eToken. Руководство администратора

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 наличия устройства чтения смарт-карт.

eToken обладает защищенной энергонезависимой памятью и используется в качестве портативного хранилища секретных данных (ключей шифрования, имен пользователя, паролей, учетных записей, сертификатов и пр.).

PIN-код

Для получения доступа к защищенным 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.

PIN-коды должны удовлетворять критериям качества, заданным в файле `%systemroot%\system32\etpass.ini` (по умолчанию для Windows XP — `C:\WINDOWS\System32\etpass.ini`).

Примечание:

Этот файл можно редактировать с помощью утилиты eToken Properties, описание которой приведено в соответствующем разделе.

Модели eToken

eToken PRO

eToken PRO имеет микросхему смарт-карты Infineon SLE66C, аппаратно реализующую алгоритмы RSA, DES, TripleDES, SHA-1. eToken PRO снабжен встроенным генератором ключевых пар RSA. При этом закрытые ключи никогда не покидают микросхему смарт-карты. Микросхемы семейства Infineon SLE66C работают под управлением операционной системы Siemens CardOS и обеспечивают высокий уровень безопасности (сертификат ITSEC LE4).

Кроме PIN-кода пользователя, в eToken PRO предусмотрен пароль администратора. С помощью него, например, можно сменить забытый PIN-код. Пароль администратора также можно менять.

eToken PRO можно форматировать с помощью утилиты eToken Properties, входящей в состав набора драйверов eToken Run Time Environment 3.66 (далее – RTE 3.66). При форматировании:

- из памяти eToken PRO удаляется вся информация;
- устанавливается PIN-код;
- возможно задание пароля администратора;
- возможно задание ключа форматирования для предотвращения несанкционированного переформатирования.

В настоящее время выпускаются две основные версии eToken PRO. Они отличаются версиями микросхемы смарт-карты, операционной системы и встроенного программного обеспечения (firmware, только для USB-ключей) и имеют следующие особенности:

eToken PRO с операционной системой Siemens CardOS/M4.0 (4.01):

- аппаратно поддерживает алгоритм RSA с ключом только 1024 бит;
- позволяет при инициализации вместо стандартного формата выбирать формат, соответствующий федеральному стандарту США по обработке информации (FIPS, только для USB-ключей eToken PRO с версиями встроенного программного обеспечения (firmware) 4.x.5.4);
- выпускается в виде USB-ключа или смарт-карты с памятью 32 КБ;

eToken PRO с операционной системой Siemens CardOS V4.20:

- аппаратно поддерживает алгоритм RSA с ключами 1024 и 2048 бит;
- аппаратно поддерживает алгоритм HMAC SHA-1;
- одновременная поддержка алгоритмов RSA с ключом 2048 бит и HMAC SHA-1 невозможна, поддерживаемый алгоритм задается при форматировании;
- выпускается в виде USB-ключа или смарт-карты с памятью 32 или 64 КБ.

eToken NG-OTP

eToken NG-OTP — комбинированное устройство, совмещающее возможности eToken PRO с операционной системой Siemens CardOS V4.20 и генератора одноразовых паролей (One Time Password – OTP). eToken NG-OTP поддерживает генерацию одноразового пароля по протоколу OATH OTP.

eToken NG-OTP выпускается в виде USB-ключа с жидкокристаллическим дисплеем, встроенным источником питания и кнопкой генерирования одноразового пароля.

Объем памяти — 32 или 64 КБ.

eToken NG-FLASH

eToken NG-FLASH — комбинированное устройство, совмещающее возможности eToken PRO с операционной системой Siemens CardOS V4.20 и устройства хранения информации (Flash-памяти).

Объем Flash-памяти — до 4GB. Объем защищенной памяти – 64 КБ.

Примечание:

Более подробно об электронных ключах eToken вы можете узнать в документе “Архитектура eToken”.

Преимущества использования eToken

Строгая аутентификация

eToken обеспечивает двухфакторную аутентификацию с использованием USB-ключа (смарт-карты) и PIN-кода. Двухфакторная аутентификация, для которой нужно *знать нечто* (PIN-код) и *иметь нечто* (eToken) намного надежнее, чем использование имен пользователя и паролей, основанное лишь на знании этих имен пользователя и паролей.

Высокая защищенность

Секретная информация хранится в защищенной памяти USB-ключа (смарт-карты).

PIN-код eToken защищен от подбора ограничением числа возможных попыток неправильного ввода PIN-кода подряд, при превышении которого PIN-код блокируется.

В целях безопасности вы можете менять PIN-код своего eToken.

Воспользоваться потерянным или украденным eToken нельзя, если его PIN-код неизвестен.

Персонализация

Каждый eToken можно персонализировать, т.е. присвоить ему уникальное имя. Это позволит, например, быстро определить хозяина потерянного eToken без знания PIN-кода.

Компактность и удобство

Смарт-карта eToken PRO — пластиковая карточка стандартного размера. Ее удобно хранить в кармане или бумажнике.

USB-ключ eToken имеет небольшой размер и легко размещается на связке с ключами. USB-ключи eToken выпускаются в цветных корпусах.

Каждый USB-ключ eToken снабжен световым индикатором режимов работы. Горящий световой индикатор свидетельствует о готовности eToken к работе. Мигание светового индикатора eToken отображает процессы чтения памяти ключа и записи в эту память.

Уникальность

Каждый eToken имеет уникальный идентификационный номер (идентификатор смарт-карты).

Одновременное подключение

Возможна одновременная работа с несколькими eToken на одном компьютере.

Single Sign-On

Один eToken может хранить пароли, цифровые сертификаты, ключи шифрования и другую информацию, используемую различными приложениями (технология *Single Sign-On*). Поэтому пользователю нет необходимости иметь несколько eToken.

Области памяти eToken

Память eToken условно можно разбить на пять областей:

- системная;
- открытая;
- закрытая;
- свободная;
- область Flash-памяти (только для eToken NG-FLASH).

Системная область содержит файловую и операционную системы. В ней хранятся имя eToken и данные, необходимые для проверки правильности вводимых PIN-кодов, паролей администратора и ключей форматирования.

Открытая, закрытая и свободная области не имеют фиксированных границ. Для получения доступа к каждому объекту, записанному в память eToken, может требоваться или не требоваться ввод PIN-кода или пароля администратора. Если ввод PIN-кода или пароля администратора требуется, то объект относится к закрытой области памяти, а если не требуется — к открытой. Свободная область памяти не содержит объектов. Возможность доступа к той или иной области памяти eToken зависит от наличия необходимых прав.

Область флеш-памяти присутствует только у eToken NG-FLASH. Данная область предназначена для хранения пользовательских данных и в операционной системе идентифицируется как дополнительный логический диск. Данная область памяти может быть разделена на секцию ROM (Read Only Memory, память только для чтения) с файловой системой CDFS и секцию Mass Storage (флеш-память, память для чтения и записи) с файловой системой FAT16, FAT32 или NTFS. Соответственно, при разделении данной области на секции ROM и Mass Storage в операционной системе появляется новый логический диск и эмулируется CD-ROM. Распределение флеш-памяти eToken NG-FLASH осуществляется с помощью утилиты eToken NG-FLASH Partition, описание которой приведено в разделе “Утилита eToken NG-FLASH Partition”.

Права доступа к eToken

В зависимости от модели eToken и параметров, выбранных при форматировании, можно выделить четыре типа прав доступа к eToken:

- гостевой — возможность просматривать объекты в открытой области памяти; возможность получения из системной области памяти общей информации относительно eToken, включающей имя eToken, идентификаторы и некоторые другие параметры;
- пользовательский — право просматривать, изменять и удалять объекты в закрытой, открытой и свободной областях памяти; возможность получения общей информации относительно eToken; право менять PIN-код и переименовывать eToken; право настраивать параметры кэширования содержания закрытой области памяти и дополнительной защиты закрытых ключей паролем (при отсутствии пароля администратора или с разрешения администратора), право просмотра и удаления сертификатов в хранилище eToken и ключевых контейнеров RSA;
- администраторский — право менять PIN-код пользователя, не зная его; право смены пароля администратора; право настраивать параметры кэширования содержания закрытой области памяти и дополнительной защиты закрытых ключей паролем, а также возможность делать эти настройки доступными в пользовательском режиме;
- инициализационный — право форматировать eToken PRO.

Для того чтобы воспользоваться гостевым правом доступа, не надо знать ни PIN-код, ни какие-либо иные параметры.

Для доступа к памяти eToken с правами пользователя необходимо ввести PIN-код.

Администраторский доступ к eToken PRO возможен только после правильного введения пароля администратора. Если пароль администратора не задан при форматировании eToken, то обратиться к eToken с правами администратора невозможно.

В зависимости от настроек, использовавшихся при форматировании eToken, для получения инициализационного права доступа может потребоваться знание следующих параметров:

- ключ форматирования — если этот параметр был задан вручную при последнем форматировании;
- PIN-код или пароль администратора (любой из этих параметров) — если eToken имеет формат Generic FIPS eToken PRO OS4 (только для USB-ключей eToken PRO с версиями встроенного программного обеспечения (firmware) 4.x.5.4).

Если eToken имеет стандартный формат, а ключ форматирования принимает значение по умолчанию, то инициализационным правом доступа к eToken может воспользоваться любой желающий. Если ключ форматирования был задан вручную при последнем форматировании eToken, то пользователь, не знающий его, не может переформатировать данный eToken.

Если eToken имеет формат Generic FIPS eToken PRO OS4, то пользователь, не знающий ни PIN-кода, ни пароля администратора, не может переформатировать данный eToken. Если при последнем форматировании eToken PRO был вручную задан ключ форматирования и использовался формат Generic FIPS eToken PRO OS4, то для переформатирования необходимо как знание ключа форматирования, так и знание PIN-кода или пароля администратора.

Системные требования

Для использования eToken персональный компьютер должен удовлетворять следующим минимальным требованиям:

- установленная операционная система Windows 95 OSR2, Windows 98, Windows NT 4.0 (с установленным пакетом обновления 6 или выше), Windows Me, Windows 2000 (с установленным пакетом обновления 4 или выше), Windows XP, Windows Server 2003 или Windows Vista. 64-битные версии операционных систем Windows не поддерживаются RTE 3.66.
- для операционных систем Windows 95 OSR2, Windows 98, Windows NT 4.0 — браузер Microsoft Internet Explorer 5.0 или выше;
- 10 МБ свободного места на жестком диске;
- при использовании USB-ключей eToken — наличие свободного работающего порта USB;
- при использовании смарт-карт eToken PRO — наличие установленного устройства чтения смарт-карт, поддерживающего смарт-карты eToken PRO (например, ASEDrive III).

Для установки программного обеспечения необходима служба Microsoft Windows Installer версии 1.2 или выше. Эта служба встроена в Windows 2000, Windows Server 2003, Windows Me, Windows XP и Windows Vista. На компьютер, работающий под управлением операционной системы Windows 98 или Windows NT 4.0, предварительно установите Microsoft Windows Installer, загрузив программу установки с Web-сервера Microsoft (http://www.microsoft.com/downloads/).

Для работы с приложениями, использующими eToken, компьютер должен также удовлетворять требованиям, изложенным в документации к этим приложениям.

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;
- форматировать eToken;
- настраивать критерии качества PIN-кодов.

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.

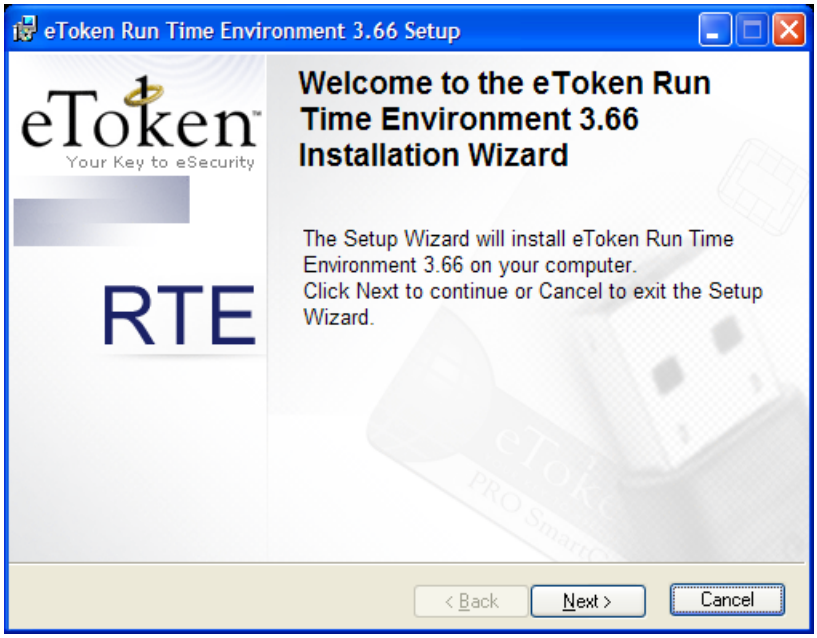
Установка и удаление на локальном компьютере

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).

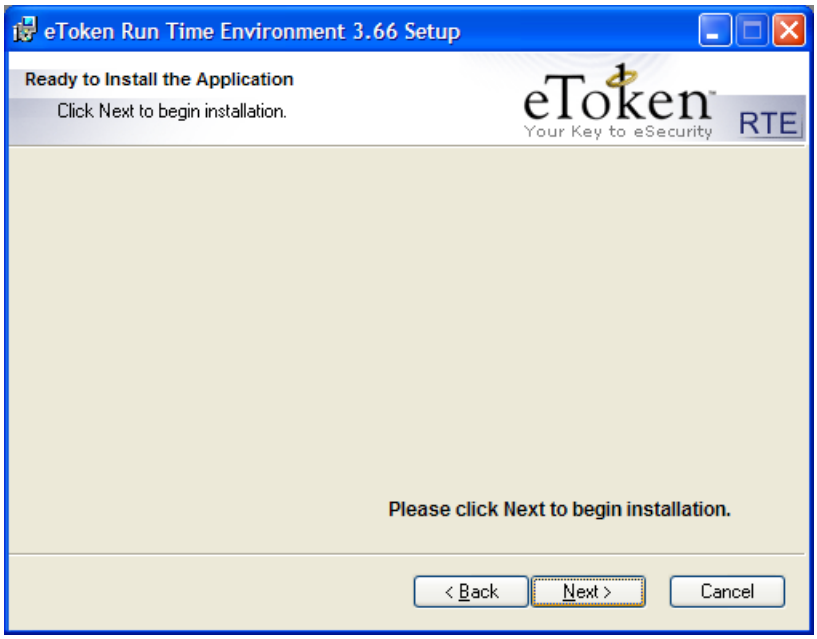


3. В окне **eToken Run Time Environment 3.66 Setup** / **End-User License Agreement** ознакомьтесь с лицензионным соглашением (на английском языке) и, если вы согласны с его условиями, выберите **I accept the license agreement** (Я принимаю лицензионное соглашение), чтобы продолжить установку.

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).

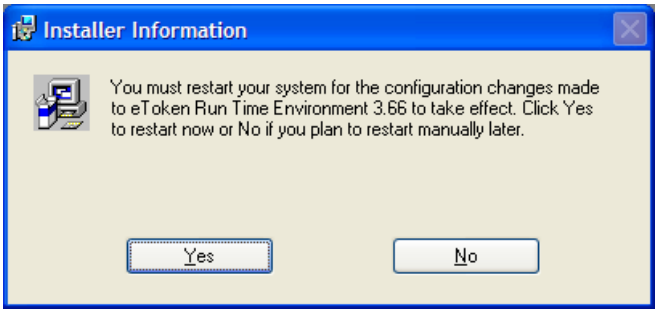
5. В окне **eToken Run Time Environment 3.66 Setup** / **Ready to Install the Application** нажмите **Next** (Далее).



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

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).

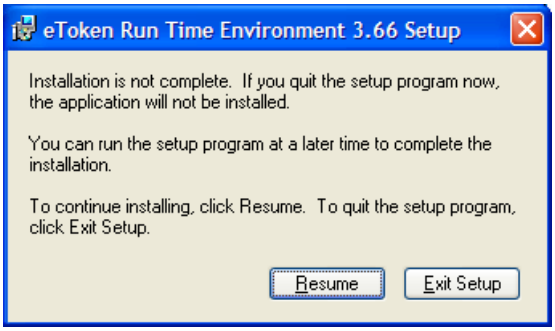
8. В конце процесса установки eToken Run Time Environment 3.66 может потребоваться перезагрузка компьютера. В этом случае в окне **Installer Information** нажмите **Yes** (Да) для немедленной перезагрузки или **No** (Нет), если вы планируете перезагрузить компьютер позднее.



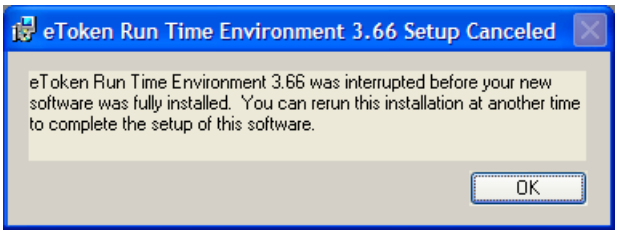
Отказ от установки

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).



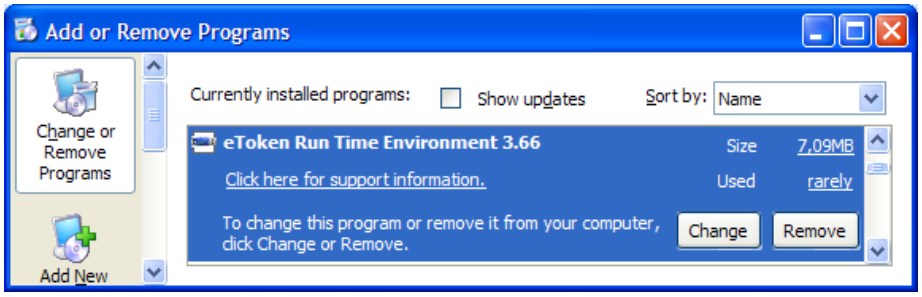
3. Нажмите **OK**.



