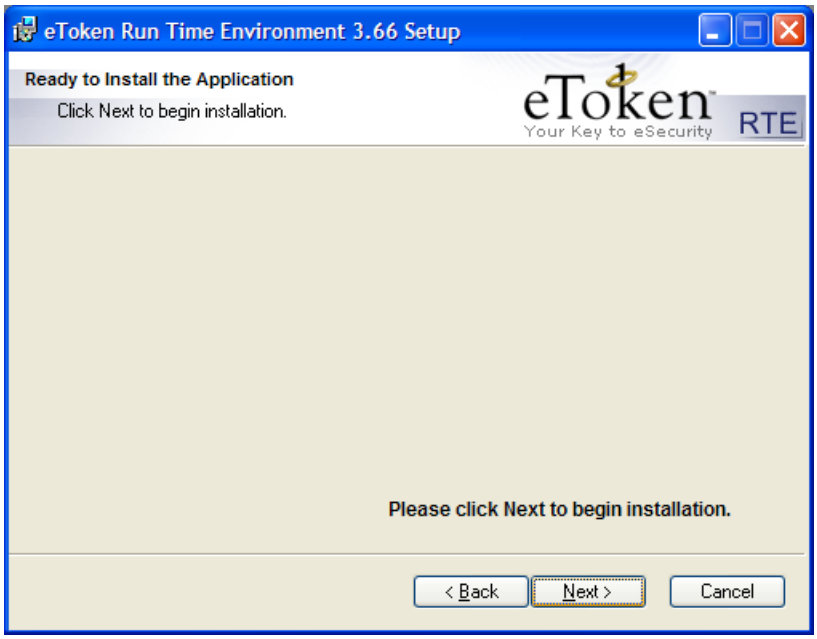


3. В окне **eToken Run Time Environment 3.66 Setup** / **End-User License Agreement** ознакомьтесь с лицензионным соглашением (на английском языке) и, если вы согласны с его условиями, выберите **I accept the license agreement** (Я принимаю лицензионное соглашение), чтобы продолжить установку.

Если вы не согласны с условиями лицензионного соглашения, нажмите **Cancel** (Отмена), а в появившемся окне — **Exit Setup** для выхода из программы установки. В этом случае eToken Run Time Environment 3.66 не будет установлен.

4. Если вы согласны с условиями лицензионного соглашения и выбрали **I accept the license agreement** (Я принимаю лицензионное соглашение), нажмите **Next** (Далее).

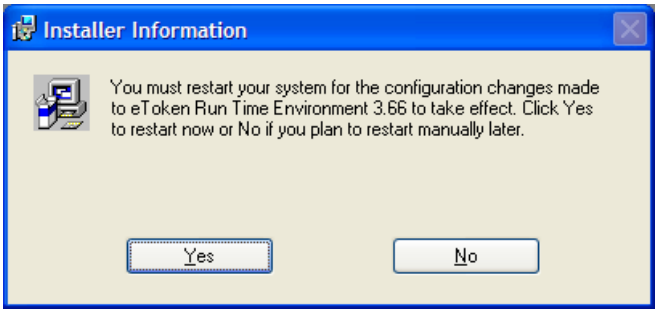
5. В окне **eToken Run Time Environment 3.66 Setup** / **Ready to Install the Application** нажмите **Next** (Далее).



6. Установка займёт некоторое время. Если на вашем компьютере был установлен eToken RTE одной из предыдущих версий, он будет удалён.

7. По завершении процесса установки eToken Run Time Environment 3.66 в окне **eToken Run Time Environment 3.66 Setup** / **eToken Run Time Environment 3.66 has been successfully installed** нажмите **Finish** (Готово).

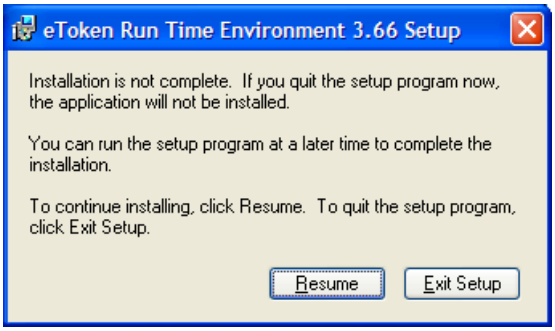
8. В конце процесса установки eToken Run Time Environment 3.66 может потребоваться перезагрузка компьютера. В этом случае в окне **Installer Information** нажмите **Yes** (Да) для немедленной перезагрузки или **No** (Нет), если вы планируете перезагрузить компьютер позднее.



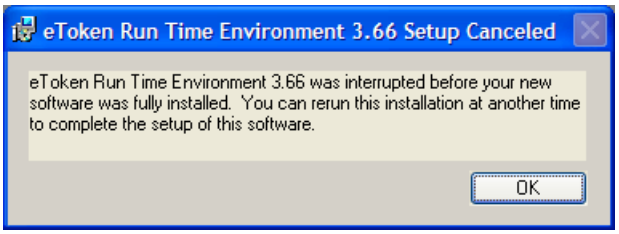
Отказ от установки

Отказаться от установки eToken RTE можно в любом окне программы установки eToken Run Time Environment 3.66 до **eToken Run Time Environment 3.66 Setup** / **Ready to Install the Application** включительно. Для этого:

1. Нажмите **Cancel** (Отмена).
2. В окне подтверждения нажмите **Exit Setup** (Выход).



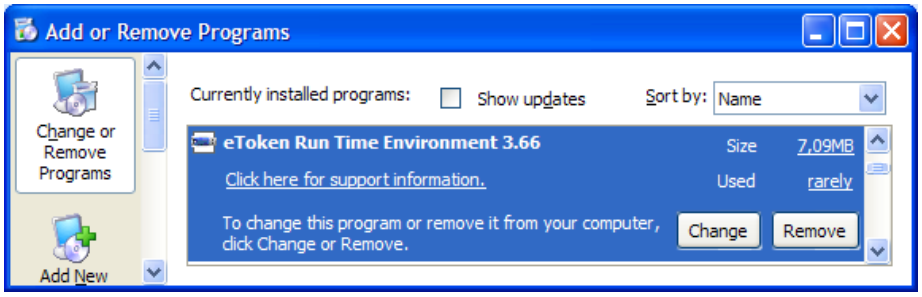
3. Нажмите **OK**.



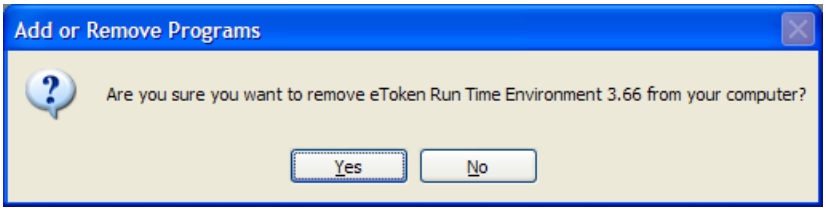
Удаление

Удалить eToken RTE из операционной системы можно стандартными средствами:

1. Откройте окно **Start > Control Panel > Add or Remove Programs** (Пуск > Панель управления > Установка и удаление программ).
2. Выберите пункт **eToken Run Time Environment 3.66**.



3. Нажмите **Remove (**Удалить).
4. В окне подтверждения нажмите **Yes** (Да).

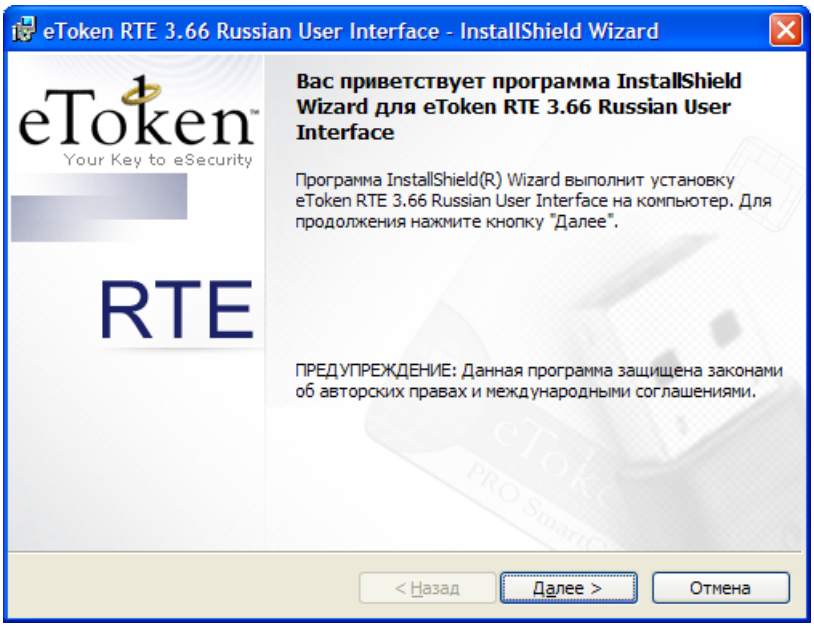


eToken RTE 3.66 RUI

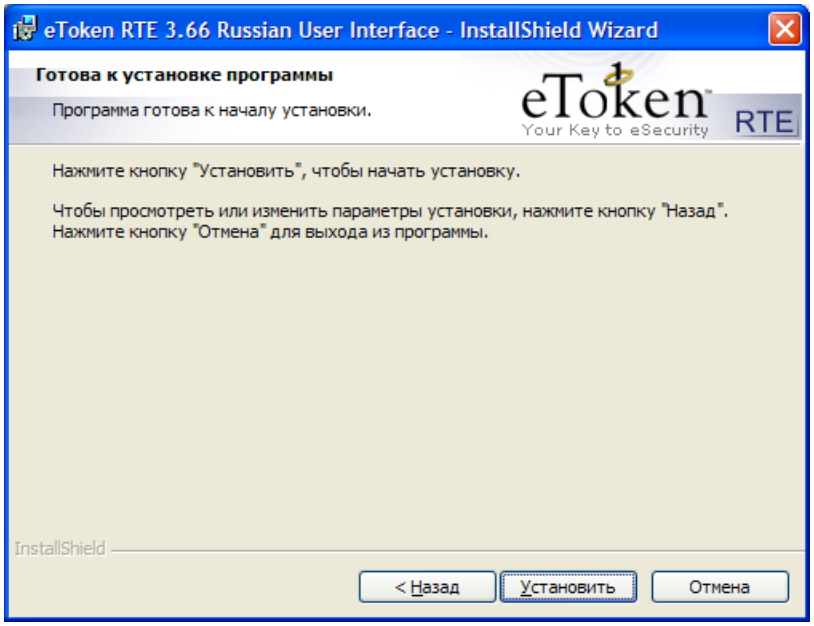
Установка

Для того чтобы установить eToken RTE 3.66 RUI, выполните следующее.

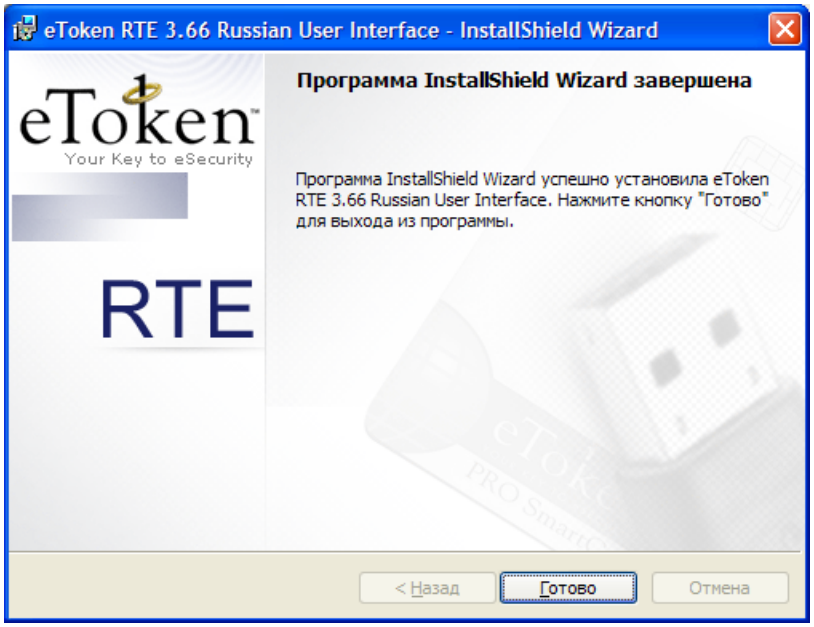
1. Запустите программу установки eToken RTE 3.66 RUI.
2. В окне приветствия программы установки eToken RTE 3.66 RUI нажмите **Далее**.



3. В окне **eToken RTE 3.66 Russian User Interface – InstallShield Wizard** / **Готова к установке программы** нажмите **Установить**.



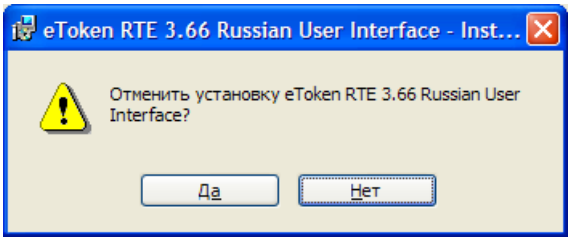
4. По завершении процесса установки eToken RTE 3.66 RUI в окне **eToken RTE 3.66 Russian User Interface – InstallShield Wizard** / **Программа InstallShield Wizard завершена** нажмите **Готово**.



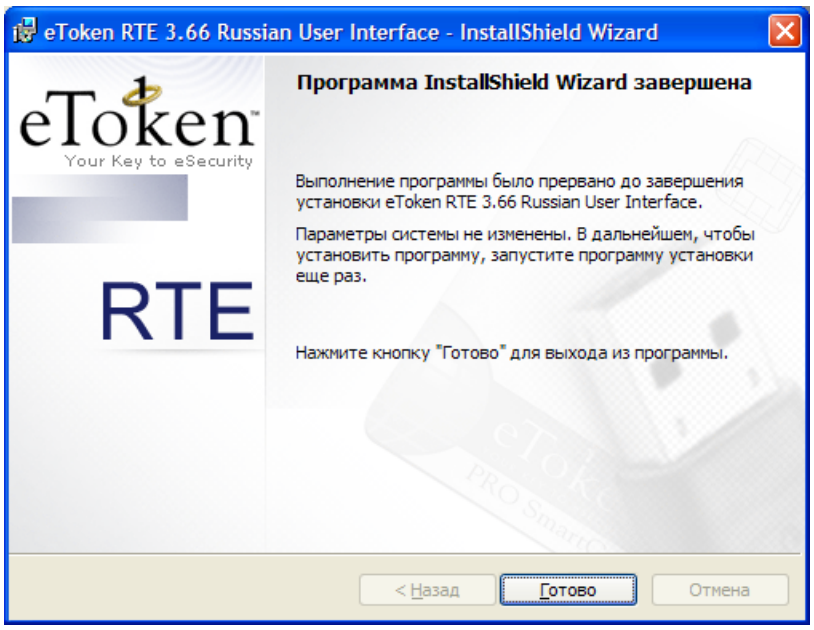
Отказ от установки

Отказаться от установки eToken RTE 3.66 RUI можно в любом окне программы установки, кроме последнего. Для этого:

- нажмите **Отмена**;
- в окне подтверждения нажмите **Да**;



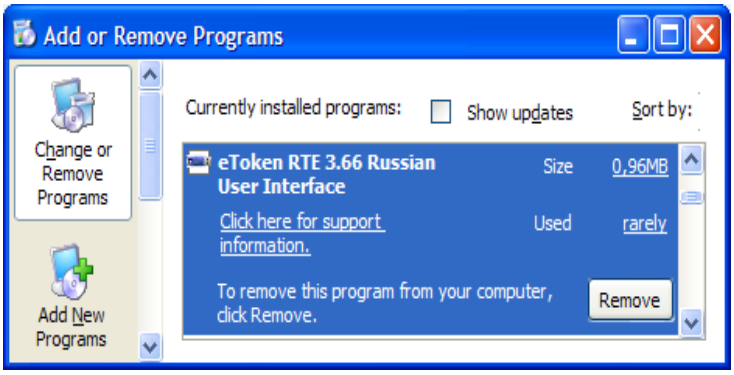
- для завершения работы программы установки нажмите **Готово**.



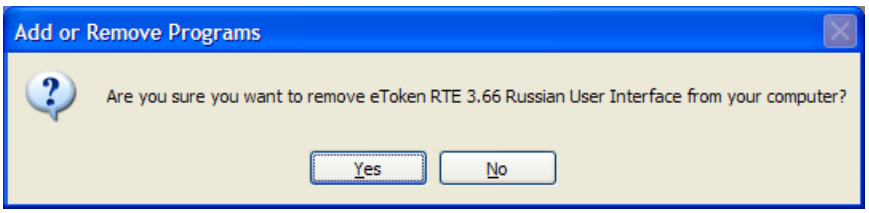
Удаление

Удалить eToken RTE 3.66 RUI из операционной системы можно стандартными средствами. Для этого выполните следующее.

1. Откройте окно **Start > Control Panel > Add or Remove Programs** (Пуск > Панель управления > Установка и удаление программ).
2. Выберите пункт **eToken RTE 3.66 Russian User Interface**.



3. Нажмите **Remove** (Удалить).
4. В окне подтверждения нажмите **Yes** (Да).



Первое подсоединение USB-ключа eToken к компьютеру

Важно: eToken нельзя подключать до установки eToken RTE.