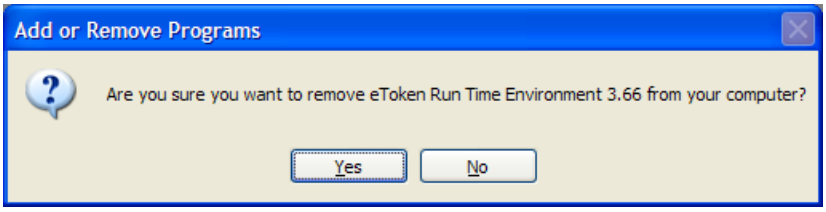
Удаление

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).

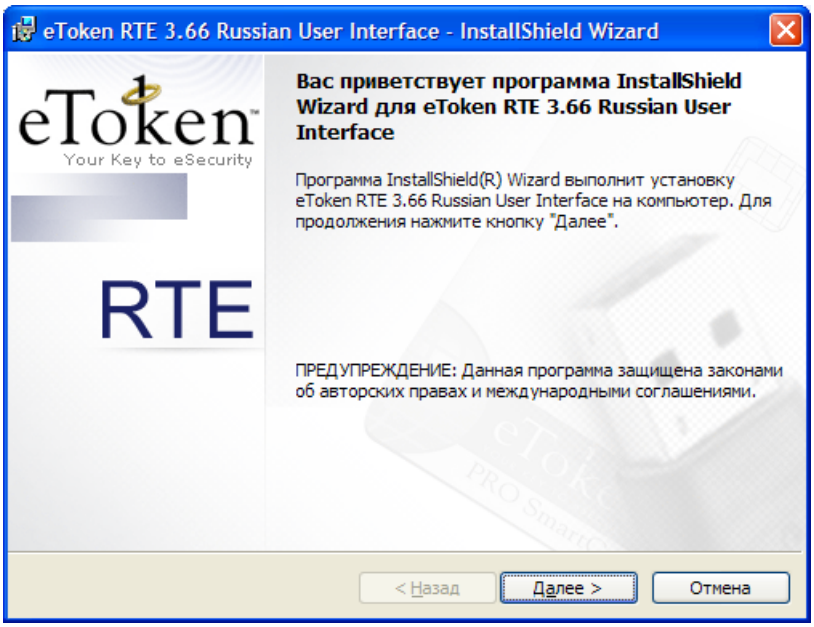


eToken RTE 3.66 RUI

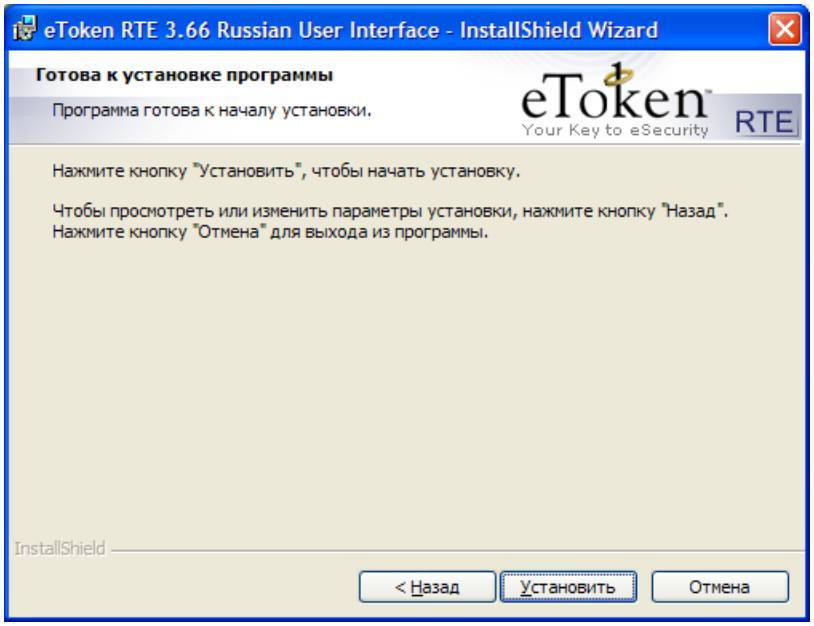
Установка

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

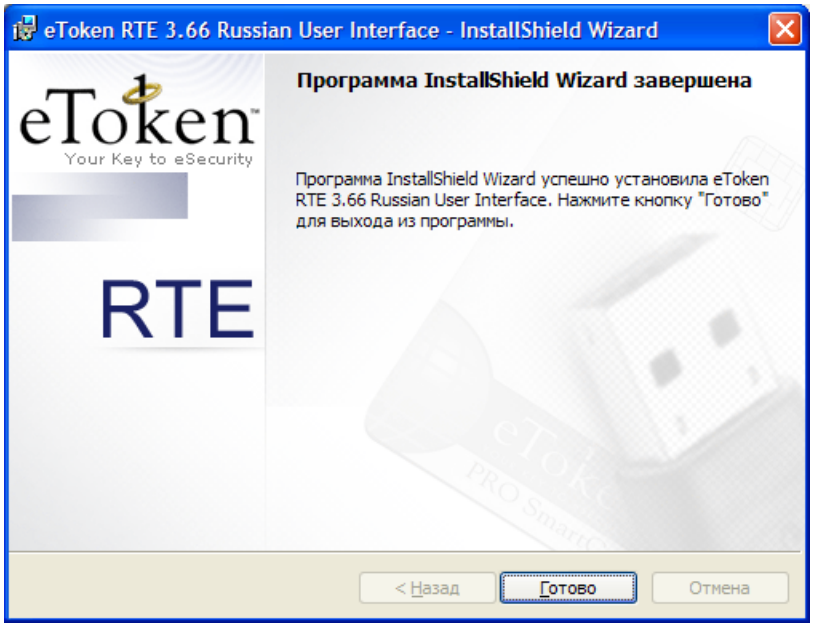
1. Запустите программу установки eToken RTE 3.66 RUI.
2. В окне приветствия программы установки eToken RTE 3.66 RUI нажмите **Далее**.



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



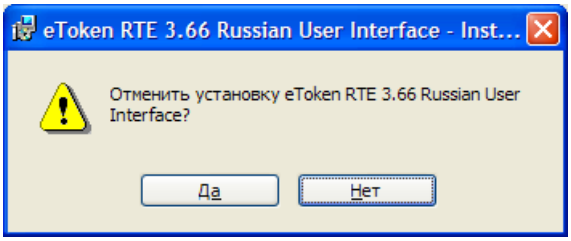
4. По завершении процесса установки eToken RTE 3.66 RUI в окне **eToken RTE 3.66 Russian User Interface – InstallShield Wizard** / **Программа InstallShield Wizard завершена** нажмите **Готово**.



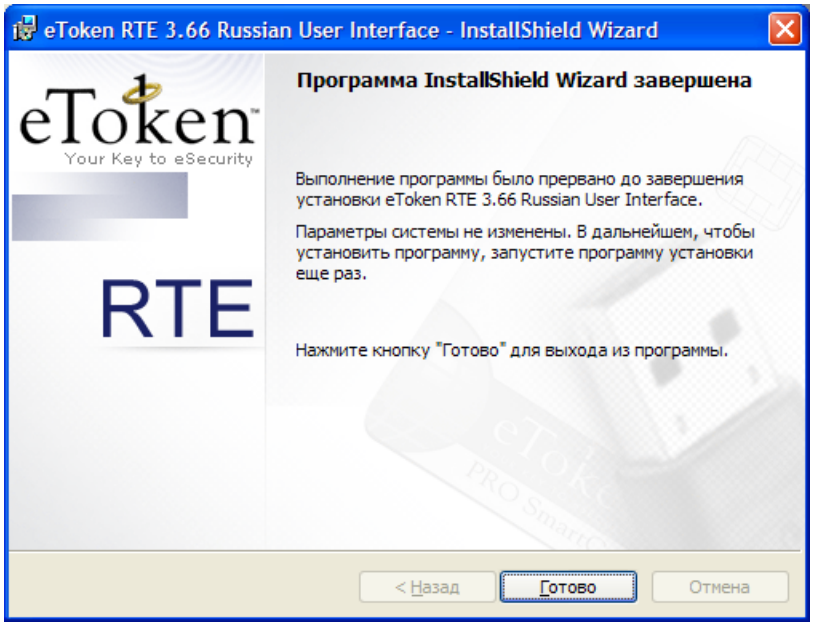
Отказ от установки

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**;



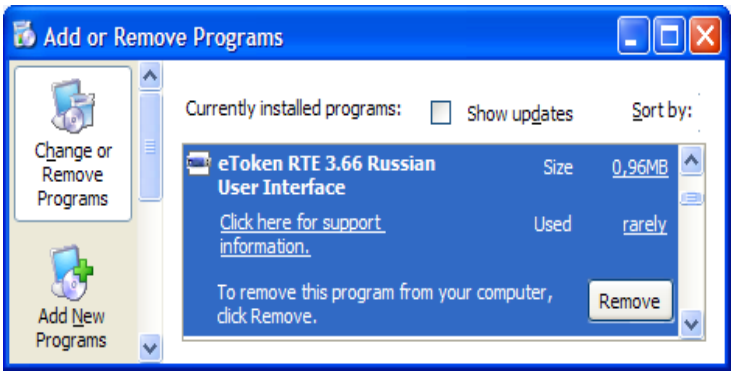
- для завершения работы программы установки нажмите **Готово**.



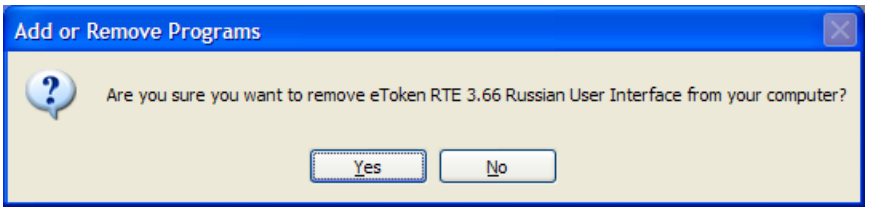
Удаление

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).



Использование командной строки

Для локальной, централизованной и удаленной установки и удаления eToken RTE 3.66 и eToken RTE 3.66 RUI можно использовать командную строку. Примеры команд:

- `msiexec /qn /i <pack.msi>` — установка eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме без диалоговых окон с параметрами по умолчанию;
- `msiexec /qb /i <pack.msi>` — установка eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме с параметрами по умолчанию и отображением процесса установки на экране;
- `<pack.msi> /q` — установка eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме без диалоговых окон с параметрами по умолчанию;
- `<pack.msi> /qb` — установка eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме с параметрами по умолчанию и отображением процесса установки на экране;
- `msiexec /qn /x <pack.msi>` — удаление eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме без диалоговых окон;
- `msiexec /qb /x <pack.msi>` — удаление eToken RTE 3.66 (eToken RTE 3.66 RUI) в автоматическом режиме с отображением процесса удаления на экране;

где `<pack.msi>` — сетевой или локальный путь к файлу `rte_3.66.msi или rte_3.66.RUI.msi`.

Дополнительные параметры

ETPROPS_MODE

По умолчанию в eToken RTE 3.66 используется основной режим интерфейса утилиты eToken Properties (Свойства eToken). При установке из командной строки вы можете выбрать пользовательский режим интерфейса. Для этого в конце команды добавьте параметр `ETPROPS_MODE=0`. Подробнее о режимах интерфейса утилиты eToken Properties см. далее в соответствующих главах разделов “Режимы интерфейса утилиты “Свойства eToken” и “Настройки eToken RTE в системном реестре”.

LOAD_LOCAL

По умолчанию eToken RTE 3.66 не копирует сертификаты из хранилища eToken в реестр автоматически. При установке из командной строки вы можете включить автоматическое копирование сертификатов из хранилища eToken в реестр. Для этого в конце команды добавьте параметр `LOAD_LOCAL=1`.

AUTO_DUPLICATION_CHECK

По умолчанию в eToken RTE 3.66 автоматическое отслеживание дубликатов закрытых ключей, расположенных в памяти eToken, не осуществляется. При установке из командной строки вы можете включить такое отслеживание. Для этого в конце команды добавьте параметр `AUTO_DUPLICATION_CHECK=1`.

FRIENDLY_NAME_VER

По умолчанию в eToken RTE 3.66 при отсутствии автоматического копирования сертификатов из хранилища eToken в реестр в качестве понятного имени сертификата, хранящегося в памяти eToken, используется имя считывателя, за котором следует наименование субъекта (например, `AKS ifdh 0::Thawte Freemail Member`). eToken RTE поддерживает и другой формат: наименование субъекта, назначение, имя считывателя (например, `Thawte Freemail Member: Проверка подлинности сертификата, Проверка подлинности клиента, Подписывание кода, Защищенная электронная почта, установка штампа времени... reader::AKS ifdh 0`). Для того чтобы этот формат был использован вместо формата по умолчанию, в конце команды добавьте параметр `FRIENDLY_NAME_VER=2` (и не добавляйте параметр `LOAD_LOCAL=1`).

CA_CERT_MODE

Если в памяти eToken, подключенного к компьютеру, содержится сертификат центра сертификации, отсутствующий в реестре, по умолчанию на экране появляется диалоговое окно, предлагающее

пользователю скопировать этот сертификат в реестр. Появление этого окна можно отключить при установке из командной строки, добавив в конце команды параметр:

- `CA_CERT_MODE=1` — для того чтобы такие сертификаты копировались в реестр автоматически;
- `CA_CERT_MODE=2` — для того чтобы отключить копирование сертификатов центров сертификации в реестр.

ET_PROCLISTMODE_X

Обычно для получения доступа к защищенным данным в памяти eToken при работе пользователю достаточно ввести PIN-код лишь однажды, при первом обращении к таким данным. Если вы хотите, чтобы при работе с некоторыми приложениями ввод PIN-кода требовался при каждом обращении к защищенным данным, задайте эти приложения при установке из командной строки, добавив в конце команды параметр `ET_PROCLISTMODE_X="<приложения>"`, где `<приложения>` имена приложений с точками с запятой на конце, например, `ET_PROCLISTMODE_X="iexplore;outlook;"`.

ET_UI_POLICY

По умолчанию в интерфейсе рабочего стола аутентификации и других программах, использующих CryptoAPI, недоступны возможности принудительной смены PIN-кода, а также смены и разблокирования PIN-кода с участием удаленного администратора. Эти возможности определяются параметром реестра `UI_Policy`, размещающимся в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCAPI`. Параметр представляет собой трехразрядное шестнадцатеричное число, каждый из разрядов которого определяет наличие той или иной возможности в приложениях, использующих CryptoAPI:

- младший разряд отвечает за возможность разблокирования заблокированного PIN-кода с участием удаленного администратора;
- средний разряд отвечает за возможность смены PIN-кода после неверного ввода с участием удаленного администратора;
- старший разряд отвечает за принудительную смену PIN-кода.

В каждом из разрядов предусмотрены следующие цифры:

- `0` — возможность отключена;
- `1` — возможность доступна только на рабочем столе аутентификации;
- `2` — возможность доступна во всех приложениях, использующих CryptoAPI, кроме рабочего стола аутентификации;
- `3` — возможность доступна во всех приложениях, использующих CryptoAPI;

Например, если вы хотите сделать доступными на рабочем столе аутентификации (но не в других приложениях, использующих CryptoAPI) принудительную смену PIN-кода, а во всех приложениях CryptoAPI — возможность разблокирования заблокированного PIN-кода с участием удаленного администратора, то при установке eToken RTE из командной строки в конце команды добавьте параметр `ET_UI_POLICY=259` (потому что $103_{16}=259_{10}$).

NO_SMARTCARD_LOGON_PIN_DLG

При переводе компьютера в ждущий или спящий режим и последующем выходе из него по умолчанию в eToken RTE 3.66 требуется повторный ввод PIN-кода (в отличие от предыдущих версий eToken RTE). Если вы хотите, чтобы в этом случае ввод PIN-кода не требовался (как в предыдущих версиях eToken RTE), при установке из командной строки добавьте в конце команды параметр *NO_SMARTCARD_LOGON_PIN_DLG=1*.

Подробнее об этих настройках см. ниже в разделах “Утилита „eToken Properties”, “Настройка параметров eToken RTE”, “Параметры хранилища сертификатов” и “Настройки eToken RTE в системном реестре”.

Пример команды с дополнительными параметрами:

- `msiexec /qb /i "C:\Documents and Settings\Administrator\Desktop\`

- RTE_3.66.msi" ETPROPS_MODE=0 LOAD_LOCAL=1 AUTO_DUPLICATION_CHECK=1 — установка eToken RTE 3.66 в автоматическом режиме без диалоговых окон с пользовательским режимом интерфейса утилиты eToken Properties, а также включенными автоматическим копированием сертификатов из хранилища eToken в реестр и отслеживанием дубликатов закрытых ключей.

Централизованные процедуры

Использование групповых политик

В домене Windows 2000/2003 eToken RTE 3.66, eToken RTE 3.66 RUI можно устанавливать и удалять с помощью групповой политики. Подробно о настройке групповых политик Windows 2000 для централизованной установки и удаления программного обеспечения можно узнать, например, в следующих материалах:

- Microsoft Knowledge Base, Article 302430: HOW TO: Assign Software to a Specific Group By Using a Group Policy;
- Microsoft Official Curriculum, Course 2154B: Implementing and Administering Microsoft Windows 2000 Directory Services, Module 9: Using Group Policy to Maintain Software;
- Зубанов Ф., Microsoft Windows 2000. Планирование, развертывание, установка, М., Русская редакция, 2000, с. 361.

При использовании Microsoft Windows Server 2003 руководствуйтесь статьей базы знаний Microsoft:

- Microsoft Knowledge Base, Article 324750: HOW TO: Assign Software to a Specific Group By Using a Group Policy in the Windows Server 2003 Family.

Использование сценариев регистрации

В домене Windows NT/2000/2003 eToken RTE 3.66, eToken RTE 3.66 RUI можно устанавливать и удалять с помощью сценариев регистрации. Для того чтобы осуществить удаленную установку или удаление, вам потребуются файлы:

- rte_3.66.msi (для установки eToken RTE 3.66), rte_3.66.RUI.msi (для установки eToken RTE 3.66 RUI;
- logon.bat.