Если на компьютере установлен eToken RTE 3.66, подключите eToken к порту USB, удлинительному кабелю или концентратору USB. После этого начнётся процесс обработки нового оборудования, который может занять некоторое время. По завершении процесса обработки нового оборудования на ключе загорится световой индикатор.

Использование eToken NG-FLASH в качестве загрузочного устройства

Существует возможность отформатировать устройство eToken NG-FLASH таким образом, чтобы некоторая часть его памяти содержала информацию, необходимую для загрузки компьютера (подробная информация доступна в документе «eToken. Руководство администратора»). Для использования eToken в качестве загрузочного устройства компьютер должен быть настроен соответствующим образом. Устройство должно быть поставлено на первое место в последовательности загрузки (boot sequence) в BIOS. Настройки отличаются для различных версий и производителей BIOS. В случае затруднений следует обратиться к системному администратору.

Свойства eToken

Об утилите eToken Properties

Утилита eToken Properties устанавливается вместе с eToken RTE. Данная утилита служит для настройки параметров eToken и его драйверов, просмотра общей информации относительно eToken, импорта, просмотра и удаления сертификатов и ключевых контейнеров RSA. С помощью этой утилиты вы можете также форматировать eToken и настраивать критерии качества PIN-кодов.

При установленном пакете RTE 3.66.RUI утилита имеет название “Свойства eToken” и русский интерфейс. Далее будет описано использование утилиты “Свойства eToken”, при этом предполагается, что пакет RTE 3.66.RUI установлен.

Режимы интерфейса утилиты “Свойства eToken”

Утилита “Свойства eToken” может работать в различных режимах интерфейса, в том числе:

- пользовательском;
- основном (по умолчанию).

В пользовательском режиме предусмотрены только следующие возможности:

- просмотр общей информации относительно eToken;
- смена PIN-кода;
- переименование eToken;
- смена и разблокирование PIN-кода с участием удалённого администратора.

В основном режиме вы можете:

- настраивать параметры eToken RTE (кроме настройки критериев качества PIN-кодов);
- осуществлять пользовательские операции с eToken.

В пользовательском режиме кнопки **Компьютер** и **Дополнительно** неактивны. Переключение режимов осуществляется администратором.

Запуск утилиты

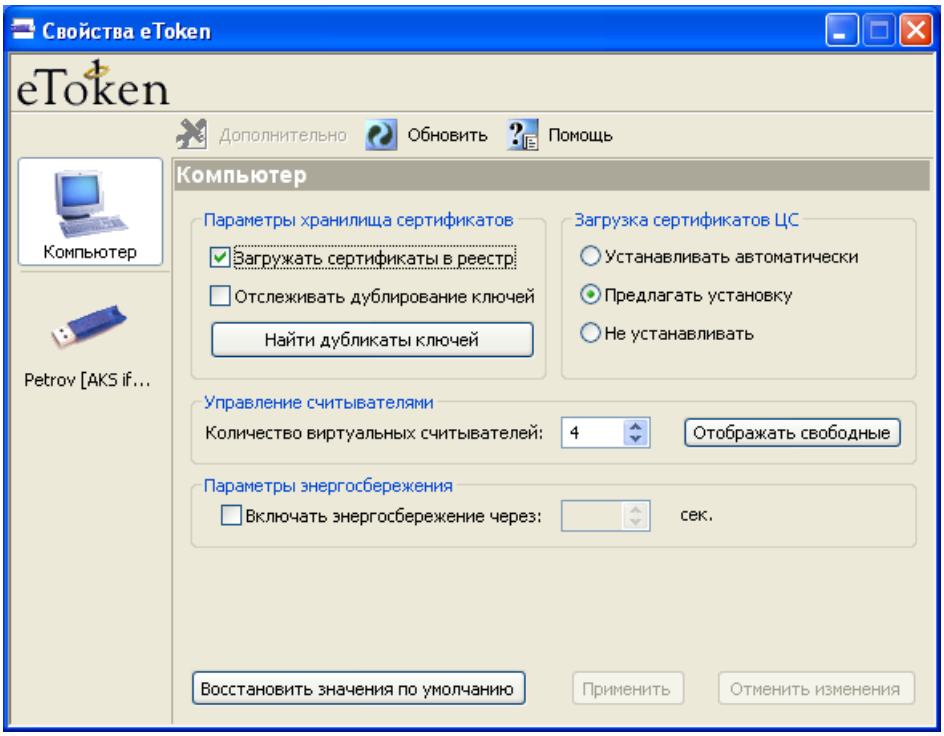
Для того чтобы запустить утилиту "Свойства eToken", щёлкните **Start** > **All Programs Programs (Programs)** > **eToken** > **eToken Properties** (Пуск > Все программы (Программы) > eToken > eToken Properties).

Настройка параметров eToken RTE

Общие параметры

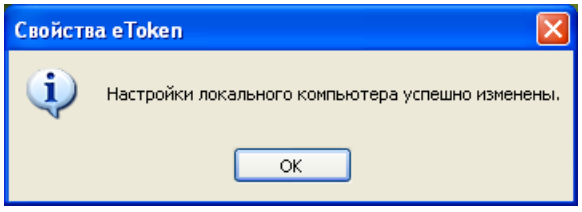
Для изменения общих параметров eToken RTE с помощью утилиты "Свойства eToken" требуются полномочия администратора.

Для того чтобы приступить к настройке, в окне **Свойства eToken** нажмите **Компьютер**.



После того как вы внесёте изменения:

- для сохранения изменений нажмите **Применить**, а затем нажмите **OK**;



- для отмены нажмите **Отменить изменения**.

Если вы хотите восстановить значения по умолчанию, нажмите **Восстановить значения по умолчанию**, а затем нажмите **Применить**.

Параметры хранилища сертификатов

Автоматическое копирование сертификатов из хранилища eToken в реестр

Если вы хотите, чтобы при подключении eToken к компьютеру все сертификаты автоматически копировались из хранилища eToken в реестр, установите флажок **Загружать сертификаты в реестр**.

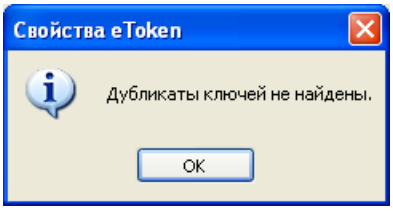
Примечание:

Копирование сертификатов может существенно ускорить работу некоторых приложений, но затруднить работу приложений, напрямую работающих с физическим хранилищем сертификатов eToken.

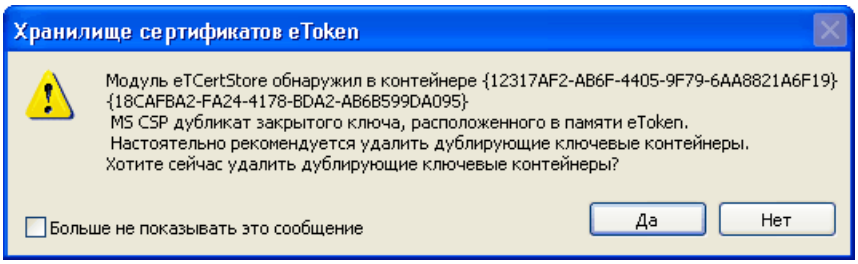
Проверка дублирования закрытых ключей

Утилита "Свойства eToken" позволяет осуществлять проверку того, имеют ли закрытые ключи в памяти eToken копии на данном компьютере. Если вы хотите сделать такую проверку автоматической, установите флажок **Отслеживать дублирование ключей**. Для того чтобы осуществить проверку вручную, нажмите **Найти дубликаты ключей**. В этом случае при отсутствии дублирования на экране появится окно **Свойства eToken** с сообщением:

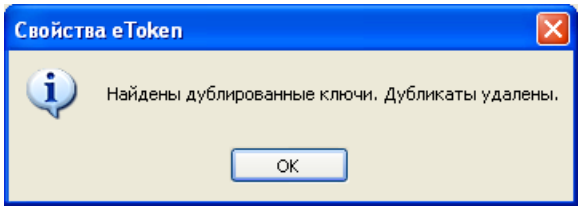
```
Дубликаты ключей не найдены.
```



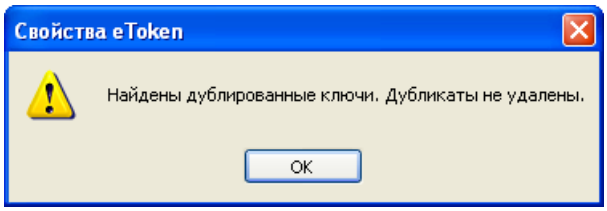
При обнаружении дублирования закрытых ключей на экране появляется диалоговое окно **Хранилище сертификатов eToken** с сообщением об обнаружении дублирования.



Для удаления дублирующего ключевого контейнера с жёсткого диска компьютера нажмите **Да** и затем **OK** в окне подтверждения.



Если вы не хотите устранять дублирование нажмите **Нет** и затем **OK** в окне подтверждения.