Файл logon.bat должен содержать строку, включающую команду установки. Например, для установки eToken RTE сохраните в файле logon.bat следующую строку:

```
if not exist %windir%\system32\etcapi.dll start rte_3.66.msi /q.
```

Подготовленные файлы поместите в соответствующий каталог, в зависимости от версии контроллера домена:

- для Windows NT — в папку %windir%\System32\Repl\Import\Scripts первичного контроллера домена;
- для Windows 2000/2003 — в папку sysvol\<имя домена>\scripts, расположенную в папке SYSVOL любого контроллера данного домена, например: C:\WINDOWS\SYSVOL\sysvol\relman.com\scripts (для контроллера домена с именем relman.com, работающего под управлением операционной системы Microsoft Windows Server 2003 с системными папками по умолчанию).

В домене Windows 2000/2003 для централизованной процедуры вместо сценариев регистрации рекомендуется использовать групповые политики.

Удаленные процедуры

В сети Windows NT/2000/XP/Server 2003/Vista программы установки/удаления eToken RTE 3.66 и eToken RTE 3.66 RUI могут быть запущены удаленно с помощью утилиты PsExec, входящей в пакет PsTools. При этом процедуры установка и удаления могут выполняться в автоматическом режиме. Пакет PsTools доступен для бесплатной загрузки на сайте Sysinternals (http://www.sysinternals.com).

Для запуска программы установки/удаления eToken RTE 3.66 (RTE 3.66 RUI) на удаленном компьютере вам потребуются:

- файл `rte_3.66.msi` (`rte_3.66.RUI.msi`);
- файл `psexec.exe`, входящий в пакет `PsTools`.

Для того чтобы установить или удалить eToken RTE 3.66 (RTE 3.66 RUI) на удаленном компьютере, выполните следующее.

1. Нажмите **Start** > **Run** (Пуск > Выполнить).
2. В окне **Run** (Запуск программы) в поле **Open** (Открыть) введите:

   `cmd`.
3. Нажмите **OK**.
4. В окне **Command Prompt** (Командная строка) для выполнения процедуры в автоматическом режиме без диалоговых окон введите:
   - для установки eToken RTE 3.66: `<psexec> \\<computer> -s msiexec /qn /i <rte_3.66.msi>`;
   - для установки eToken RTE 3.66 RUI: `<psexec> \\<computer> -s msiexec /qn /i <rte_3.66.RUI.msi>`;
   - для удаления eToken RTE 3.66 RUI: `<psexec> \\<computer> -s msiexec /qn /x <rte_3.66.RUI.msi>`;
   - для удаления eToken RTE 3.66: `<psexec> \\<computer> -s msiexec /qn /x <rte_3.66.msi>`;
   - где:
     - `<psexec>` — путь к файлу `psexec.exe`;
     - `<computer>` — имя удаленного компьютера;
     - `<rte_3.66.msi>` — сетевой путь к файлу `rte_3.66.msi` или локальный путь к этому файлу на удаленном компьютере;
     - `<rte_3.66.RUI.msi>` — сетевой путь к файлу `rte_3.66.RUI.msi` или локальный путь к этому файлу на удаленном компьютере.

Примечание:

> Подробнее о командах, которые можно вводить после `<psexec> \\<computer> -s`, см. выше в разделе “Использование командной строки”.

5. В случае успешного завершения удаленной процедуры в командной оболочке появится сообщение:

   `msiexec exited on <computer> with error code 0`,

   где `<computer>` — имя удаленного компьютера.

Первое подсоединение USB-ключа eToken к компьютеру

Важно: eToken нельзя подключать до установки eToken RTE.

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

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"

Пользовательский, основной и расширенный режимы

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

- пользовательском;
- основном (по умолчанию);
- расширенном.

В пользовательском режиме предусмотрены только следующие возможности:

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

В основном режиме вы можете:

- настраивать параметры eToken RTE (кроме настройки критериев качества PIN-кодов);
- осуществлять все операции с eToken (кроме форматирования и назначения вспомогательного ключевого контейнера).

В расширенном режиме доступны все инструменты утилиты "Свойства eToken", включая возможности настройки критериев качества PIN-кодов, форматирование eToken PRO, eToken NG-OTP и eToken NG-FLASH и назначение вспомогательного ключевого контейнера.

Переключение режимов интерфейса утилиты "Свойства eToken"

Режим интерфейса утилиты "Свойства eToken" определяется параметром реестра `Advanced`, относящимся к разделу `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties`:

Значение (шестнадцатеричное)	Режим
0	Пользовательский
1	основной
1F	расширенный

Если вы измените значение этого параметра при запущенной утилите "Свойства eToken", то новый режим вступит в силу при следующем запуске утилиты. Подробнее о настройке режимов интерфейса утилиты "Свойства eToken" в системном реестре см. в разделе "Настройки eToken RTE в системном реестре".

Запуск утилиты

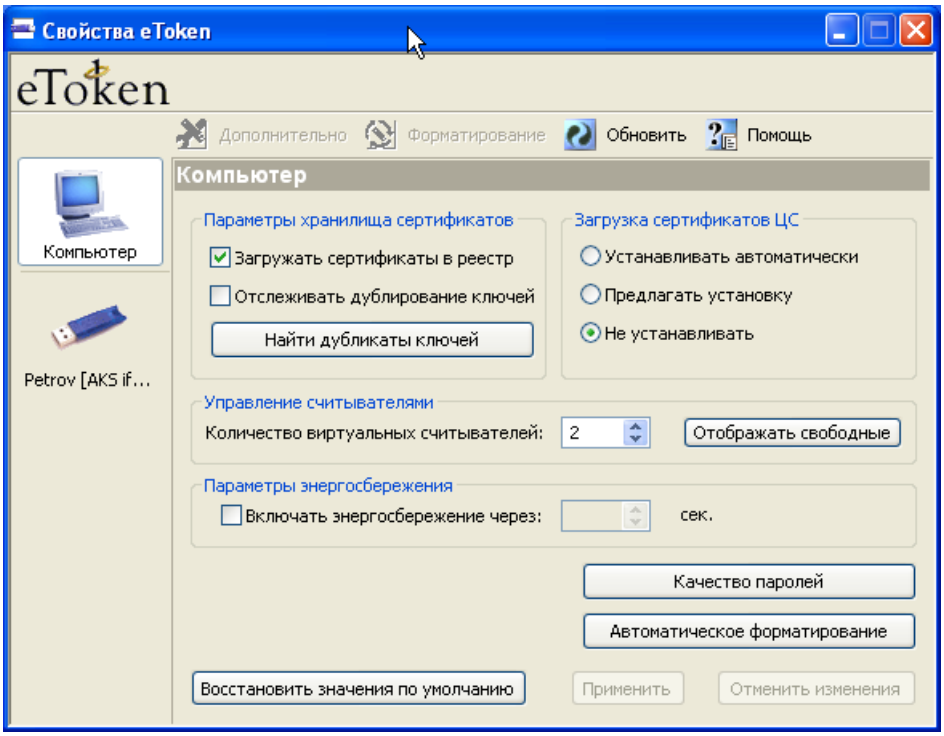
Для того чтобы запустить утилиту "Свойства eToken", щелкните **Start** > **All Programs Programs (Programs)** > **eToken** > **eToken Properties** (Пуск > Все программы (Программы) > eToken > eToken Properties).

Настройка параметров eToken RTE

Общие параметры

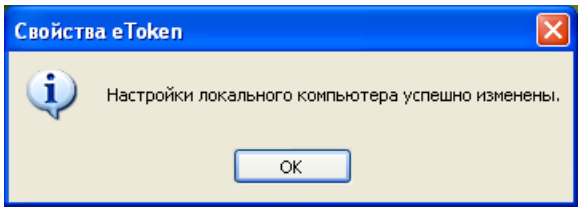
Для изменения общих параметров eToken RTE с помощью утилиты "Свойства eToken" требуются полномочия администратора.

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



После того как вы внесете 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**.

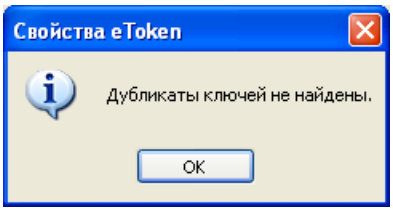
Примечание:

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

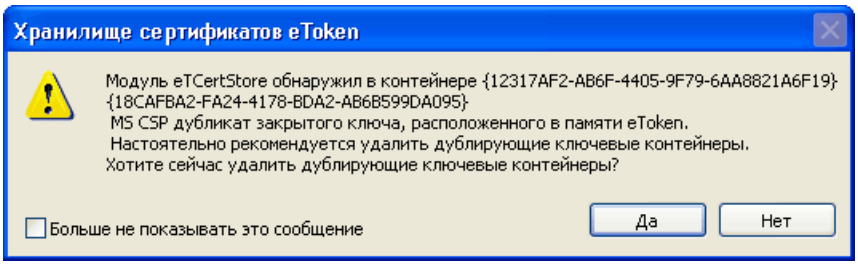
Проверка дублирования закрытых ключей

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:

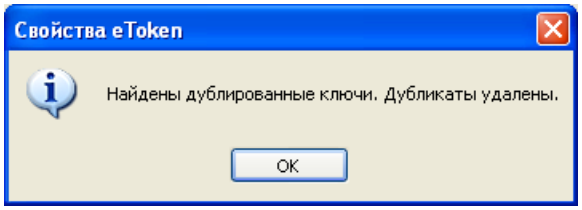
```
Дубликаты ключей не найдены.
```



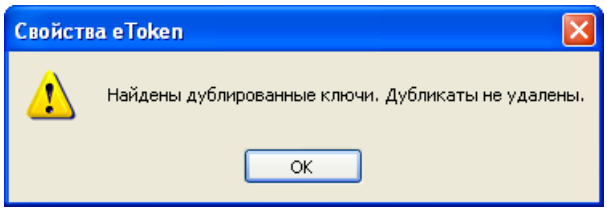
При обнаружении дублирования закрытых ключей на экране появляется диалоговое окно **Хранилище сертификатов eToken** с сообщением о том, что найдены дубликаты ключей. Для удаления дублирующего ключевого контейнера с жесткого диска компьютера нажмите **Да.**



После вывода сообщения об удалении дубликатов ключей нажмите **OK**.



Если вы не хотите устранять дублирование, то в окне обнаружения дубликатов ключей нажмите **Нет**. После появления сообщения о том, что дубликаты ключей не удалены, нажмите **OK**.



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 подсоединенных 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 настройке 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.

Критерии качества PIN-кодов

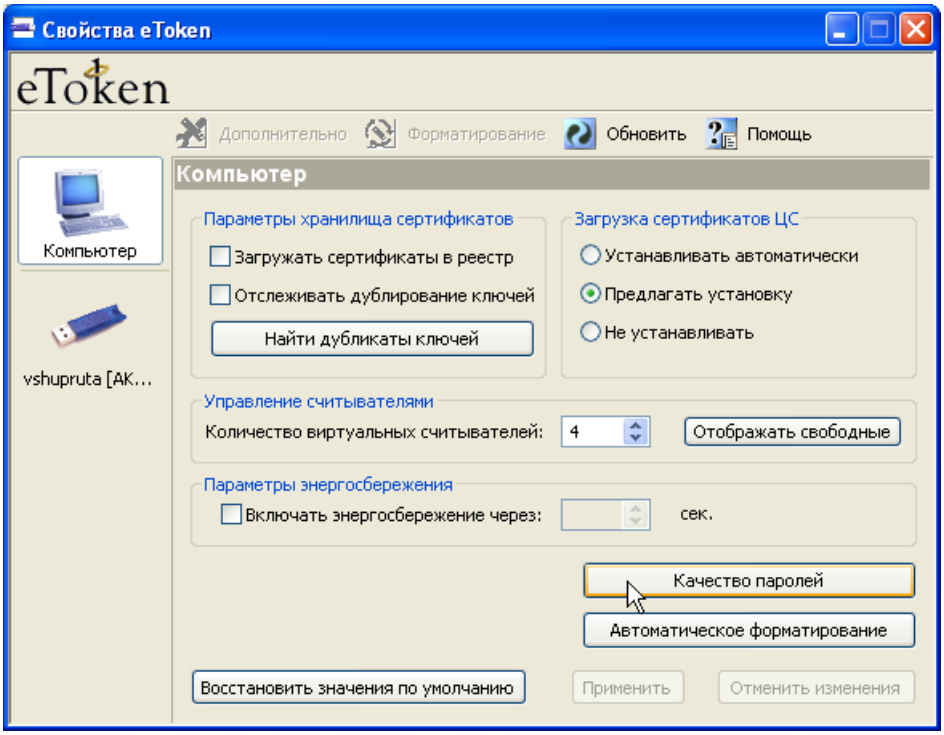
Окно настройки

Информация о корпоративных требованиях в отношении качества PIN-кодов eToken хранится в файле `etpass.ini`, расположенном в системной папке `%systemroot%\system32` (по умолчанию для Windows XP и Windows Vista — `C:\WINDOWS\System32`). Утилита "Свойства eToken" предоставляет удобный интерфейс для редактирования этого файла, а также создания, и редактирования подобных файлов, предназначенных для распространения на предприятии.

Примечание:

> Файлы `etpass.ini` можно также редактировать с помощью любого текстового редактора.

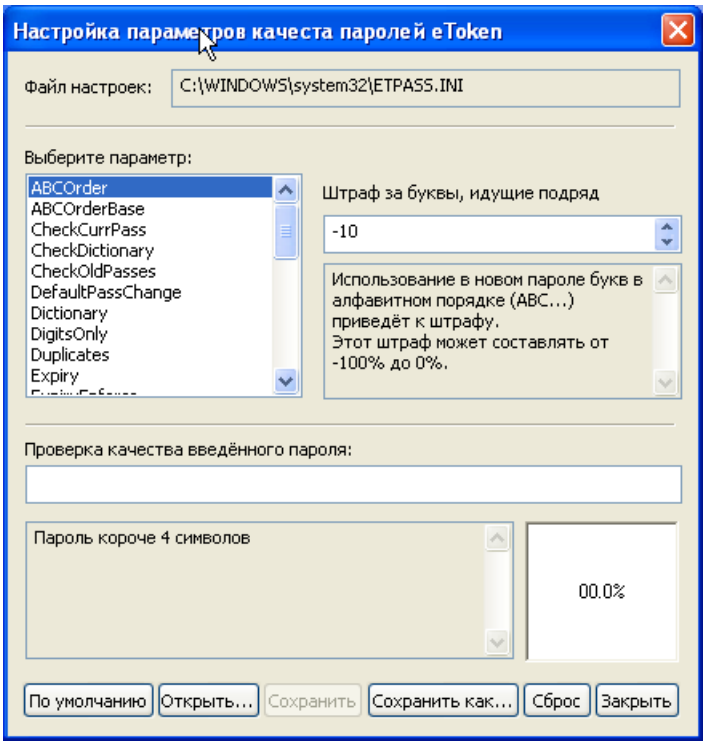
Для того чтобы открыть окно настройки качества PIN-кодов, нажмите **Качество паролей**.



Примечание:

> Наличие или отсутствие этой кнопки зависит от режима интерфейса утилиты "Свойства eToken". Если кнопка отсутствует, измените режим.

В этом окне вы можете редактировать файл `etpass.ini` и аналогичные файлы. Для того чтобы открыть файл, нажмите **Открыть** и выберите файл.



Для того чтобы изменить критерий качества, выберите его в списке **Выберите параметр** и внесите соответствующее изменение.

Если вы хотите загрузить параметры из текущего файла `etpass.ini`, нажмите **По умолчанию**.

Для того чтобы сохранить открытый и отредактированный файл, нажмите **Сохранить**.

Если вы хотите сохранить сделанные настройки в другом файле, нажмите **Сохранить как...** и выберите папку и файл.

Для того чтобы восстановить значения, используемые в eToken RTE по умолчанию, нажмите **Сброс**.

Для того чтобы проверить соответствие пароля выбранным критериям, введите пароль в строку **Проверка качества введенного пароля**. Под этой строкой выводится информация о причинах несоответствия введенного пароля выбранным критериям в процентах, а также графически и в процентах условно отображается качество введенного пароля согласно выбранным критериям.

Для того чтобы закрыть окно настройки, нажмите **Закрыть**.

Перечень критериев

В таблице приведены критерии качества PIN-кода и указаны их настраиваемые значения. В качестве значения критерия может быть использована отрицательная величина, выраженная в процентах. Такое значение называется штрафом.

Критерий	Описание	Возможные значения	Значение по умолчанию
ABCOrder	PIN-код содержит последовательность символов в алфавитном порядке	–100%—0%	–10%
ABCOrderBase	длина последовательности символов для критерия ABCOrder	2—100	3
CheckCurrPass	новый пароль равен текущему	–100%—0%	–100%
CheckDictionary	пароль из словаря	–100%—0%	–100%
CheckOldPasses	новый пароль равен одному из предыдущих	–100%—0%	0%

Критерий	Описание	Возможные значения	Значение по умолчанию
DefaultPassChange	смена пароля, принятого по умолчанию	None (смена пароля не требуется); Warning (выводится сообщение с предупреждением); Enforce (использование пароля по умолчанию невозможно)	Enforce
Dictionary	файл словаря	абсолютный путь к файлу словаря	не задано
DigitsOnly	пароль только из цифр	–100%—0%	–5%
Duplicates	наличие двух одинаковых символов	–100%—0%	–20%
Expiry	срок действия до появления предупреждения о необходимости смены (в днях)	0—3650	360
ExpiryEnforce	максимальный срок действия в днях	0—3650	0 (не установлен)
KeyboardProximity	наличие нескольких символов в том же порядке, как на клавиатуре	–100%—0%	–10%
KeyboardProximityBase	длина последовательности символов для критерия KeyboardProximity	2—100	3
LikeDictionary	пароль похож на пароль из словаря	–100%—0%	–80%
MinChangePeriod	минимальный срок действия в днях	0—3650	0 (не установлен)
MinimalLength	минимальная длина в символах	0—100	4
MinimalQuality	минимальная стойкость в процентах	0—100	30
NoDigits	отсутствие цифр	–100%—0%	–5%
NoLowerCase	отсутствие строчных букв	–100%—0%	–5%
NonPrintable	использование букв русского алфавита, непечатаемых и некоторых служебных символов	–100%—0%	–100%
NoPunctuation	отсутствие знаков препинания и служебных символов	–100%—0%	–5%
NoUpperCase	отсутствие прописных букв	–100%—0%	–5%
OptimalLength	рекомендуемая длина в символах	0—100	12
PhonesAndSerialNimbers	использование в пароле номеров телефонов, серийных номеров, и т.п.	–100%—0%	–5%
Repeating	наличие повторяющихся символов	–100%—0%	–20%
SaveOldPasses	количество использованных ранее паролей, хранящихся в памяти eToken для проверки по критерию CheckOldPasses	0—20	3
SmallPassword	длина пароля меньше WarningLength	–100%—0%	–5%
WarningLength	если длина пароля меньше WarningLength, при проверке качества пароля появляется предупреждение	0—100	6
WhiteSpaces	пароль содержит символы пробела	–100%—0%	–100%

Словарь

Для того чтобы задать список недопустимых или нежелательных паролей, создайте текстовый файл. Каждый недопустимый пароль внесите в этот файл в отдельной строке.