Примечание:

Аппаратная генерация закрытых ключей с помощью eToken исключает возможность их дублирования.

Сертификаты центров сертификации

При подключении к компьютеру eToken, в памяти которого содержится хотя бы один сертификат центра сертификации, eToken RTE 3.66 может автоматически копировать такие сертификаты в реестр. По умолчанию перед таким копированием на экране появляется диалоговое окно, предлагающее пользователю одобрить или отменить это действие. Вы можете отключить появление

этого окна, изменив значение параметра **Загрузка сертификатов ЦС**. Этот параметр может принимать следующие значения:

- **Устанавливать автоматически** — сертификаты центров сертификации устанавливаются в реестр автоматически, диалоговое окно на экране не появляется;
- **Предлагать установку** — при обнаружении в памяти подключенного eToken сертификата центра сертификации eToken RTE 3.66 предлагает пользователю установить этот сертификат в реестр;
- **Не устанавливать** — при обнаружении в памяти подключенного eToken сертификата центра сертификации eToken RTE 3.66 не предлагает пользователю установить этот сертификат в реестр и не устанавливает его самостоятельно.

Считыватели

Виртуальные считыватели

При подсоединении USB-ключа eToken к компьютеру eToken RTE автоматически назначает ему один из имеющихся в системе виртуальных считывателей. При установке eToken RTE в системе создаются два таких виртуальных устройства. Если число подсоединённых к компьютеру USB-ключей eToken больше числа виртуальных считывателей, то последнему из подключенных USB-ключей eToken виртуальный считыватель не назначен, и этот eToken недоступен для многих программ.

Имея полномочия администратора, вы можете добавить в систему один или несколько виртуальных считывателей, по количеству имеющихся портов USB. Некоторые приложения, работающие только с одним eToken, корректно работают только при наличии в системе ровно одного виртуального считывателя. В таких случаях может потребоваться удаление из системы излишних виртуальных считывателей.

Определение количества виртуальных считывателей и изменение этого количества

Количество виртуальных считывателей отображается в разделе **Управление считывателями**. Для того чтобы уменьшить или увеличить это количество, измените значение соответствующего поля.

Отображение свободных считывателей

Если вы хотите, чтобы в окне **Свойства eToken** отображались считыватели, к которым не подключено ни одного eToken, нажмите **Отображать свободные**. Для того чтобы отменить отображение свободных считывателей, нажмите **Скрывать свободные**.

Режим энергосбережения

Если вы хотите, чтобы при переходе компьютера в ждущий режим отключалось питание от eToken, установите флажок **Включать энергосбережение через** и укажите время в секундах, по прошествии которого в случае отсутствия обращений к eToken питание может быть отключено. Если при осуществлении настройки режима энергосбережения к компьютеру был подключен eToken, сделанная настройка будет распространяться на него лишь после отключения и повторного подключения данного eToken.

Примечание:

Для того чтобы осуществлять настройки режима энергосбережения, необходимо иметь полномочия администратора.

Операции с eToken

Выбор eToken

В списке eToken в окне **Свойства eToken** присутствуют eToken, подключенные к считывателям. В списке отображаются цвет, имя eToken и имя считывателя. Для того чтобы выбрать eToken, нажмите на соответствующий значок.

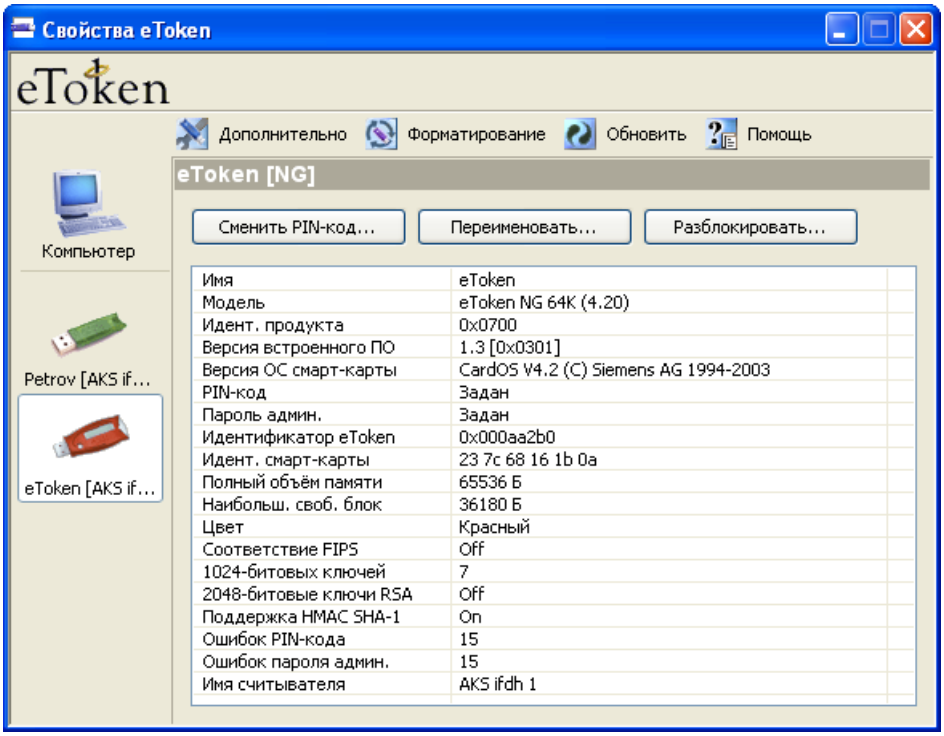
Режимы работы с eToken

Различным типам прав доступа к eToken соответствуют четыре режима работы с eToken в утилите "Свойства eToken".

1. **Гостевой режим** — доступ к общей информации относительно eToken.
2. **Пользовательский режим** — осуществление основных и дополнительных операций.

Гостевой режим

До того как вы ввели PIN-код или пароль администратора, утилита "Свойства eToken" работает с вашим eToken в гостевом режиме.



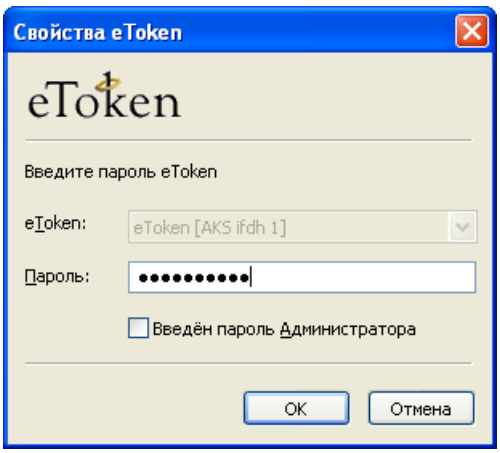
Для перехода в другие режимы вам потребуется вводить PIN-код или/и пароль администратора. После этого интерфейс гостевого режима (кроме кнопки для смены и разблокирования PIN-кода с участием удалённого администратора) будет доступен во вкладке **Подробности**.

Переход из гостевого режима в пользовательский

Для перехода из гостевого режима в пользовательский:

- нажмите Дополнительно;

- в поле **Пароль** введите PIN-код;



- при наличии флажка **Введён пароль Администратора** убедитесь в том, что он не установлен;
- нажмите **OK**.

Доступ к общей информации

Для того чтобы просмотреть информацию о значении основных параметров одного из подключенных устройств eToken, отображённых в окне **Свойства eToken**, выберите этот eToken. В гостевом режиме в окне сразу появится общая информация относительно данного eToken. В других режимах откройте вкладку **Подробности**.

Основные параметры eToken:

- **Имя** — имя eToken;
- **Тип —** тип устройства eToken (eToken PRO, eToken NG-OTP, eToken NG FLASH). Для eToken NG-FLASH дополнительно указывается размер флеш-памяти;
- **Модель** — строка, характеризующая конкретный вариант реализации ключа eToken и встроенного программного обеспечения;
- **Версия встроенного ПО** (только для USB-ключей) — версия встроенного программного обеспечения (firmware);
- **Идент. Продукта —** идентификатор продукта;
- **Версия ОС смарт-карты** — версия операционной системы смарт-карты;
- **PIN-код** — параметр, принимающий значение `Не задан` для неинициализированных eToken и значение `Задан` для всех прочих исправных eToken;
- **Пароль admин.** — параметр, принимающий значение `Не задан` для eToken, при форматировании которых не был установлен пароль администратора, и значение `Задан`, если пароль администратора установлен;
- **Идентификатор eToken** (только для USB-ключей) — уникальный идентификатор eToken;
- **Идентификатор смарт-карты** — уникальный идентификатор смарт-карты;
- **Полный объём памяти** — общий объём памяти;
- **Наибольш. своб. блок** — объём наибольшего непрерывного фрагмента свободной области памяти;
- **Цвет** — цвет;
- **Соответствие FIPS** (только для USB-ключей eToken PRO с версиями встроенного программного обеспечения (firmware) 4.x.5.4) — параметр, принимающий значение **On**, если eToken соответствует федеральному стандарту США по обработке информации (FIPS), и **Off** в противном случае;

- **1024-битовых ключей** — максимальное количество 1024-битовых ключей RSA, которые можно хранить в памяти данного eToken;
- **2048-битовые ключи RSA** — параметр, принимающий значение **On**, если eToken поддерживает генерирование и хранение ключей RSA длиной 2048 бит, и **Off** в противном случае;
- **Поддержка HMAC SHA-1** — параметр, принимающий значение **On**, если eToken поддерживает алгоритм HMAC SHA-1, и **Off** в противном случае;
- **Ошибок PIN-кода** — количество попыток ввода неправильного PIN-кода подряд, при достижении которого PIN-код блокируется.
- **Ошибок пароля админ.** — количество попыток ввода неправильного пароля администратора, при достижении которого пароль администратора блокируется.
- **Запоминающее устройство (только для eToken NG-FLASH)** — параметр, принимающий значение **Задан** для устройств eToken NG-FLASH;
- **Имя считывателя** — имя физического или виртуального устройства чтения смарт-карт, к которому подключен eToken.