Пример текста файла словаря:

```
anna

annette

bill

password

william
```

Назначьте критерию Dictionary путь к созданному файлу. При распространении конфигурационного файла среди пользователей организации следует, помимо файла `etpass.ini`, распространять также и файл словаря. При этом путь к файлу словаря на каждом компьютере должен совпадать со значением критерия Dictionary.

Использование критерия OptimalLength

Критерий OptimalLength используется следующим образом. Штраф по критерию OptimalLength равен отношению (разности длины пароля и OptimalLength) и OptimalLength. Например, при OptimalLength=10 и длине пароля 6 штраф по критерию OptimalLength равен –40%. Если длина пароля больше величины OptimalLength или равна ей, критерий считается удовлетворенным.

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.
3. **Администраторский режим** — администрирование eToken.
4. **Смешанный режим** — комбинация пользовательского и администраторского режимов.

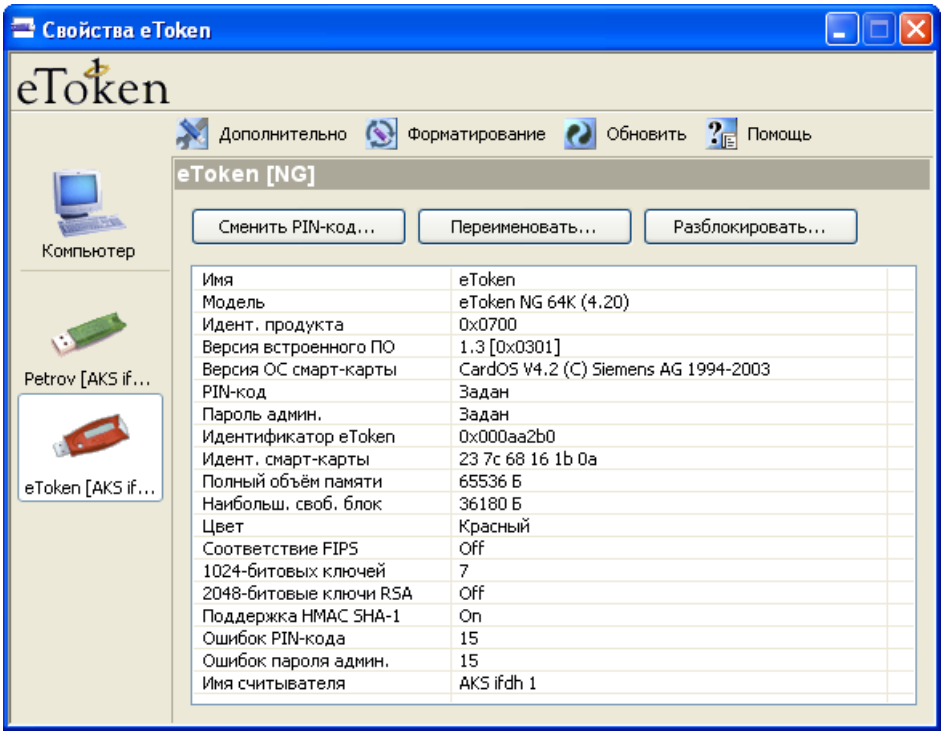
Примечания:

1. Пользовательский, администраторский и смешанный режимы работы с eToken в утилите "Свойства eToken" невозможны в пользовательском режиме интерфейса утилиты.
2. Администраторский и смешанный режимы предусмотрены только для eToken с установленным при форматировании паролем администратора.

Переключение режимов работы с eToken в утилите “Свойства eToken”

Гостевой режим

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

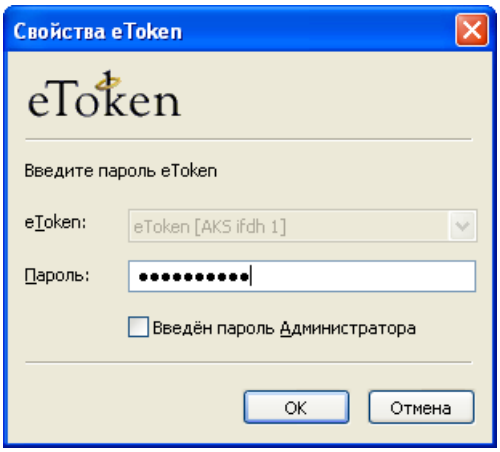


Для перехода в другие режимы вам потребуется вводить PIN-код или/и пароль администратора. После этого интерфейс гостевого режима (кроме кнопки для смены и разблокирования PIN-кода с участием удаленного администратора) будет доступен во вкладке **Подробности**.

Переход из гостевого режима в пользовательский

Для перехода из гостевого режима в пользовательский:

- нажмите Дополнительно;
- в поле **Пароль** введите PIN-код;

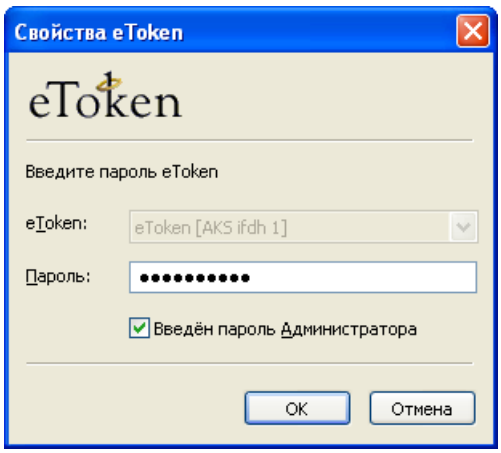


- при наличии флажка **Введен пароль Администратора** убедитесь в том, что он не установлен;
- нажмите **OK**.

Переход из гостевого режима в администраторский

Для перехода из гостевого режима в администраторский:

- нажмите Дополнительно;
- в поле **Пароль** введите пароль администратора;

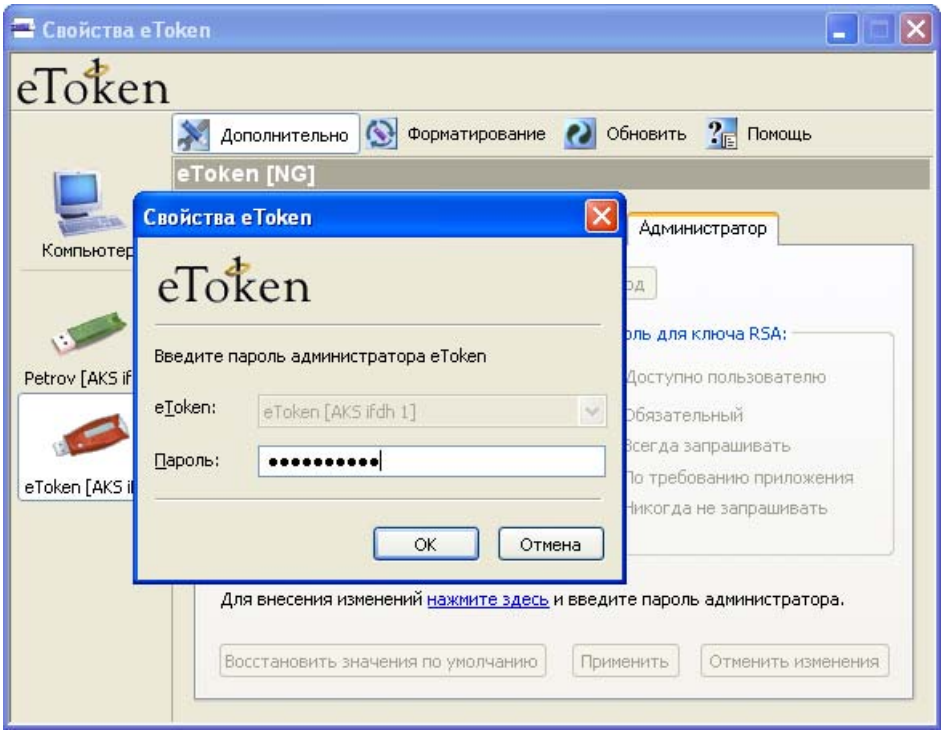


- установите флажок Введен пароль Администратора;
- нажмите **OK**.

Переход из пользовательского режима в смешанный

Для перехода из пользовательского режима в смешанный:

- откройте вкладку **Администратор**;

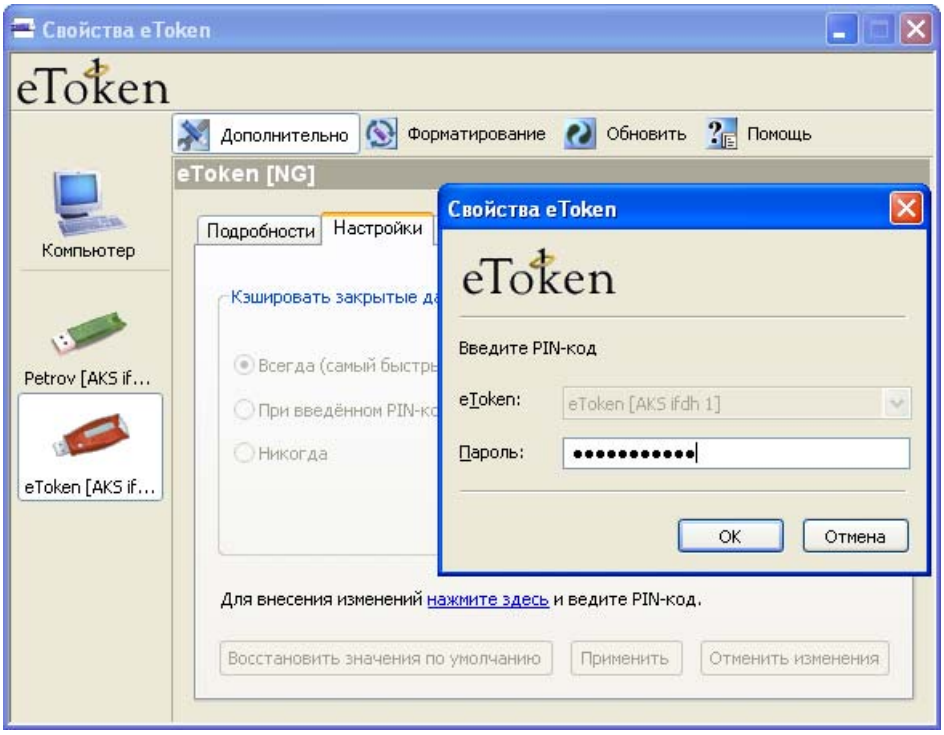


- нажмите на гиперссылку **нажмите здесь**;
- в поле **Пароль** введите пароль администратора;
- нажмите **OK**.

Переход из администраторского режима в смешанный

Для перехода из администраторского режима в смешанный:

- откройте вкладку **Настройки**;



- нажмите на гиперссылку **нажмите здесь**;
- в поле **Пароль** введите PIN-код;
- нажмите **OK**.

Доступ к общей информации

Для того чтобы просмотреть информацию о значении основных параметров одного из подключенных устройств eToken, отображенных 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;
- **Идент**. **Продукта** — идентификатор продукта;
- **Версия встроенного ПО** (только для USB-ключей) — версия встроенного программного обеспечения (firmware);
- **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 объем памяти** — общий объем памяти;
- **Наибольш. своб. блок** — объем 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.

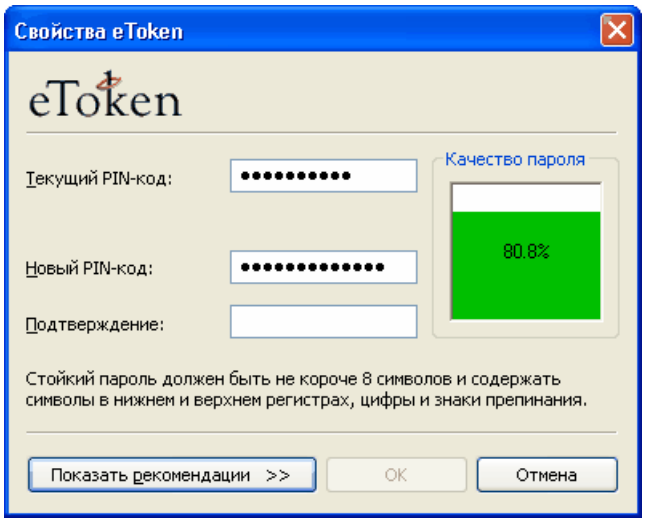
Основные операции

Смена PIN-кода

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**;



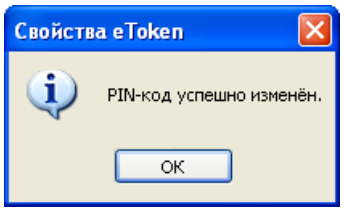
- оценка качества PIN-кода отображается в области **Качество пароля**;

Примечание:

> PIN-код должен удовлетворять требованиям качества, подробно рассмотренным в разделе "Настройка критериев качества PIN-кодов".