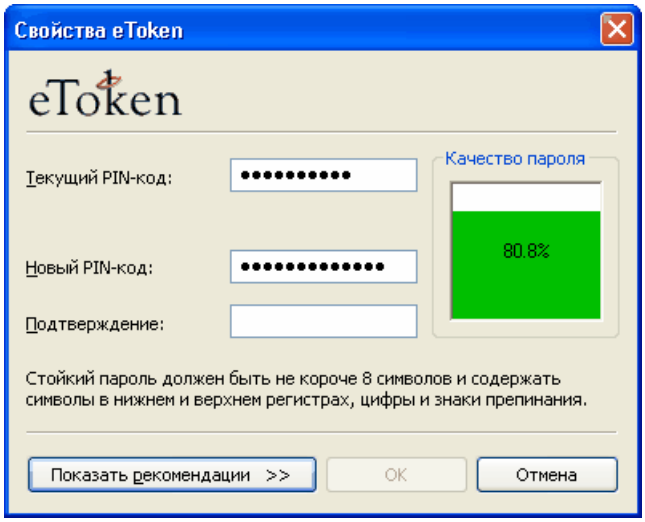
Основные операции

Смена PIN-кода пользователем

Новые eToken имеют предустановленный на заводе PIN-код со значением 1234567890.

В целях безопасности рекомендуется сменить PIN-код. Для того чтобы сменить PIN-код выбранного eToken:

- в гостевом режиме или во вкладке **Подробности** нажмите **Сменить PIN-код**;
- в появившемся окне введите текущий PIN-код в поле **Текущий PIN-код**, а новый PIN-код — в поля **Новый PIN-код** и **Подтверждение**;



- оценка качества PIN-кода отображается в области **Качество пароля**;

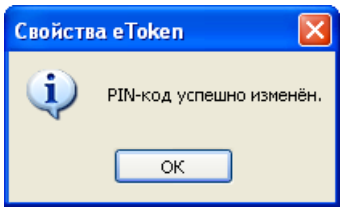
Примечание:

PIN-код должен удовлетворять требованиям качества, которые задаются администратором.

- для получения сведений о недостатках введённого PIN-кода вы можете нажать **Показать рекомендации**;
- кнопка **OK** будет неактивной до тех пор, пока не введена удовлетворительная информация в поля **Текущий PIN-код** и **Новый PIN-код**;
- нажмите **OK**;

- в случае успешной смены PIN-кода на экране появится окно **Свойства eToken** с сообщением:

  PIN-код успешно изменён.

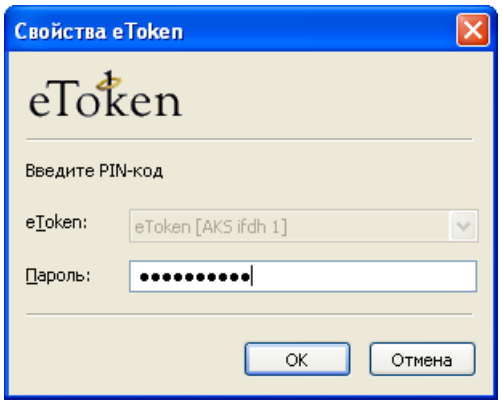


- нажмите **OK**.

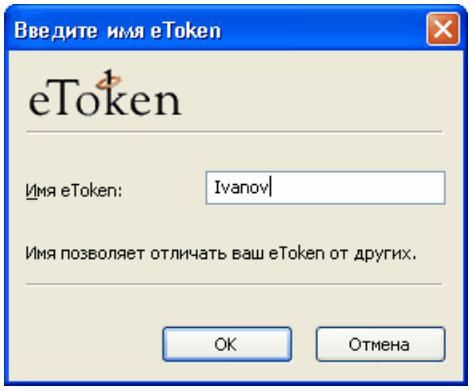
Переименование eToken

Для того чтобы изменить имя выбранного eToken:

- в гостевом режиме или во вкладке **Подробности** нажмите **Переименовать**;
- при необходимости введите PIN-код eToken и нажмите **OK**;



- в окне **Введите имя eToken** внесите изменения в поле **Имя eToken**.



Примечание:

Не рекомендуется использовать в имени eToken русские буквы.

- нажмите **OK**.

Дополнительные операции

Настройка кэширования содержания закрытой области памяти

В целях повышения производительности eToken RTE может кэшировать содержание закрытой области памяти eToken (кроме закрытых ключей). Однако использование этой возможности понижает безопасность.

Если eToken имеет пароль администратора, то администратор может лишить пользователя права настраивать параметры кэширования содержания закрытой области памяти.

Для того чтобы настроить параметры кэширования, выполните следующую последовательность действий.

1. В пользовательском режиме откройте вкладку **Настройки**, а в администраторском — вкладку **Администратор**.
2. Во вкладке **Администратор** можно разрешать или запрещать настройки кэширования закрытой области памяти в пользовательском режиме. Для этого в области **Кэшировать закрытые данные** соответственно устанавливайте или снимайте флажок **Доступно пользователю**.
3. В области **Кэшировать закрытые данные** выберите режим кэширования. Вы можете выбрать один из трёх режимов:
   - **Всегда** — режим с наибольшей производительностью и наименьшей безопасностью;
   - **При введённом PIN-коде** — кэширование только во время сеанса работы с eToken;
   - **Никогда** — кэширование отключено.

После того как вы внесёте изменения:

- для сохранения изменений нажмите **Применить**, а затем нажмите **OK**;
- для отмены нажмите **Отменить изменения**.

Если вы хотите восстановить значения по умолчанию, нажмите **Восстановить значения по умолчанию**, а затем нажмите **Применить**.

Настройки паролей закрытых ключей

Закрытый ключ RSA, генерируемый в eToken, может быть при создании дополнительно защищён паролем, не зависящим от PIN-кода и пароля администратора. В eToken RTE предусмотрено четыре варианта настройки eToken PRO для таких паролей:

- **Обязательный** — пароль обязательно задаётся для каждого нового закрытого ключа; при генерировании закрытого ключа на экране появляется окно для задания пароля; в случае нажатия кнопки **Отмена** генерирования ключей не происходит;
- **Всегда запрашивать** — при генерировании каждого закрытого ключа на экране появляется окно для задания пароля; пользователь может либо ввести пароль, либо отменить ввод пароля, нажав **Отмена**;
- **По требованию приложения** — окно для задания пароля появляется на экране только в случае, если приложение, для которого создаётся ключевая пара, требует повышенной защиты закрытого ключа;
- **Никогда не запрашивать** — дополнительная защита закрытого ключа с помощью пароля запрещена.

Если eToken имеет пароль администратора, то администратор может лишить пользователя права настраивать пароль закрытого ключа.

Для внесения изменений в настройки пароля закрытого ключа выполните следующее.

1. В пользовательском режиме откройте вкладку **Настройки**, а в администраторском или смешанном — вкладку **Администратор**.
2. Во вкладке **Администратор** можно разрешать или запрещать выбор настройки пароля закрытого ключа в пользовательском режиме. Для этого в области **Пароль для ключа RSA** соответственно устанавливайте или снимайте флажок **Доступно пользователю**.
3. В области **Пароль для ключа RSA** выберите вариант настройки пароля закрытого ключа.