- для получения сведений о недостатках введенного 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 изменен.
```

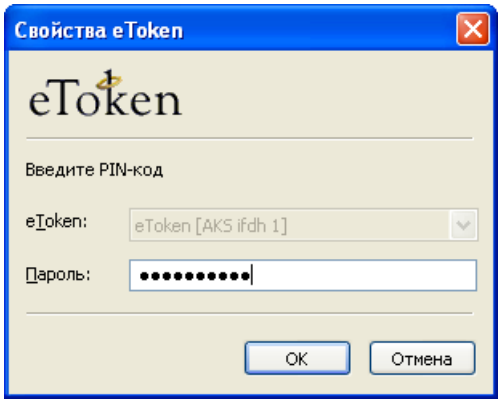


- нажмите **OK**.

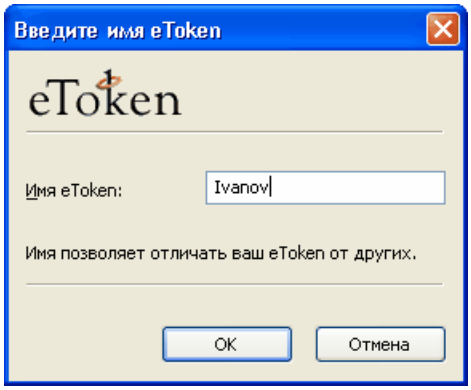
Переименование eToken

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 среда eToken RTE может кэшировать содержане 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 или смешанном — 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 трех режимов:
   - **Всегда** — режим с наибольшей производительностью и наименьшей безопасностью;
   - **При введенном PIN-коде** — кэширование только во время сеанса работы с eToken;
   - **Никогда** — кэширование отключено.

После того как вы внесете 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 защищен паролем, не зависящим от PIN-кода и пароля администратора. В eToken RTE предусмотрено четыре варианта настройки eToken PRO для таких паролей:

- **Обязательный** — пароль обязательно задается 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 создается 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 внесете изменения:

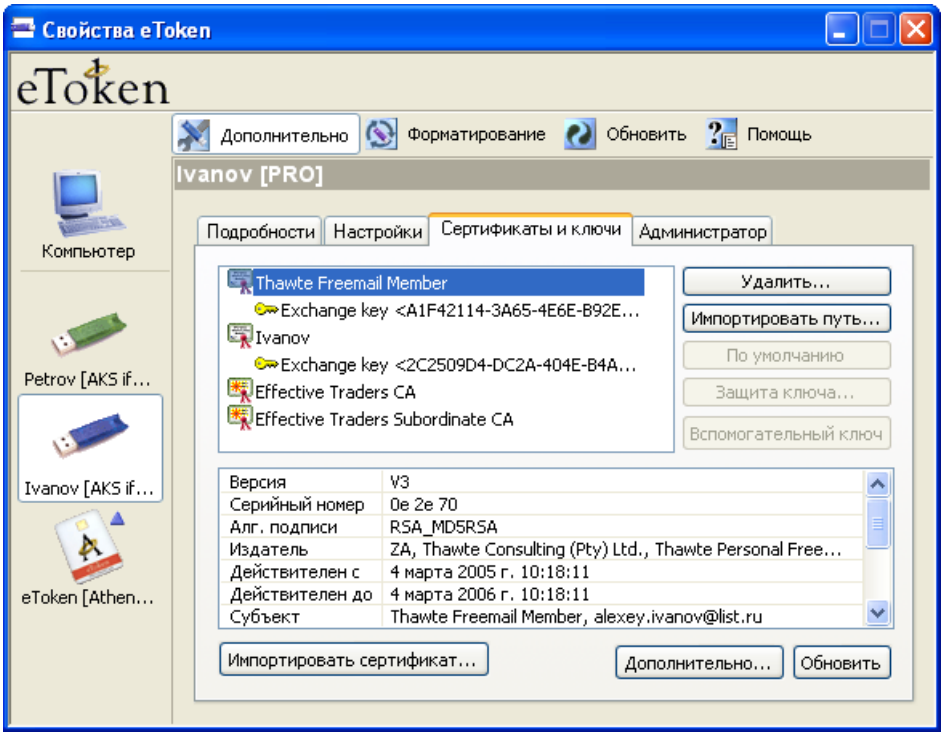
- для сохранения изменений нажмите **Применить**, а затем нажмите **OK**;
- для отмены нажмите **Отменить изменения**.

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;

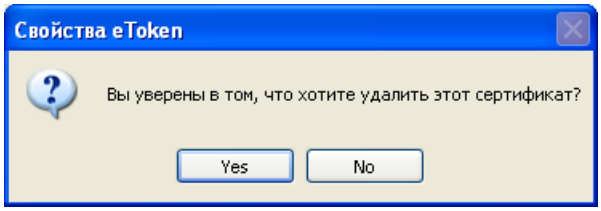


- выберите сертификат или ключевой контейнер;

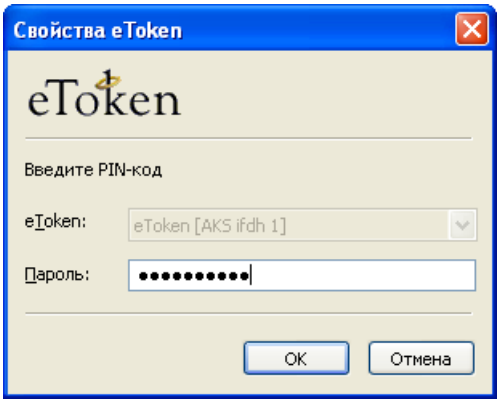
- просмотрите параметры выбранного объекта.

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

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

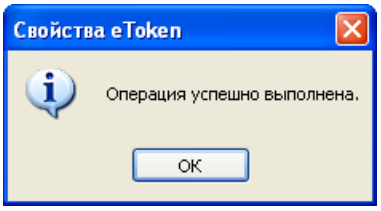


- при необходимости введите PIN-код и нажмите **OK**;



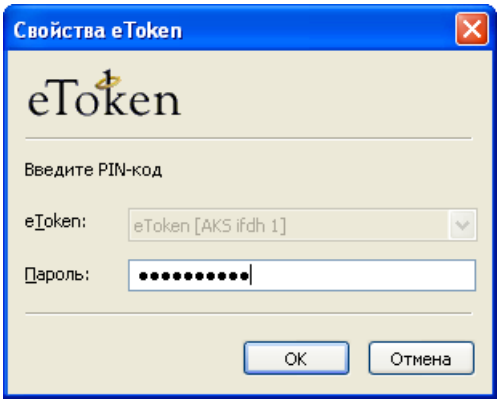
Важно: если вы удаляете ключевой контейнер, с которым связаны сертификаты, эти сертификаты также будут удалены из памяти eToken.

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

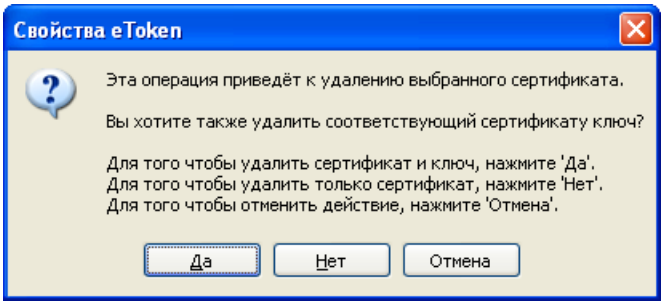


Для удаления выбранного сертификата, связанного с ключевым контейнером:

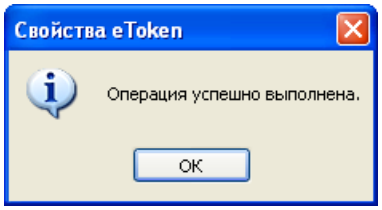
- нажмите **Удалить**;
- если утилита “Свойства eToken” работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**;



- если вы хотите, чтобы вместе с сертификатом был удален 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:

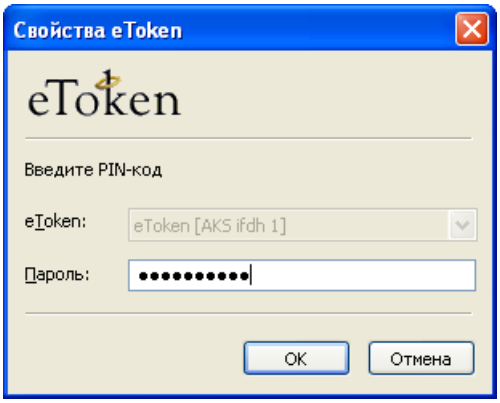


- нажмите **OK**.

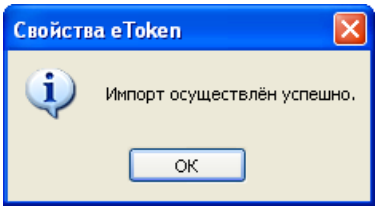
Импорт пути сертификации

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 осуществлен 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 всегда можете выбирать, какой из них использовать. Вместо этого такие приложения обращаются к сертификату, соответствующему ключевому контейнеру по умолчанию.

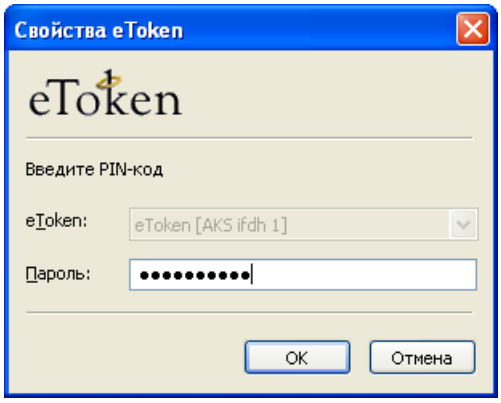
Утилита "Свойства eToken" позволяет выбирать ключевой контейнер, который будет использоваться в таких случаях по умолчанию. Если вы измените ключевой контейнер по умолчанию, прежний ключевой контейнер по умолчанию будет удален вместе с соответствующим сертификатом. Для того чтобы сделать это:

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

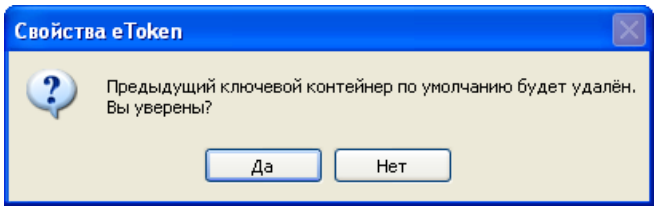
Примечания:

- 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;

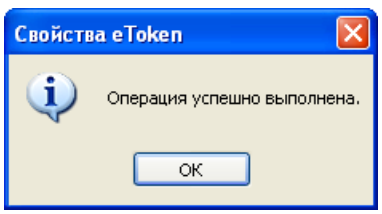
- если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**;



- 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, защищенный паролем;

Примечание:

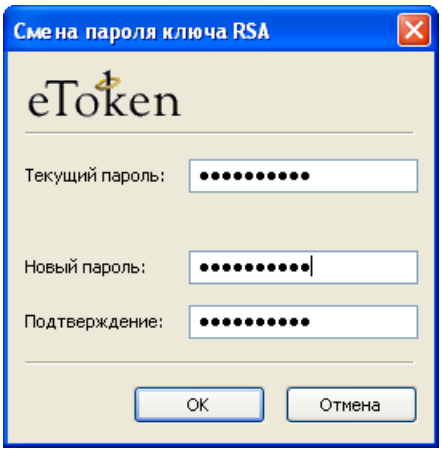
значок ключевого контейнера, защищенного паролем, содержит изображение замка ( );

- нажмите Защита ключа;

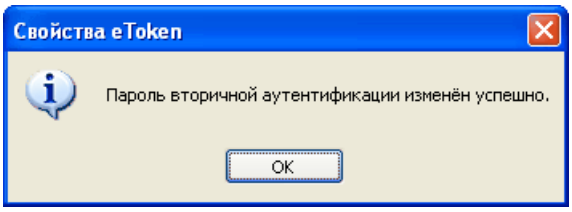
Примечание:

эта кнопка активна только при выбранном ключевом контейнере, защищенном 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**.

Назначение вспомогательного ключевого контейнера

В некоторых приложениях, использующих CryptoAPI, не указывается явно, какой из имеющихся в памяти eToken сертификат с соответствующим ключевым контейнером следует использовать при аутентификации. Примером такого приложения может служить клиент VPN, встроенный в операционную систему Microsoft Windows.

Для того чтобы явно указать ключевой контейнер и соответствующий сертификат, которые должны использоваться при работе с такими приложениями, назначьте ключевой контейнер вспомогательным.

Примечание:

Возможность назначения ключевого контейнера вспомогательным имеется не во всех режимах интерфейса утилиты "Свойства eToken". Подробнее об этом см. ранее в главе "Режимы интерфейса утилиты „Свойства eToken" настоящего раздела, а также далее в главе "Переключение режимов интерфейса утилиты „Свойства eToken" раздела "Настройки eToken RTE в системном реестре".

Для того чтобы назначить ключевой контейнер вспомогательным:

- откройте вкладку Сертификаты и ключи;
- выберите ключевой контейнер, не являющийся вспомогательным;

Примечание:

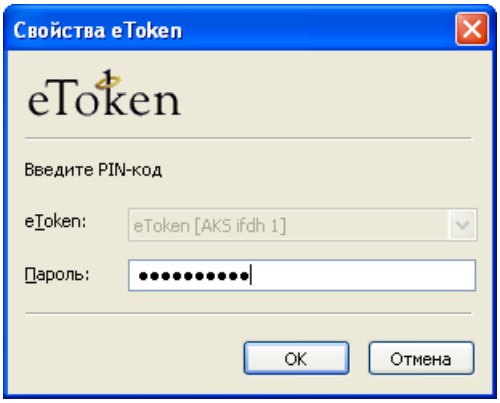
У вспомогательного ключевого контейнера параметр **Вспомог. КК** принимает значение `Yes`, а у ключевого контейнера, не являющегося вспомогательным, этот параметр принимает значение `No`.

- нажмите Вспомогательный ключ;

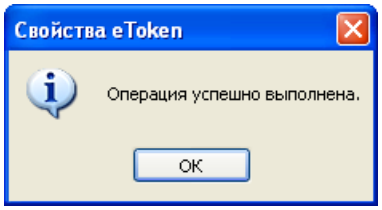
Примечание:

Кнопка **Вспомогательный ключ** активна только для контейнеров, не являющихся вспомогательными.

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



- после назначения нового вспомогательного ключевого контейнера на экране появится окно с сообщением об успешном выполнении операции;



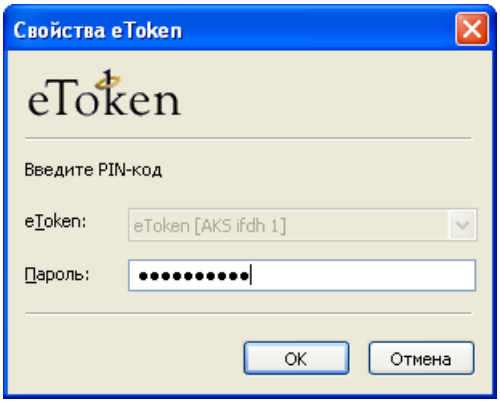
- нажмите **OK**.

Импорт сертификата с закрытым ключом

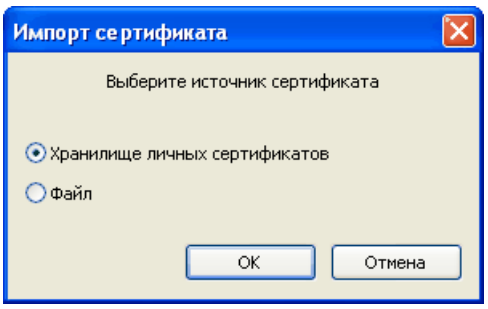
Импорт сертификата из хранилища Личные/Personal с закрытым ключом

Для того чтобы скопировать в память eToken сертификат, находящийся в хранилище Личные/Personal, вместе с соответствующим закрытым 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**.

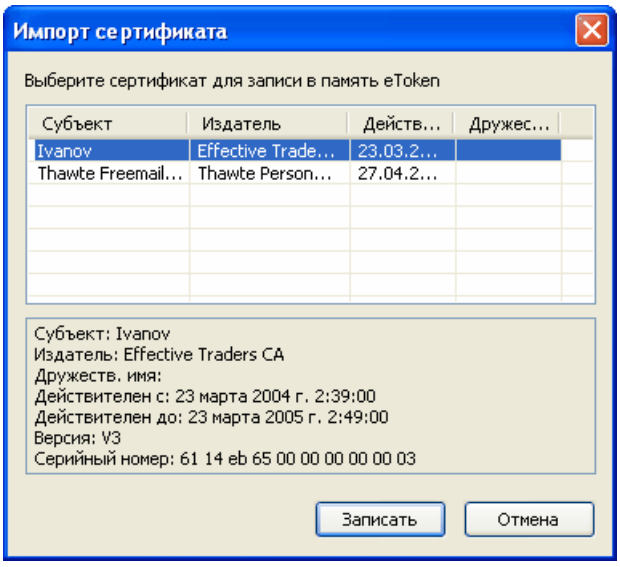


4. Выберите **Хранилище личных сертификатов** и нажмите **OK**.

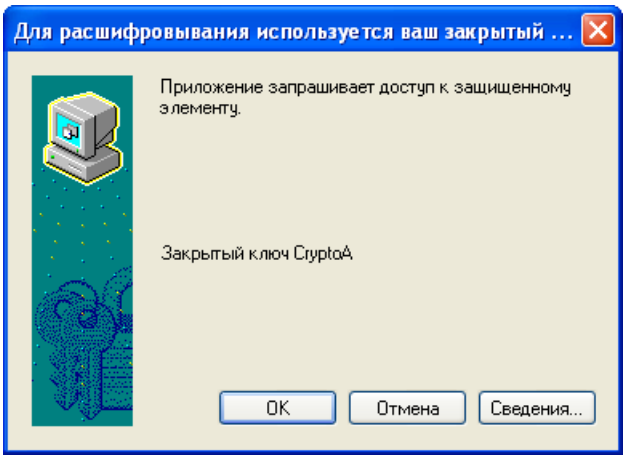


5. На экране появится список сертификатов, которые можно записать в память eToken. Он включает:
   - сертификаты, для которых соответствующие закрытые ключи уже расположены в памяти eToken;
   - сертификаты, которые могут быть импортированы с компьютера вместе с соответствующими закрытыми ключами (только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

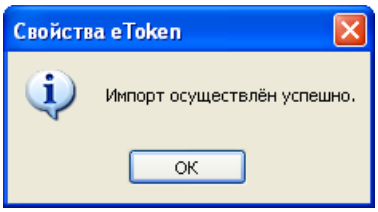
   Выберите сертификат и нажмите **Записать**.



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



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

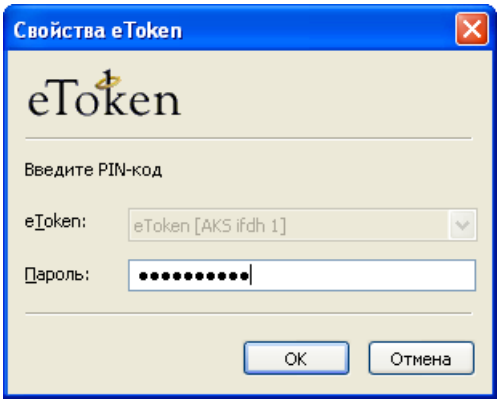


8. Нажмите **OK**.

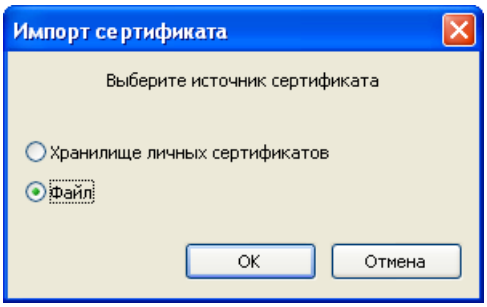
Импорт сертификата с закрытым ключом из файла

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

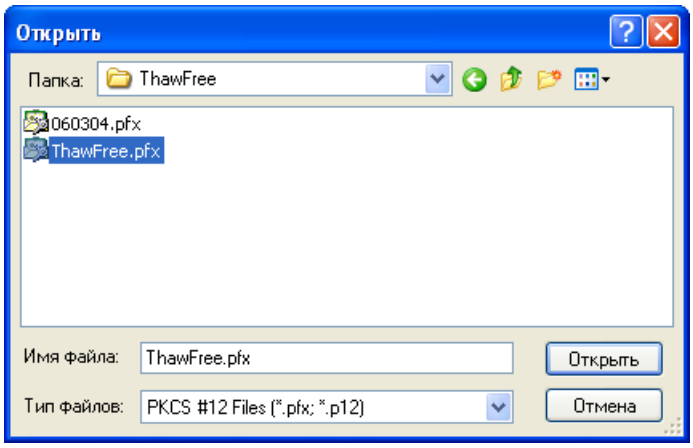
1. Откройте вкладку **Сертификаты и ключи**.
2. Нажмите **Импортировать сертификат**.
3. Если утилита "Свойства eToken" работала с eToken в администраторском режиме, то в окне **Свойства eToken** введите PIN-код и нажмите **OK**.



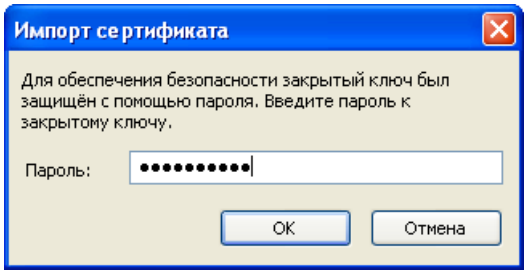
4. Выберите **Файл** и нажмите **OK**.



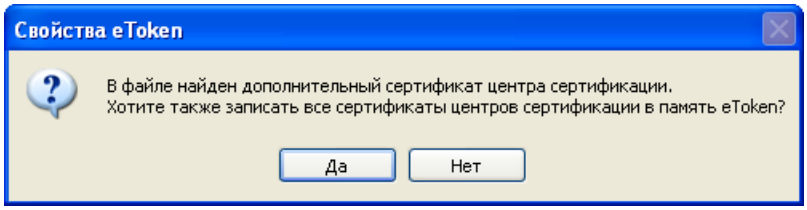
5. Укажите файл, в котором содержатся сертификат и закрытый ключ, и нажмите **Открыть**.



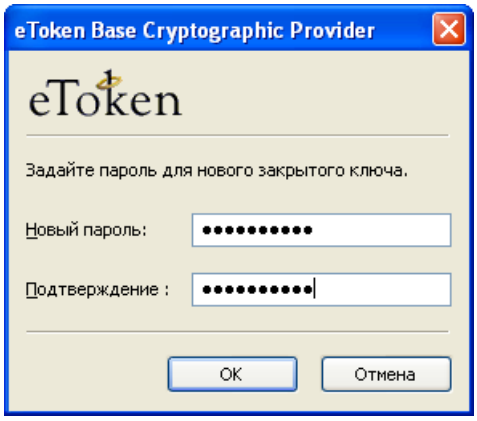
6. Для доступа к закрытому ключу, хранящемуся в файле, введите соответствующий пароль и нажмите **OK**.



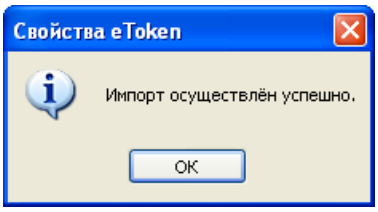
7. Если в файле содержатся сертификаты центров сертификации, на экране появится окно, информирующее вас об этом. Если вы хотите скопировать их вместе с импортируемым сертификатом в память eToken, нажмите **Да**. В противном случае нажмите **Нет**.



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.

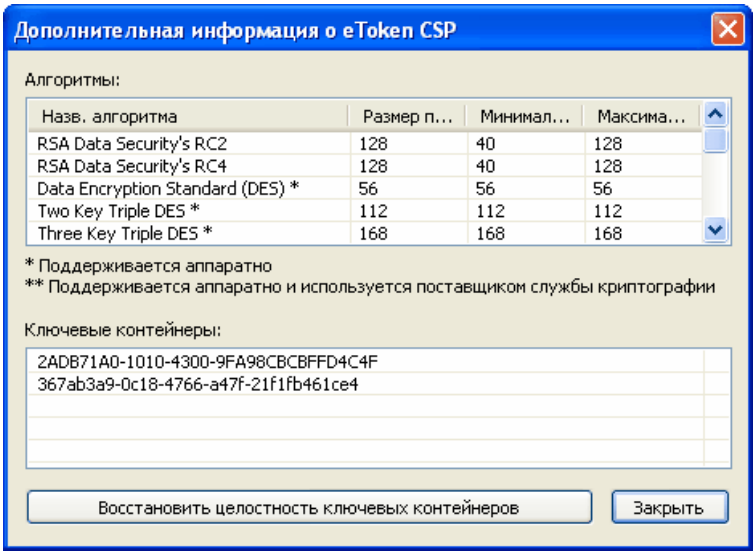


9. Если импорт будет осуществлен успешно, на экране появится окно с сообщением об этом.



Дополнительная информация о eToken CSP

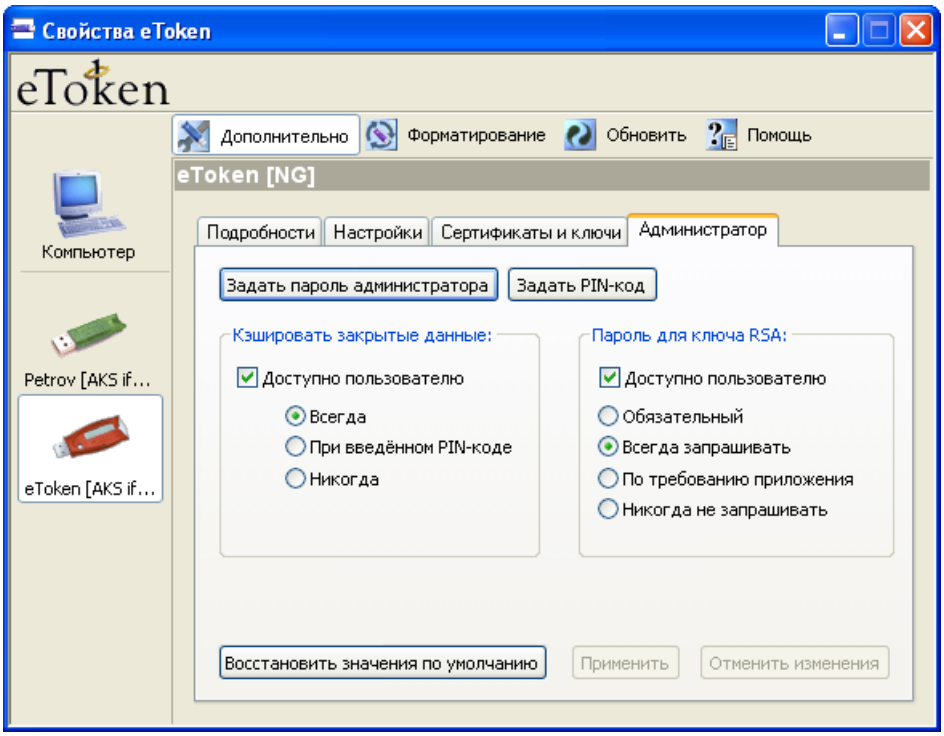
Для того чтобы получить информацию о доступных алгоритмах и ключевых контейнерах, в окне **Сертификаты и ключи** нажмите **Дополнительно**.



Администрирование eToken PRO

Локальные действия

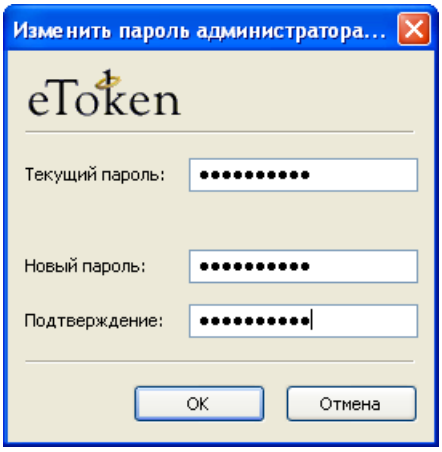
В режиме администрирования во вкладке **Администратор** вы можете изменить пароль администратора и/или неизвестный PIN-код пользователя.



Смена пароля администратора

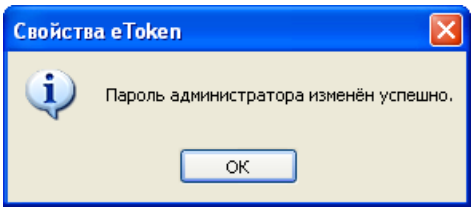
Для смены пароля администратора:

- нажмите **Задать пароль администратора**;
- в поле **Текущий пароль** введите текущий пароль администратора, а в поля **Новый пароль** и **Подтверждение** — новый пароль администратора;



- нажмите **OK**.
- при успешном изменении пароля на экране появится окно **Свойства eToken** с сообщением:

  `Пароль администратора изменен успешно.`

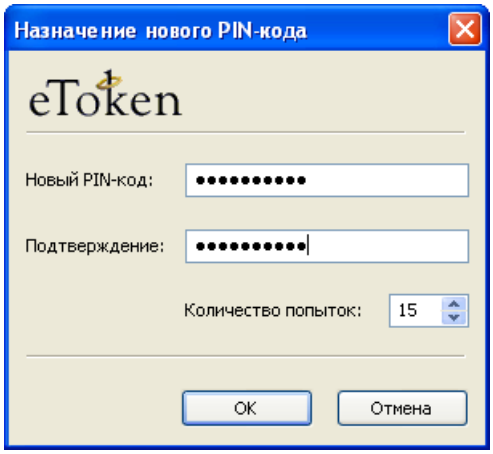


- нажмите **OK**.

Локальная смена PIN-кода администратором

Для изменения PIN-кода выполните следующую последовательность действий.

1. Нажмите **Задать PIN-код**.
2. В поля **Новый PIN-код** и **Подтверждение** введите новый PIN-код.

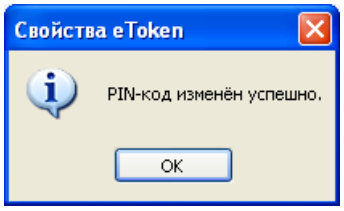


3. В поле **Количество попыток** введите предельное число попыток ввода неправильного PIN-кода подряд.

По умолчанию пользователь имеет 15 попыток. Это значит, что если он введет неверный PIN-код 15 раз подряд, то eToken заблокируется. После удачной попытки счетчик сбрасывается. Вы можете ввести значения от 1 до 15.

4. Нажмите **OK**.
5. При успешном изменении пароля на экране появится окно **Свойства eToken** с сообщением:

   `PIN-код изменен успешно.`



6. Нажмите **OK**.

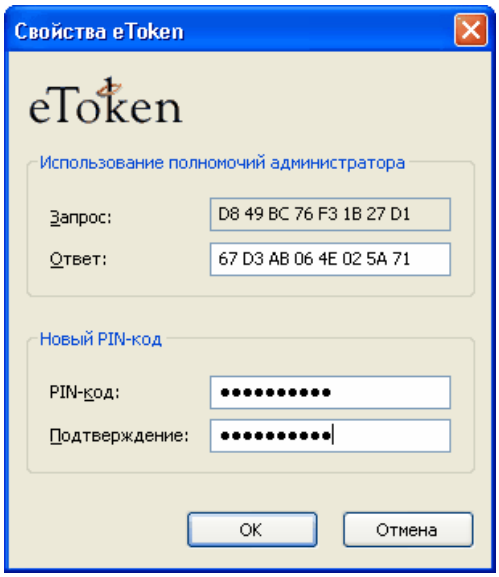
Смена и разблокирование PIN-кода с участием удаленного администратора

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 удаленно:

- пользователь обращается к администратору и сообщает ему запрос, отображаемый утилитой "Свойства eToken", а затем вводит ответ, сообщенный 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. Сообщенный администратором ответ пользователь вводит в поле **Ответ**.
4. Пользователь вводит новый PIN-код в поля **PIN-код** и **Подтверждение**.



5. Пользователь нажимает **OK**.

Примечания:

1. 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 придется повторять процедуру с начала.
2. О действиях на стороне администратора см. в документации Token Management System (TMS).

Форматирование eToken

О форматировании eToken

При форматировании eToken из памяти eToken удаляются все файлы, включая лицензии, сертификаты и ключевые контейнеры, восстанавливается PIN-код по умолчанию. При этом администраторы имеют возможность выполнить настройки eToken в соответствии с правилами, принятыми в организации, или режимом безопасности.

Форматирование eToken целесообразно, например, в случае, когда сотрудник покидает организацию. Оно позволит полностью удалить персональные данные, подготовив eToken к использованию другим сотрудником.

Разработчики программного обеспечения также могут использовать форматирование eToken при тестировании для восстановления eToken в исходное состояние и выполнения различных настроек.

Помимо PIN-кода, при форматировании задаются такие параметры, как:

- пароль администратора (необязательный параметр);
- счетчики неудачных попыток ввода PIN-кода и пароля администратора;
- ключ форматирования (для предотвращения последующего несанкционированного переформатирования);
- режим соответствия или несоответствия требованиям FIPS (только для USB-ключей eToken PRO с версиями встроенного программного обеспечения (firmware) 4.x.5.4).

Для того чтобы ключ форматирования нельзя было подобрать перебором, в eToken предусмотрено только десять попыток форматирования с указанием неверного ключа форматирования. В случае превышения этого количества попыток ключ форматирования заблокируется и отформатировать eToken будет нельзя.

Форматирование выбранного eToken

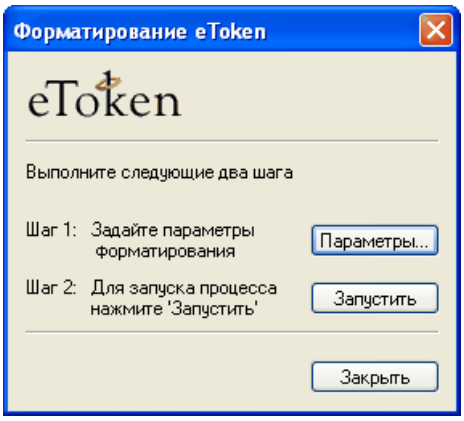
Для того чтобы отформатировать eToken:

1. Нажмите **Форматирование**.

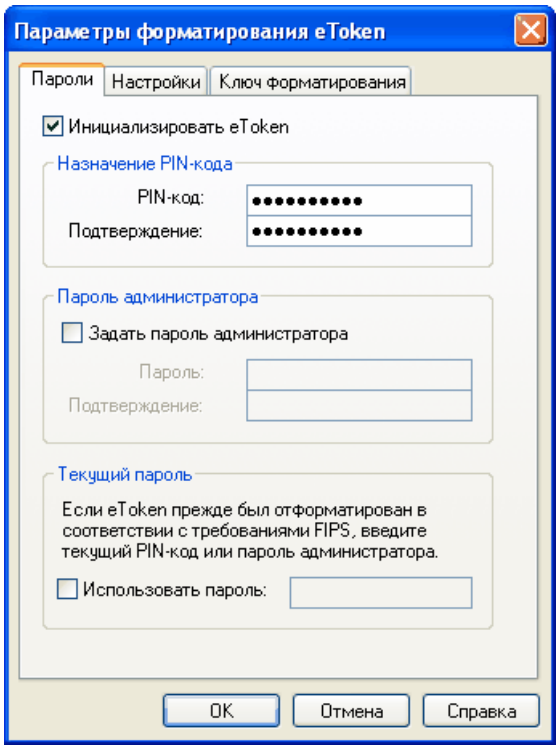
Примечание:

Кнопка **Форматирование** доступна не во всех режимах интерфейса утилиты "Свойства eToken". Если кнопка отсутствует, измените режим интерфейса утилиты (см. также раздел «Часто задаваемые вопросы»).

2. На экране появится окно **Форматирование eToken**.



3. В окне **Форматирование eToken** нажмите **Параметры...**.
4. На экране появится окно **Параметры форматирования eToken**.



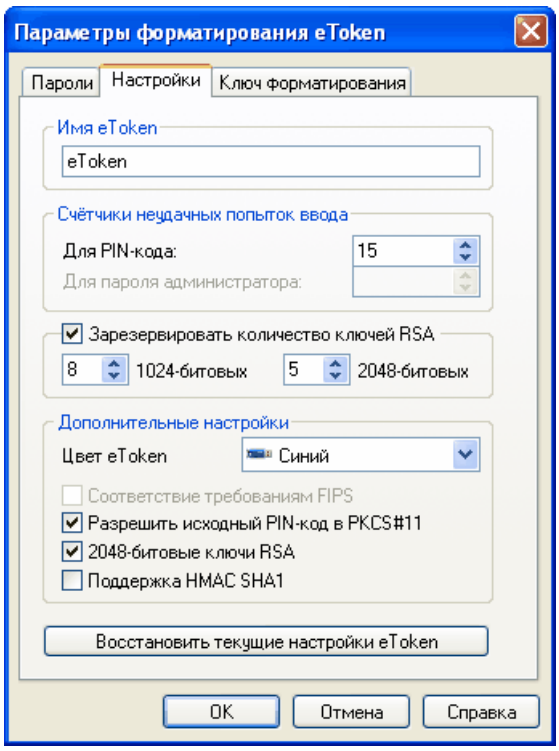
5. Убедитесь в том, что установлен флажок **Инициализировать eToken**. Этот флажок позволяет вводить данные в разделы **Назначение PIN-кода** и **Пароль администратора**.

   Если флажок **Инициализировать eToken** не установлен, eToken после форматирования окажется пустым. В нем, однако, будет задан ключ форматирования.

   Для того чтобы в результате форматирования eToken его можно было использовать с программным обеспечением, поддерживающим eToken, вы должны установить флажок **Инициализировать eToken**. Это позволит настроить все основные параметры форматирования.

6. Установите новый PIN-код в поле **PIN-код** (PIN-код пол умолчанию: 1234567890), и введите его еще раз в поле **Подтверждение**.
7. Если вы хотите задать **Пароль администратора** eToken:
   - установите флажок **Задать пароль администратора**;
   - в области **Пароль администратора** введите желаемый пароль администратора в поля **Пароль** и **Подтверждение**.

8. Если вы пытаетесь переформатировать USB-ключ eToken, соответствующий требованиям FIPS, установите флажок **Использовать пароль** и введите текущий PIN-код или пароль администратора в текстовое поле.
9. Откройте вкладку **Настройки**.



10. В поле **Имя eToken** введите строку символов. При вводе имени не рекомендуется использовать русские буквы.
11. Предусмотрено два счетчика неудачных попыток. Счетчик **Для PIN-кода** установлен всегда, а счетчик **Для пароля администратора** устанавливается только в случае, если в предыдущей вкладке задан пароль администратора. Для того чтобы установить **Счетчики неудачных попыток ввода**, введите в поле **Для PIN-кода** и в поле **Для пароля администратора** числа, лежащие в диапазоне 1—15.

    По умолчанию пользователь (администратор) имеет 15 попыток. Это значит, что если он введет неверный PIN-код (пароль администратора) 15 раз подряд, то PIN-код (пароль администратора) заблокируется.
12. Если вы хотите ограничить количество ключей RSA в памяти eToken, установите флажок **Зарезервировать количество ключей RSA** и введите значение в соответствующее поле.

    Параметр количества зарезервированных ключей RSA определяет максимальное количество 1024-битовых и 2048-битовых ключей RSA, которые можно хранить в памяти eToken. Остающаяся память eToken используется для прочих целей, но не для сохранения дополнительных 1024-битовых или 2048-битовых ключей RSA.

    Если загружен модуль поддержки 2048-битовых ключей RSA, при попытке изменения количества зарезервированных 1024-битовых ключей RSA изменяется и количество 2048-битовых ключей RSA. Аналогично, при изменении количества зарезервированных 2048-битовых ключей RSA изменяется количество 1024-битовых ключей RSA.
13. При необходимости выберите новый цвет в списке **Цвет eToken**.
14. Если вы хотите, чтобы формат eToken соответствовал стандарту FIPS, установите флажок **Соответствие требованиям FIPS**.

Примечание:

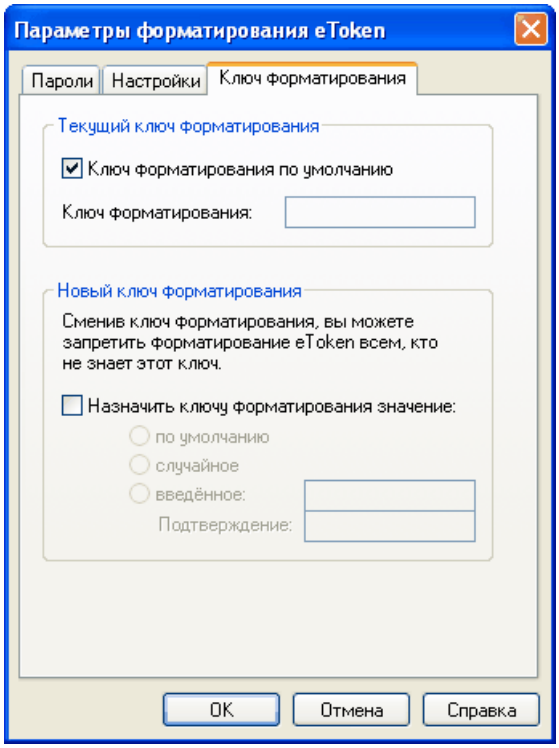
формат, соответствующий стандарту FIPS, поддерживают только USB-ключи eToken с версиями встроенного программного обеспечения (firmware) 4.x.5.4.

15. Если вы не хотите, чтобы библиотека eToken PKCS#11 сообщала об инициализации PIN-кода eToken, снимите флажок **Разрешить исходный PIN-код в PKCS#11**. В этом случае некоторые приложения, использующие API PKCS#11, не смогут работать с eToken до инициализации PIN-кода.

Примечание:

Если eToken не инициализирован в интерфейсе PKCS#11, вы можете сменить PIN-код, и это инициализирует интрефейс PKCS#11 без необходимости переформатирования eToken.

16. Установите флажок **2048-битовые ключи RSA** или **Поддержка HMAC SHA1**, если вы хотите использовать один из соответствующих модулей:
    - модуль поддержки 2048-битовых ключей RSA позволяет генерировать и использовать 2048-битовые ключи RSA;
    - модуль поддержки HMAC SHA1 позволяет использовать алгоритм HMAC SHA1 для токенов одноразовых паролей.
17. Для того чтобы автоматически использовать текущие настройки выбранного eToken, нажмите **Восстановить текущие настройки eToken**.
18. Откройте вкладку **Ключ форматирования**.



Ключ форматирования защищает процесс форматирования. Без знания этого ключа форматирование данного eToken невозможно.

19. Если ключ форматирования для устройства eToken, которое вы хотите переформатировать, отличается от ключа форматирования по умолчанию, вы должны указать текущий ключ форматирования. Для этого снимите флажок **Ключ форматирования по умолчанию** и введите текущий ключ форматирования в поле **Ключ форматирования**.
20. Изменяя ключ форматирования, вы можете контролировать и защищать процесс форматирования. Только лицо, которому известен ключ форматирования (если не используется ключ форматирования по умолчанию), имеет возможность отформатировать eToken.

    Для того чтобы задать новый ключ форматирования:
    - в разделе **Новый ключ форматирования** установите флажок **Назначить ключу форматирования значение**;

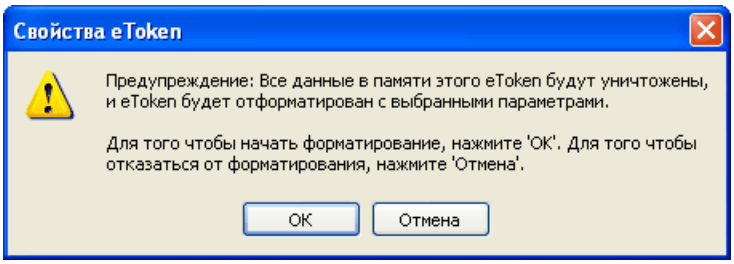
- если вы хотите, чтобы для последующего переформатирования eToken не требовалось знание ключа форматирования, выберите **по умолчанию**;
- если вы хотите сделать последующее переформатирование eToken невозможным, выберите **случайное**;
- если вы хотите задать ключ форматирования вручную:

  выберите **введенное**;

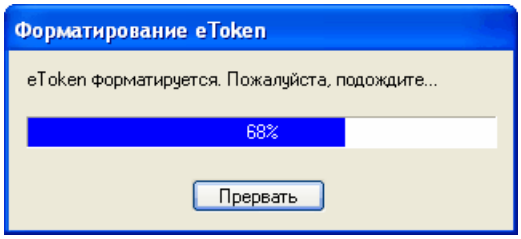
  введите новый ключ форматирования;

  введите новый ключ форматирования еще раз в поле **Подтверждение**.

21. Для того чтобы закрыть окно параметров форматирования eToken, нажмите **OK**.
22. В окне **Форматирование eToken** нажмите **Запустить**.
23. В окне подтверждения нажмите **OK**.



24. Во время форматирования на экране отображается степень завершенности процесса.

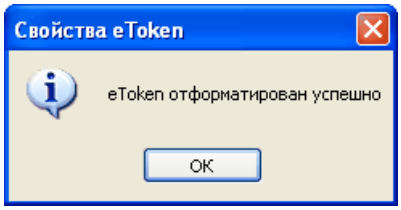


Сразу после начала форматирования и до успешного его завершения устройство eToken становится непригодным для использования. Кнопка **Прервать** позволяет вам прекратить процесс и пересмотреть настройки eToken перед повторным форматированием. В результате остановки форматирования eToken оказывается в неопределенном состоянии. Для приведения его в работоспособное состояние вы должны отформатировать его.

Примечание:

Использовать кнопку **Прервать** не рекомендуется, поскольку это может привести eToken в неисправное состояние, при котором отформатировать его будет уже нельзя.

25. По окончании форматирования на экране появляется подтверждающее сообщение.



26. Нажмите **OK**.

Автоматическое форматирование

Форматировать устройства eToken можно не только по одному, но и партиями. Для этого в утилите "Свойства eToken" предусмотрен режим, при котором все подключаемые к компьютеру eToken автоматически форматируются с одинаковыми параметрами. Количество eToken, которые могут быть одновременно отформатированы, зависит от установленного количества виртуальных считывателей.

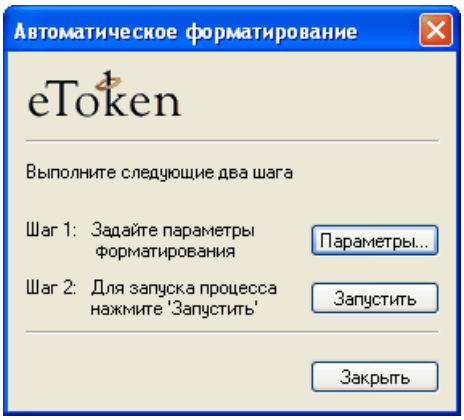
Для того чтобы автоматически форматировать каждый подключаемый eToken, выполните следующее:

1. В окне **Свойства eToken** нажмите **Компьютер**.
2. Подключите один или несколько eToken для форматирования.
3. Нажмите **Автоматическое форматирование**.

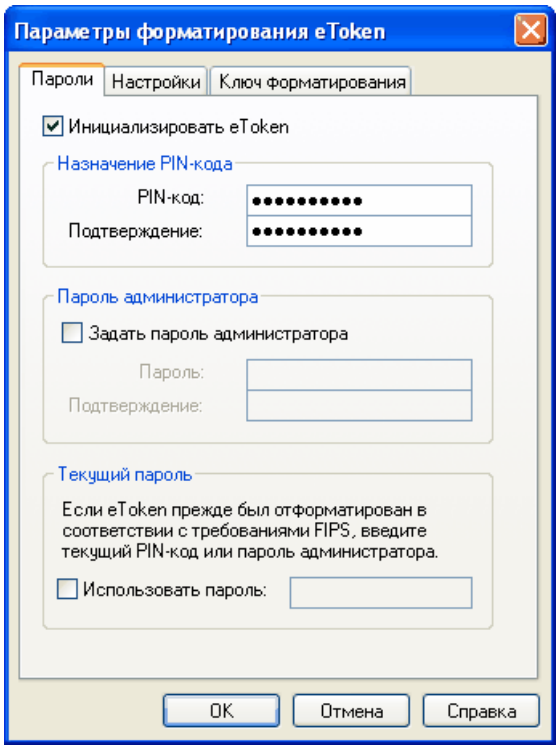