После того как вы внесёте изменения:

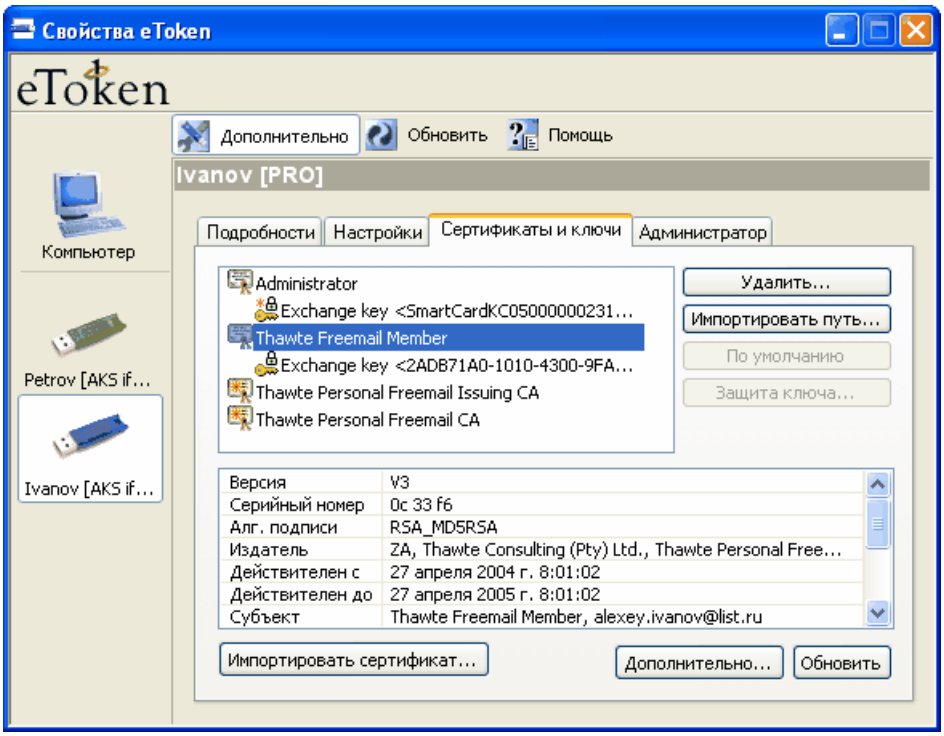
- для сохранения изменений нажмите **Применить**, а затем нажмите **OK**;
- для отмены нажмите **Отменить изменения**.

Если вы хотите вернуть исходные значения, нажмите **Восстановить значения по умолчанию**, а затем нажмите **Применить**.

Просмотр и удаление сертификатов и ключевых контейнеров

В пользовательском и администраторском режимах вы можете с помощью утилиты "Свойства eToken" просматривать и удалять сертификаты из хранилища eToken и ключевые контейнеры. Для этого:

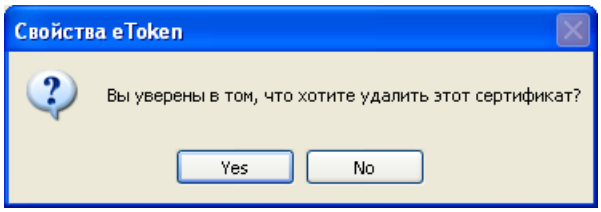
- откройте вкладку Сертификаты и ключи;



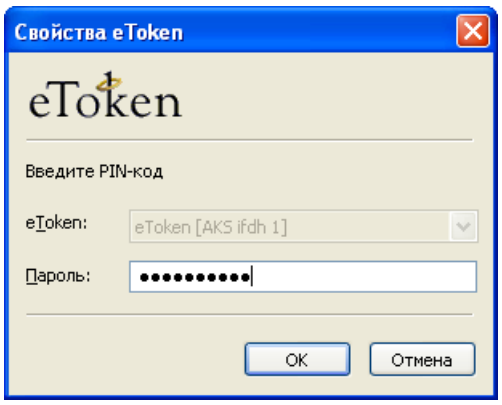
- выберите сертификат или ключевой контейнер;
- просмотрите параметры выбранного объекта.

Для удаления выбранного ключевого контейнера или сертификата, не связанного с ключевым контейнером:

- нажмите **Удалить**;
- в окне подтверждения нажмите **Yes** (Да);

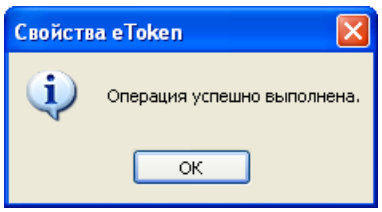


- при необходимости введите PIN-код и нажмите **OK**;



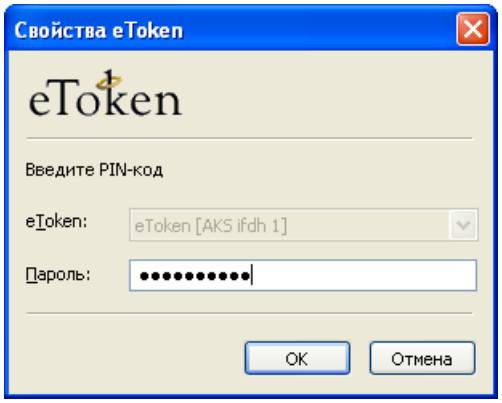
Важно: если вы удаляете ключевой контейнер, с которым связаны сертификаты, эти сертификаты также будут удалены из памяти eToken.

- в случае успешного выполнения операции на экране появится окно с подтверждением:

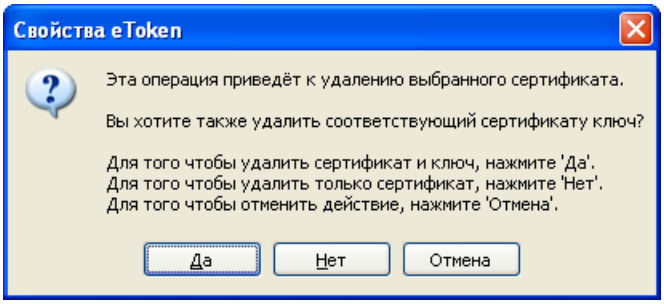


Для удаления выбранного сертификата, связанного с ключевым контейнером:

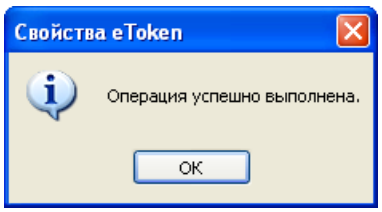
- нажмите **Удалить**;
- если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**;



- если вы хотите, чтобы вместе с сертификатом был удалён и связанный с ним ключевой контейнер, нажмите **Да**, если же вы хотите удалить сертификат, сохранив ключевой контейнер, нажмите **Нет**;



- в случае успешного выполнения операции на экране появится окно с подтверждением:

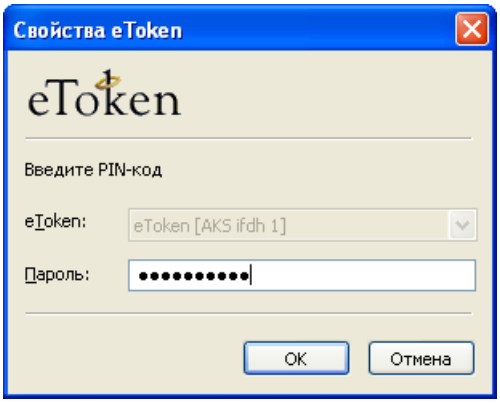


- нажмите **OK**.

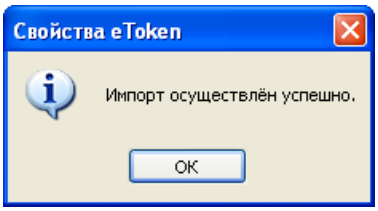
Импорт пути сертификации

Для того чтобы скопировать в память eToken сертификаты всех центров сертификации, входящих в путь сертификации выбранного сертификата:

- откройте вкладку Сертификаты и ключи;
- выберите сертификат;
- нажмите Импортировать путь;
- если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**;



- если импорт будет осуществлён успешно, на экране появится окно с сообщением об этом;



- нажмите **OK**.

Сертификаты центров сертификации появятся в списке сертификатов и ключей.

Выбор ключевого контейнера по умолчанию

Если в памяти вашего eToken присутствуют два сертификата пользователя со смарт-картой, в некоторых приложениях вы не можете всякий раз выбирать, какой из них использовать. Вместо этого такие приложения обращаются к сертификату, соответствующему ключевому контейнеру по умолчанию.

Утилита "Свойства eToken" позволяет выбирать ключевой контейнер, который будет использоваться в таких случаях по умолчанию. Если вы измените ключевой контейнер по умолчанию, прежний ключевой контейнер по умолчанию будет удалён вместе с соответствующим сертификатом. Для того чтобы сделать это:

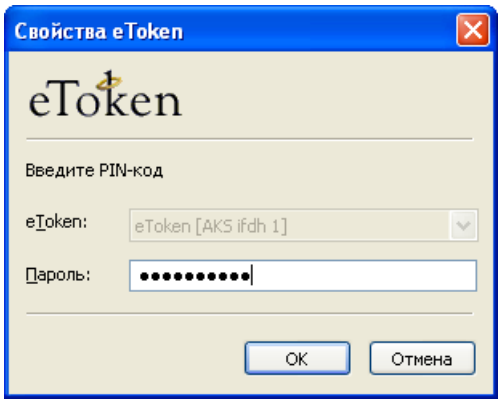
- откройте вкладку Сертификаты и ключи;
- выберите ключевой контейнер, соответствующий сертификату пользователя со смарт-картой, не являющийся ключевым контейнером по умолчанию;

- нажмите **По умолчанию**;

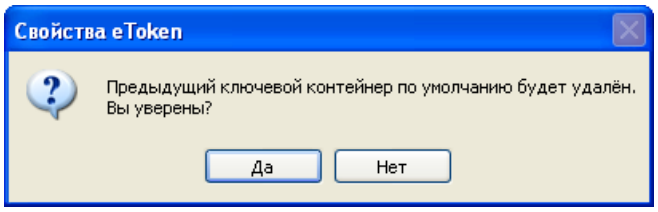
Примечания:

- значок ключевого контейнера по умолчанию содержит символ * (), а значок ключевого контейнера, не являющегося контейнером по умолчанию, не содержит этого символа ();
- кнопка **По умолчанию** активна только для контейнеров, соответствующих сертификатам пользователя со смарт-картой и не являющихся контейнерами по умолчанию;

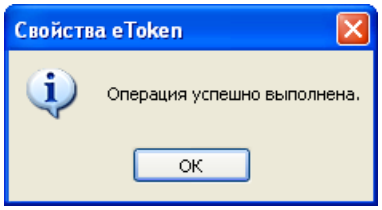
- если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**;



- убедитесь в том, что вам больше не нужны ключевой контейнер и соответствующий сертификат, использовавшиеся по умолчанию прежде, и нажмите **Да**;



- после назначения нового ключевого контейнера по умолчанию и удаления прежнего вместе с соответствующим сертификатом на экране появится окно с сообщением об успешном выполнении операции;



- нажмите **OK**.

Смена пароля ключа RSA

С помощью утилиты "Свойства eToken" вы можете сменить пароль вторичной аутентификации ключа RSA. Для того чтобы сделать это:

- откройте вкладку Сертификаты и ключи;
- выберите ключевой контейнер, защищённый паролем;

Примечание:

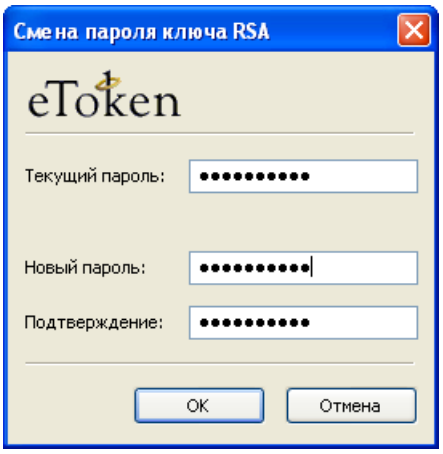
значок ключевого контейнера, защищённого паролем, содержит изображение замка ();

- нажмите Защита ключа;

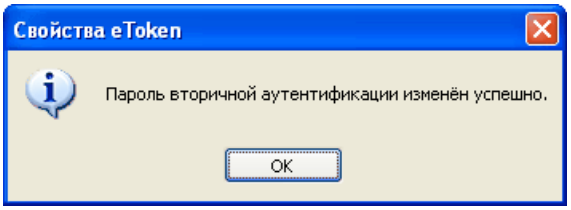
Примечание:

эта кнопка активна только при выбранном ключевом контейнере, защищённом паролем;

- в окне **Смена пароля ключа RSA** введите текущий пароль;



- введите новый пароль в поля **Новый пароль** и **Подтверждение**;
- нажмите **OK**;
- в случае успешной смены пароля на экране появится окно с подтверждающим сообщением;



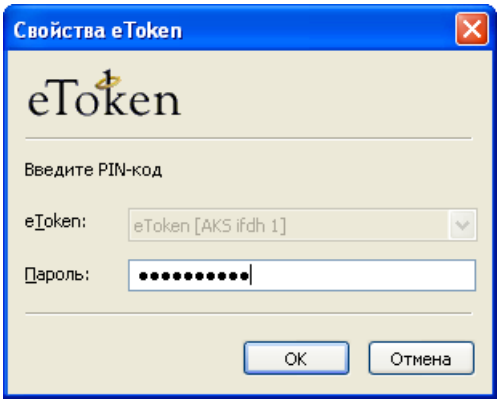
- нажмите **OK**.

Импорт сертификата с закрытым ключом

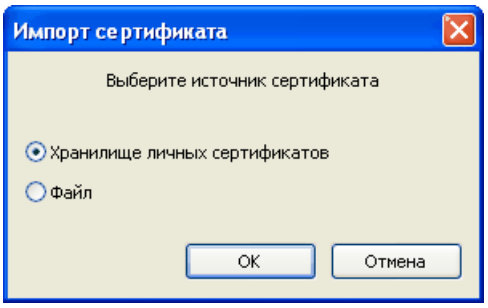
Импорт сертификата из хранилища Личные/Personal с закрытым ключом

Для того чтобы скопировать в память eToken сертификат, находящийся в хранилище Личные/Personal, вместе с соответствующим закрыты ключом, выполните следующее:

1. Откройте вкладку **Сертификаты и ключи**.
2. Нажмите **Импортировать сертификат**.
3. Если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**.

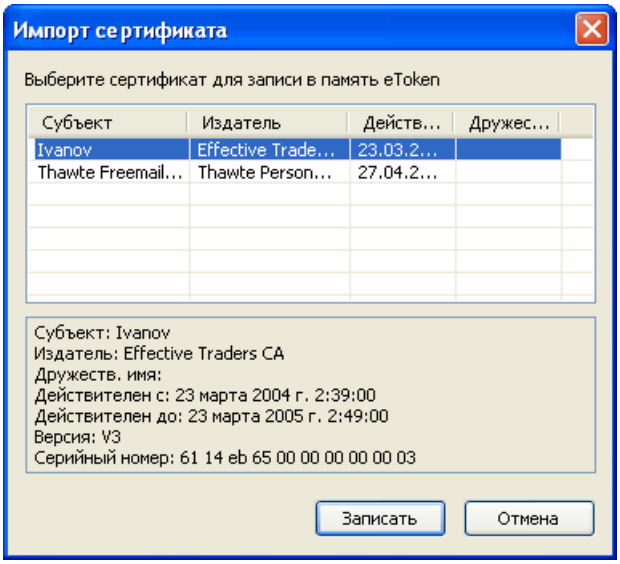


4. Выберите **Хранилище личных сертификатов** и нажмите **OK**.

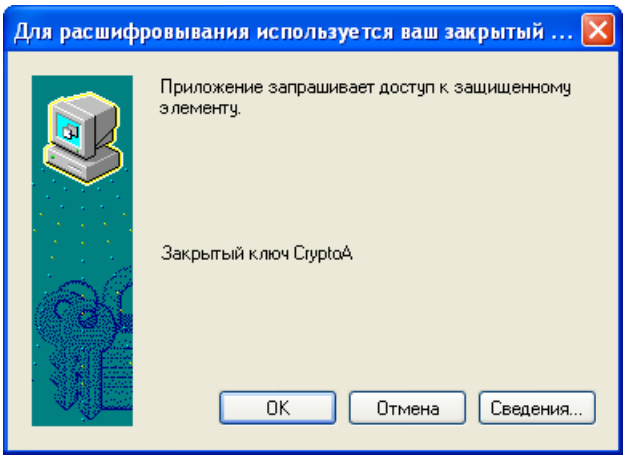


5. На экране появится список сертификатов, которые можно записать в память eToken. Он включает:
   - сертификаты, для которых соответствующие закрытые ключи уже расположены в памяти eToken;
   - сертификаты, которые могут быть импортированы с компьютера вместе с соответствующими закрытыми ключами (только для Windows XP, Windows 2000 и Windows Vista).

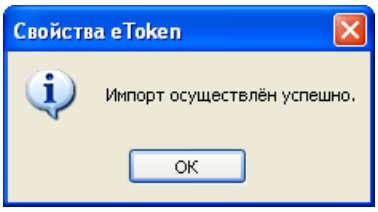
   Выберите сертификат и нажмите **Записать**.



6. При необходимости, для того чтобы разрешить доступ к закрытому ключу, который предстоит скопировать в память eToken, нажмите **OK**.



7. Если импорт будет осуществлён успешно, на экране появится окно с сообщением об этом.

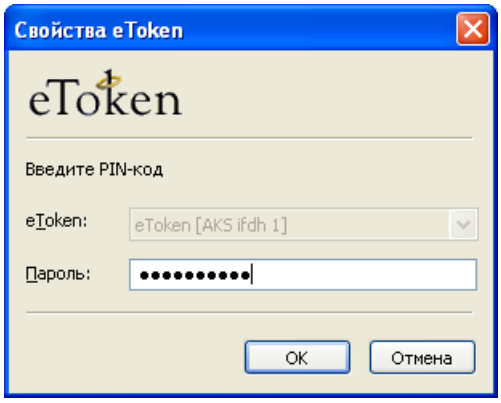


8. Нажмите **OK**.