Примечание:

Кнопка **Автоматическое форматирование** доступна не во всех режимах интерфейса утилиты "Свойства eToken". Если кнопка отсутствует, измените режим интерфейса утилиты.

4. На экране появится окно **Автоматическое форматирование**.



5. В окне **Автоматическое форматирование** нажмите **Параметры...**.
6. На экране появится окно Параметры форматирования eToken.

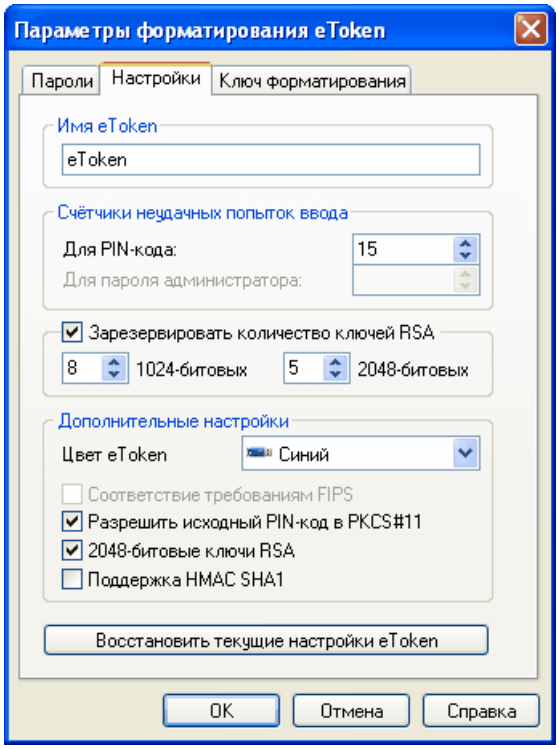


7. Убедитесь в том, что установлен флажок **Инициализировать eToken**. Этот флажок позволяет вводить данные в разделы **Назначение PIN-кода** и **Пароль администратора**.

   Если флажок **Инициализировать eToken** не установлен, eToken после форматирования окажутся пустыми. В них, однако, будет задан ключ форматирования.

Для того чтобы в результате форматирования eToken их можно было использовать с программным обеспечением, поддерживающим eToken, вы должны установить флажок **Инициализировать eToken**. Это позволит настроить все основные параметры форматирования.

8. Установите новый PIN-код в поле **PIN-код** (PIN-код пол умолчанию: 1234567890), и введите его еще раз в поле **Подтверждение**.
9. Если вы хотите задать **Пароль администратора** eToken:
   - установите флажок **Задать пароль администратора**;
   - в области **Пароль администратора** введите желаемый пароль администратора в поля **Пароль** и **Подтверждение**.
10. Если вы пытаетесь переформатировать USB-ключи eToken, соответствующие требованиям FIPS, установите флажок **Использовать пароль** и введите текущий PIN-код или пароль администратора в текстовое поле.
11. Откройте вкладку **Настройки**.



12. В поле **Имя eToken** введите строку символов. При вводе имени не рекомендуется использовать русские буквы.
13. Предусмотрено два счетчика неудачных попыток. Счетчик **Для PIN-кода** установлен всегда, а счетчик **Для пароля администратора** устанавливается только в случае, если в предыдущей вкладке задан пароль администратора. Для того чтобы установить **Счетчики неудачных попыток ввода**, введите в поле **Для PIN-кода** и в поле **Для пароля администратора** числа, лежащие в диапазоне 1—15.

    По умолчанию пользователь (администратор) имеет 15 попыток. Это значит, что если он введет неверный PIN-код (пароль администратора) 15 раз подряд, то PIN-код (пароль администратора) заблокируется.
14. Если вы хотите, чтобы формат eToken соответствовал стандарту FIPS, установите флажок **Соответствие требованиям FIPS**.

Примечание:

формат, соответствующий стандарту FIPS, поддерживают только USB-ключи eToken PRO с версиями встроенного программного обеспечения (firmware) 4.x.5.4.

15. Если вы хотите ограничить количество ключей RSA в памяти eToken, установите флажок **Зарезервировать количество ключей RSA** и введите значение в соответствующее поле.

    Параметр количества зарезервированных ключей RSA определяет максимальное количество 1024-битовых и 2048-битовых ключей RSA, которые можно хранить в памяти eToken. Остающаяся память eToken используется для прочих целей, но не для сохранения дополнительных 1024-битовых или 2048-битовых ключей RSA.

    Если загружен модуль поддержки 2048-битовых ключей RSA, зарезервированное количество таких ключей зависит от зарезервированного количества 1024-битовых ключей RSA.

16. При необходимости выберите новый цвет в списке **Цвет eToken**.

17. Если вы не хотите, чтобы библиотека eToken PKCS#11 сообщала об инициализации PIN-кода eToken, снимите флажок **Разрешить исходный PIN-код в PKCS#11**. В этом случае некоторые приложения, использующие API PKCS#11, не смогут работать с eToken до инициализации PIN-кода.

Примечание:

Если eToken не инициализирован в интерфейсе PKCS#11, вы можете сменить PIN-код, и это инициализирует интерфейс PKCS#11 без необходимости переформатирования eToken.

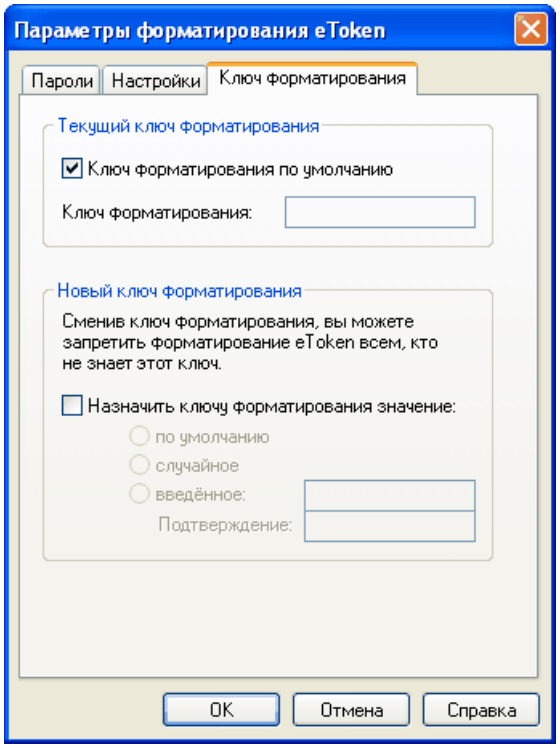
18. Установите флажок **2048-битовые ключи RSA** или **Поддержка HMAC SHA1**, если вы хотите использовать один из соответствующих модулей:

    - модуль поддержки 2048-битовых ключей RSA позволяет генерировать и использовать 2048-битовые ключи RSA;
    - модуль поддержки HMAC SHA1 позволяет использовать алгоритм HMAC SHA1 для токенов одноразовых паролей.

Примечание:

Эти модули доступны только для eToken PRO с операционной системой Siemens CardOS V4.20, eToken NG-OTP и eToken NG-FLASH.

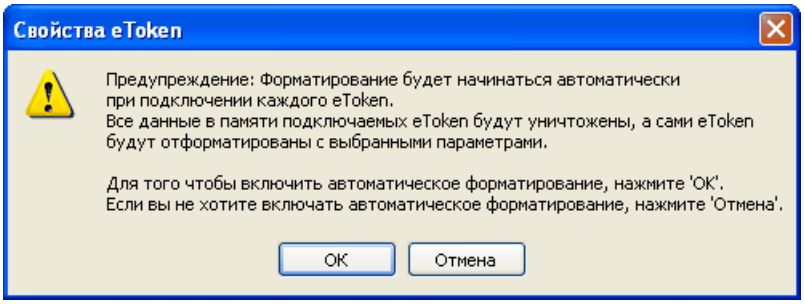
19. Откройте вкладку **Ключ форматирования**.



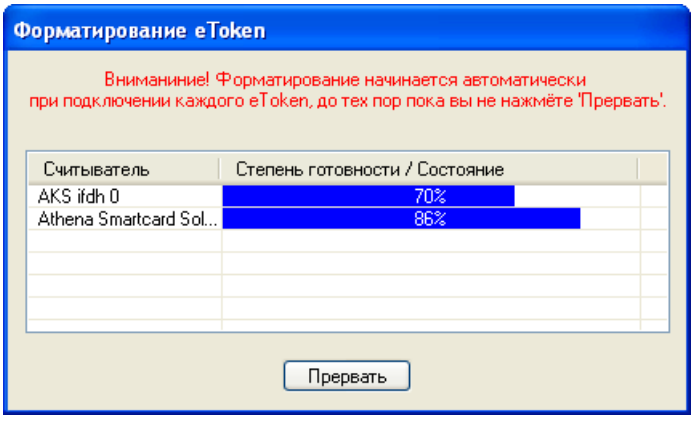
20. Все устройства eToken, которые вы хотите автоматически отформатировать, должны иметь общий ключ форматирования. Если этот ключ форматирования отличается от ключа форматирования по умолчанию, вы должны указать текущий ключ форматирования. Для этого снимите флажок **Ключ форматирования по умолчанию** и введите текущий ключ форматирования в поле **Ключ форматирования**.
21. Изменяя ключ форматирования, вы можете контролировать и защищать процесс форматирования. Только лицо, которому известен ключ форматирования (если не используется ключ форматирования по умолчанию), имеет возможность отформатировать eToken.

    Для того чтобы задать новый ключ форматирования:

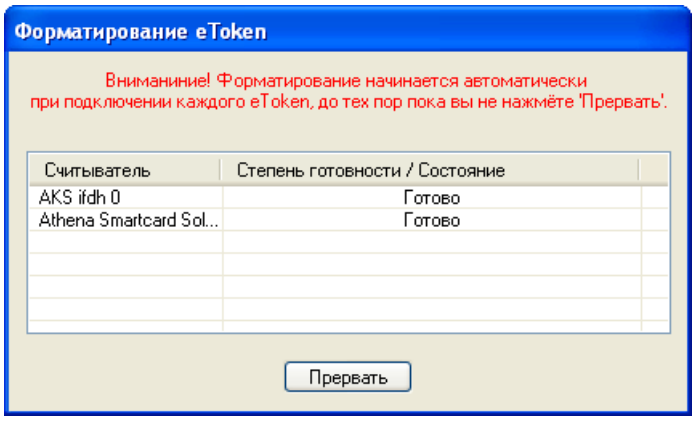
    - в разделе **Новый ключ форматирования** установите флажок **Назначить ключу форматирования значение**;
    - если вы хотите, чтобы для последующего переформатирования eToken не требовалось знание ключа форматирования, выберите **по умолчанию**;
    - если вы хотите сделать последующее переформатирование eToken невозможным, выберите **случайное**;
    - если вы хотите задать ключ форматирования вручную:
        - выберите **введенное**;
        - введите новый ключ форматирования;
        - введите новый ключ форматирования еще раз в поле **Подтверждение**.
22. Для того чтобы закрыть окно параметров форматирования eToken, нажмите **OK**.
23. В окне **Автоматическое форматирование** нажмите **Запустить**.
24. В окне подтверждения нажмите **OK**.



25. Для каждого устройства eToken на экране отображается степень завершения форматирования.



26. Когда форматирование подключенного eToken завершено, поле **Степень готовности / Состояние** принимает значение **Готово**.



27. Для того чтобы завершить процесс автоматического форматирования, нажмите **Прервать**.

Завершение работы утилиты “Свойства eToken”

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

Утилита eToken NG-FLASH Partition

Общие сведения

Утилита eToken NG-FLASH Partition не входит в пакет eToken RTE 3.66 и поставляется отдельно. Она служит для настройки параметров флеш-памяти eToken NG-FLASH. Память может быть разбита на один или два раздела следующих типов – раздел, доступный пользователю только в режиме чтения (Read Only Memory – **ROM**) и раздел, доступный для записи пользовательских файлов (**Mass Storage**).

Установка и удаление

Утилита eToken NG-FLASH Partition не требует отдельного процесса установки и может быть запущена из любой папки на жестком диске или на сменном носителе. Для запуска утилиты следует использовать файл NgFlashPartition.exe. При копировании утилиты следует также копировать файл CDFS.dll, поставляемый с ней в комплекте. Для удаления достаточно удалить выше указанные файлы; утилита не создает записей в системном реестре и/или дополнительных временных файлов.

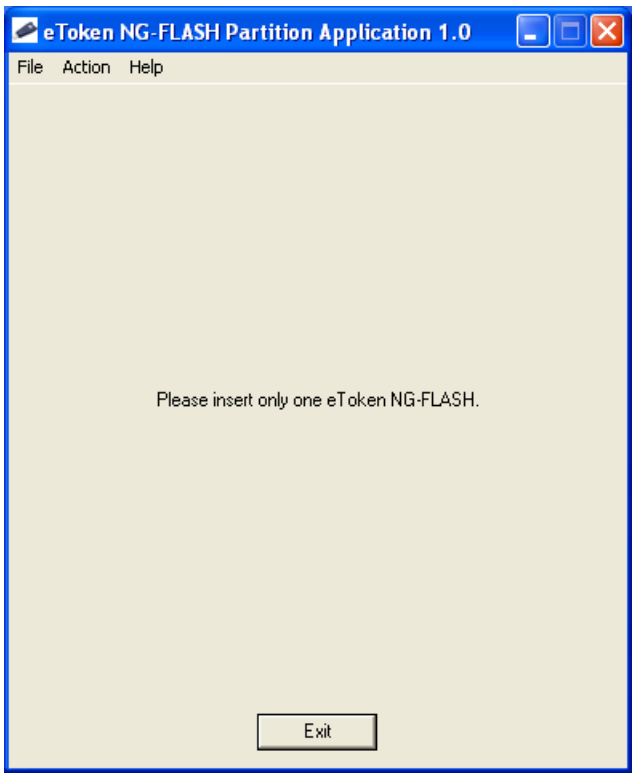
Использование утилиты

Запуск утилиты

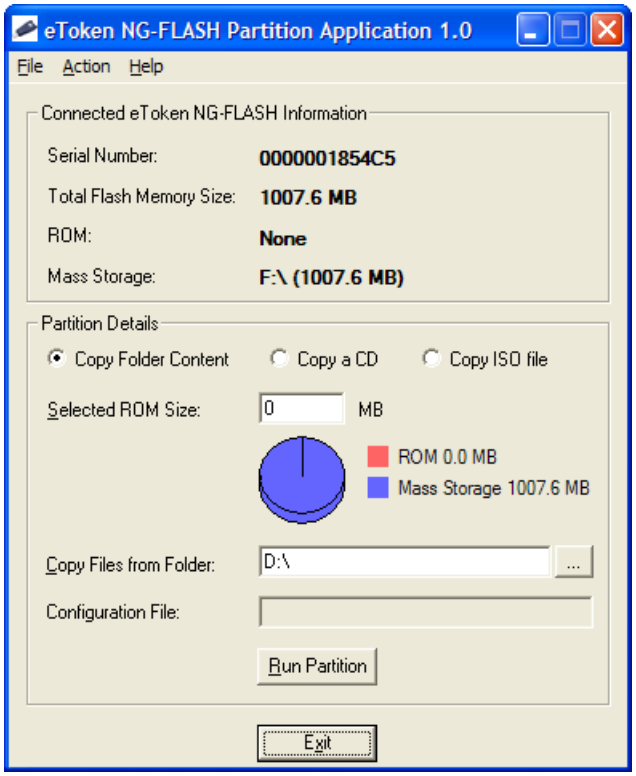
Для запуска утилиты необходимы полномочия локального администратора.

Для того чтобы запустить eToken NG-FLASH Partition Application 1.0, запустите файл NgFlashPartition.exe.

Данная утилита работает только с подключенными eToken NG-FLASH. Если в системе нет подключенных устройств eToken NG-FLASH или подключено несколько устройств eToken NG-FLASH, то будет выдано сообщение `Please insert only one eToken NG-FLASH` (`Пожалуйста, вставьте только один eToken NG-FLASH`):



При подключении eToken NG-FLASH окно утилиты принимает следующий вид:



Задание параметров распределения памяти eToken NG-FLASH

Окно приложения разделено на два раздела:

1. **Connected eToken NG-FLASH Information** (Информация о подключенном eToken NG-FLASH).

   Этот раздел служит для отображения информации о подключенном устройстве:

   - **Serial Number** — серийный номер;
   - **Total Flash Memory Size** — общее количество флеш-памяти;
   - **ROM** — количество памяти только для чтения;
   - **Mass Storage —** количество доступной флеш-памяти для чтения и записи.

2. **Partition Details** (Информация о разбиении памяти устройства на секции **ROM** и **Mass Storage**).

   Этот раздел используется для выбора режима работы утилиты:

   - **Copy Folder Content –** в **ROM** секцию копируются все файлы из выбранной папки и вложенных папок;
   - **Copy a CD** – в **ROM** секцию копируются все файлы с выбранного компакт-диска, а также данные о структуре диска, включая загрузочный код (если он есть на диске) – таким образом можно будет использовать eToken NG-FLASH в качестве загрузочного устройства;
   - **Copy ISO file** – режим аналогичен режиму **Copy a CD**, за исключением того, что данные считываются не с физического диска, а из его образа, сохраненного в виде ISO файла.

   Также раздел используется для ввода следующих параметров:

   - **Selected ROM Size** — размер памяти только для чтения (эмуляция устройства CD-ROM), этот параметр не доступен в режимах **Copy a CD** и **Copy ISO file**, т.к. при этом размер памяти определяется размером данных на CD или в ISO файле;
   - **Copy Files from Folder** — папка, из которой будут скопированы файлы в секцию **ROM**, при работе режиме **Copy Folder Content**; привод CD/DVD, в который вставлен диск с данными, при работе в режиме **Copy a CD**; путь к ISO файлу с образом диска при работе в режиме **Copy ISO file**.

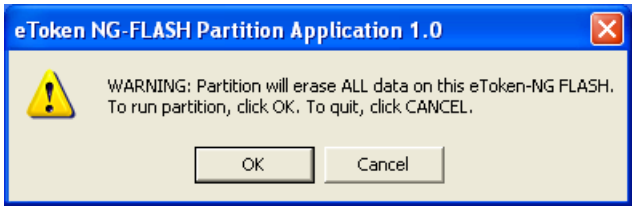