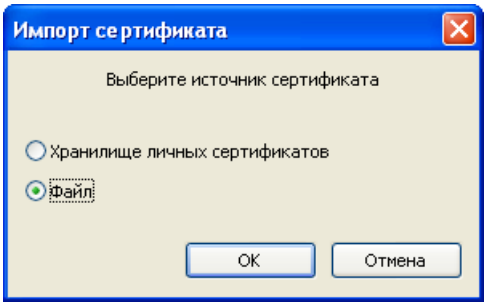
Импорт сертификата с закрытым ключом из файла

Для того чтобы импортировать сертификат с закрытым ключом из файла, выполните следующее:

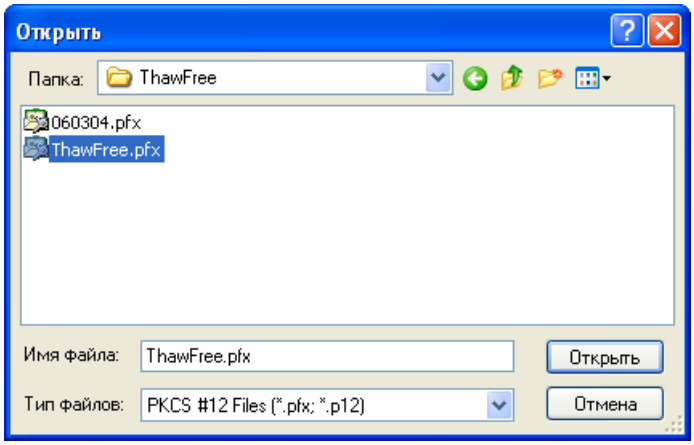
1. Откройте вкладку **Сертификаты и ключи**.
2. Нажмите **Импортировать сертификат**.
3. Если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**.



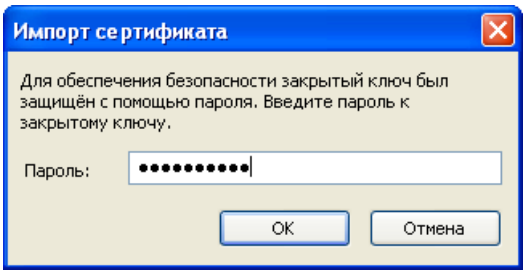
4. Выберите **Файл** и нажмите **OK**.



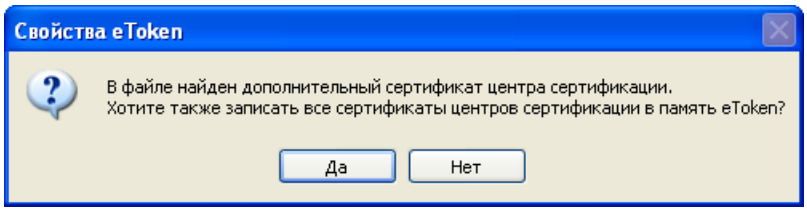
5. Укажите файл, в котором содержатся сертификат и закрытый ключ, и нажмите **Открыть**.



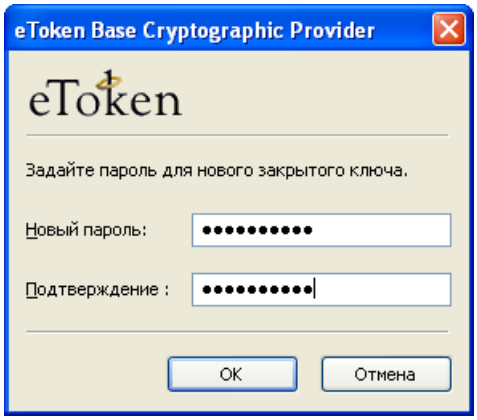
6. Для доступа к закрытому ключу, хранящемуся в файле, введите соответствующий пароль и нажмите **OK**.



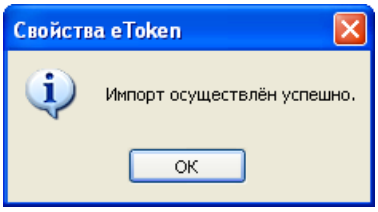
7. Если в файле содержатся сертификаты центров сертификации, на экране появится окно, информирующее вас об этом. Если вы хотите скопировать их вместе с импортируемым сертификатом в память eToken, нажмите **Да**. В противном случае нажмите **Нет**.



8. При необходимости задайте пароль вторичной аутентификации для создаваемого в памяти eToken закрытого ключа. Появление соответствующего окна и поведение утилиты "Свойства eToken" в случае нажатия кнопки **Отмена** зависит от настройки паролей закрытых ключей, описанной выше в соответствующем разделе.

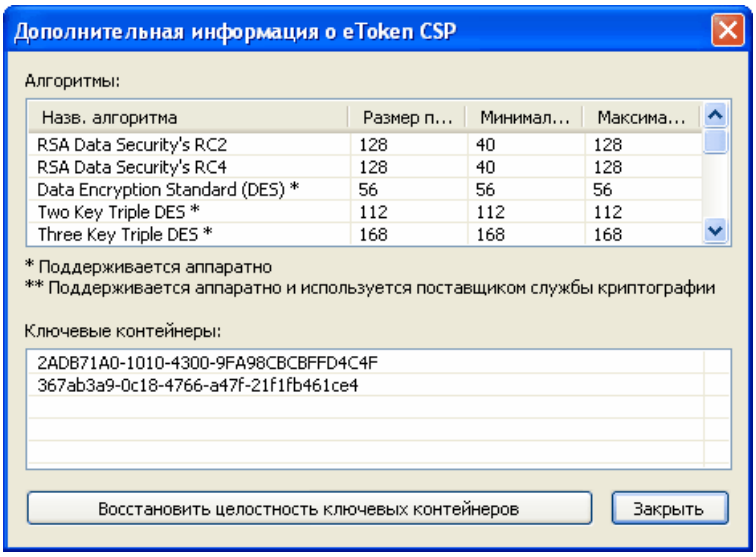


9. Если импорт будет осуществлён успешно, на экране появится окно с сообщением об этом.



Дополнительная информация о eToken CSP

Для того чтобы получить информацию о доступных алгоритмах и ключевых контейнерах, в окне **Сертификаты и ключи** нажмите **Дополнительно**.



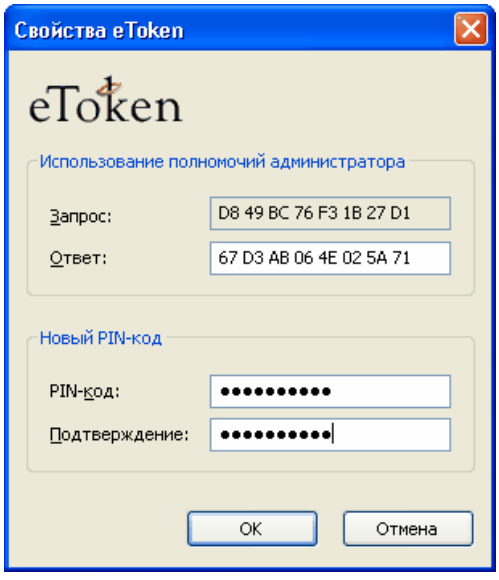
Удаленная смена PIN-кода администратором

С помощью утилиты “Свойства eToken” на стороне пользователя и системы управления токенами (Token Management System, TMS) пользователь и администратор могут сменить забытый или разблокировать заблокированный PIN-код. При этом администратор участвует в процедуре удалённо:

- пользователь обращается к администратору и сообщает ему запрос, отображаемый утилитой “Свойства eToken”, а затем вводит ответ, сообщённый администратором;
- после этого пользователь вводит PIN-код (один из предыдущих или новый) и блокировка PIN-кода снимается.

На стороне пользователя выполняются следующие шаги:

1. В гостевом режиме работы утилиты “Свойства eToken” с eToken пользователь нажимает **Разблокировать**.
2. На экране появится окно с запросом. Пользователь сообщает запрос администратору.
3. Сообщённый администратором ответ пользователь вводит в поле **Ответ**.
4. Пользователь вводит новый PIN-код в поля **PIN-код** и **Подтверждение**.



5. Пользователь нажимает **OK**.

Примечание:

После сообщения запроса администратору пользователь **НЕ ДОЛЖЕН** предпринимать никаких действий с eToken до получения ответа и завершения процедуры разблокирования. Если во время этого процесса с eToken будут осуществляться какие-либо иные действия, они повлияют на контекст процесса запроса. В этом случае разблокировать или сменить неизвестный PIN-код не удастся и придётся повторять процедуру с начала.

Завершение работы утилиты “Свойства eToken”

Для выхода из программы закройте основное окно **Свойства eToken**.

Предметный указатель