При задании параметров разбиения можно увидеть на рисунке, какая часть памяти устройства отведена для **ROM** (красный цвет), а какая — для **Mass Storage** (синий цвет).

Примечания:

1. Необходимо учитывать, что существуют различия между используемыми файловыми системами для организации ROM-секции (CDFS) и организации секции Mass Storage (FAT32, NTFS). Соответственно, при задании размера ROM-секции в режиме Copy Folder Content необходимо оставлять некоторый запас свободного места.
2. При задании папки-контейнера для ROM-секции нельзя использовать корневые каталоги дисков, а также одиночные файлы.
3. Размер загрузочного диска или ISO образа загрузочного диска должен быть больше 8 Мб.
4. При длительных операциях (например, запись информации в флеш-память) не показывается никаких визуальных индикаторов прогресса; таким образом, у пользователя может возникнуть впечатление, что программа «зависла». Это нормальное поведение программы, и в этом случае следует дождаться корректного завершения операции. Об активности процесса записи можно судить по мигающему индикатору на eToken NG-FLASH.

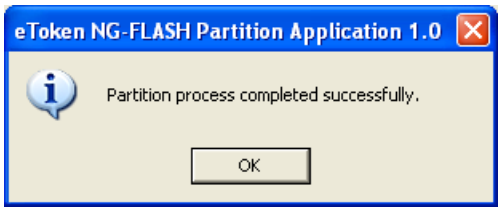
Для разбиения памяти eToken NG-FLASH в соответствии с введенными параметрами:

1. Нажмите **Run Partition** (Запуск распределения памяти).
2. В окне подтверждения нажмите **OK**.



Внимание: помните, что при выполнении данной операции все данные (как в ROM-области, так и в области Mass Storage) будут удалены.

3. По завершении операции в окне программы появится сообщение `Please reinsert the eToken NG-FLASH` (`Пожалуйста, извлеките eToken NG-FLASH и подключите его снова`).
4. Извлеките eToken NG-FLASH и подключите его снова.
5. При появлении окна с сообщением `Partition process completed successfully (Распределение памяти успешно завершено)` нажмите **OK**.



6. С помощью раздела **Connected eToken NG-FLASH Information** (Информация о подключенном eToken NG-FLASH) проконтролируйте правильность распределения флеш-памяти eToken.

Использование файла конфигурации

При необходимости введенные параметры распределения памяти можно сохранить в файле конфигурации. Сделать это можно с помощью пунктов меню **File > Save** (Файл > Сохранить) или **File > Save as...** (Файл > Сохранить как…).

Чтобы применить параметры разбиения, сохраненные в файле конфигурации, воспользуйтесь пунктом меню **File > Open** (Файл > Открыть).

Примечание:

имя файла конфигурации должно содержать только ASCI-символы.

Завершение работы

Для завершения работы утилиты нажмите **Exit** (Выход) в окне программы или выберите в меню пункт **File > Exit** (Файл > Выход).

Настройки eToken RTE в системном реестре

Полномочия

Некоторыми параметрами eToken RTE можно управлять с помощью системного реестра. Полномочия пользователей по управлению этими параметрами определяются администратором стандартными средствами.

Переключение режимов интерфейса утилиты “Свойства eToken”

Режим интерфейса утилиты определяется параметром реестра `Advanced`, относящимся к разделу `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties`. Этот параметр представляет собой пять битовых флагов:

- младший бит отвечает за возможность настраивать параметры eToken RTE (кроме критериев качества PIN-кодов) и осуществлять все операции с eToken (кроме форматирования): `1` — инструменты активны, `0` — инструменты недоступны;
- второй бит справа отвечает за возможность форматирования выбранного eToken (`1` — форматирование возможно, `0` — форматирование невозможно);
- третий бит справа отвечает за возможность автоматического форматирования (`1` — автоматическое форматирование возможно, `0` — автоматическое форматирование невозможно);

- четвертый бит справа отвечает за инструмент настройки качества PIN-кода (`1` — инструмент доступен, `0` — инструмент недоступен);
- старший бит отвечает за возможность назначения вспомогательного ключевого контейнера (`1` — соответствующий инструмент доступен, `0` — инструмент недоступен).

Особенности интерфейса утилиты таковы, что возможности, управляемые старшими битами, доступны только при ненулевом младшем бите. С учетом этого, вы можете вычислить необходимое значение параметра `Advanced`, сложив числа, соответствующие нужным битовым флагам:

- младшему биту соответствует число 1 ($1 \bullet 2^0$);
- второму биту — число 2 ($1 \bullet 2^1$);
- третьему биту — число 4 ($1 \bullet 2^2$);
- четвертому биту — число 8 ($1 \bullet 2^3$)
- старшему биту — число 16 ($1 \bullet 2^4$).

Например, если необходимо разрешить только автоматическое форматирование и инструмент настройки качества PIN-кода, назначьте параметру `Advanced` значение $1+4+8 = 13_{10}=D_{16}$. Ниже перечислены все возможные значения параметра `Advanced` и указаны соответствующие режимы интерфейса.

Значение (шестнадцатеричное)	Значение (двоичное)	Режим
0	00000	пользовательский
1	00001	основной
3	00011	основной с возможностью форматирования выбранного eToken
5	00101	основной с возможностью автоматического форматирования
7	00111	основной со всеми возможностями форматирования
9	01001	основной с инструментом настройки качества PIN-кодов
B	01011	основной с возможностью форматирования выбранного eToken и инструментом настройки качества PIN-кодов
D	01101	основной с возможностью автоматического форматирования и инструментом настройки качества PIN-кодов
F	01111	расширенный без возможности назначения вспомогательного ключевого контейнера
11	10001	основной с возможностью назначения вспомогательного ключевого контейнера
13	10011	основной с возможностями форматирования выбранного eToken и назначения вспомогательного ключевого контейнера

Значение (шестнадцатеричное)	Значение (двоичное)	Режим
15	10101	основной с возможностями автоматического форматирования и назначения вспомогательного ключевого контейнера
17	10111	расширенный без инструмента настройки качества PIN-кода
19	11001	основной с инструментом настройки качества PIN-кодов и возможностью назначения вспомогательного ключевого контейнера
1B	11011	расширенный без возможности автоматического форматирования
1D	11101	расширенный без возможности форматирования выбранного eToken
1F	11111	расширенный

Если вы измените значение этого параметра при запущенной утилите "Свойства eToken", то новый режим вступит в силу при следующем запуске утилиты.

Дополнительный логотип

При желании в окно "Свойства eToken" можно добавить логотип или любое другое изображение со следующими размерами:

- высота — не более 33 пикселов;
- ширина — не более 512 пикселов.

Соответствующий графический файл должен иметь формат BMP.

Для того чтобы добавить или заменить изображение в окне "Свойства eToken", создайте или отредактируйте строковый параметр `Logo` в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties`, указав в качестве значения параметра путь к графическому файлу.

Если вы хотите использовать в изображении прозрачный цвет, изменяющийся вместе с системными настройками цвета рельефных объектов, то в качестве такового можно назначить цвет правой верхней точки. Для этого создайте или отредактируйте в том же разделе реестра параметр `LogoTransparency` типа DWORD, назначив ему ненулевое значение.

Загрузка сертификатов в реестр

Автоматическое копирование сертификатов из хранилища eToken в реестр можно настроить в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore`. Использование этого режима контролируется параметром `LoadLocal`. Если этот параметр принимает значение `1`, то при подключении eToken к компьютеру все сертификаты автоматически копируются из хранилища eToken в реестр. Если этот параметр принимает значение `0`, автоматического копирования сертификатов в реестр не происходит.

Режим автоматического копирования сертификатов из хранилища eToken в реестр не распространяется на процессы, имена которых хранятся в качестве значения параметра `ProcLoadLocalIgnore` в том же разделе реестра. При этом в конце каждого имени процесса должна стоять точка с запятой. Пример: `eTProps;AppViewer;capiView;ckView;eTCertConv;`. При необходимости отредактируйте значение этого параметра.

Отслеживание дублирования закрытых ключей

Автоматическое отслеживание в системе дубликатов закрытых ключей, имеющихся в памяти eToken, можно настроить в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore`. Использование этого режима контролируется параметром `DuplicateKeyTest`. Если этот параметр принимает значение `0`, то отслеживание дубликатов закрытых ключей не производится, а если он принимает ненулевое значение, то производится.

Доступ к закрытым данным

Обычно для получения доступа к защищенным данным в памяти eToken при работе пользователю достаточно ввести PIN-код лишь однажды, при первом обращении к таким данным. Данный режим можно изменить таким образом, что для некоторых приложений ввод PIN-кода будет требоваться при каждом обращении к таким данным. Настройки режима доступа находятся в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCAPI`. Настройки режима контролируются параметром `ProcListModeX`. Например, значением этого параметра могут быть имена приложений, для которых будет требоваться ввод PIN-кода при каждом обращении к закрытым данным `ProcListModeX = "iexplore;outlook;"`.

Понятные имена сертификатов

eToken RTE 3.66 при отсутствии автоматического копирования сертификатов из хранилища eToken в реестр поддерживает два формата понятных имен сертификатов, хранящихся в памяти eToken:

- формат 1: имя считывателя, наименование субъекта (например, `AKS ifdh 0::Thawte Freemail Member`);
- формат 2: наименование субъекта, назначение, имя считывателя (например, `Thawte Freemail Member: Проверка подлинности сертификата, Проверка подлинности клиента, Подписывание кода, Защищенная электронная почта, установка штампа времени... reader::AKS ifdh 0`).

Номер используемого формата является значением параметра `FriendlyNameVer` в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore`.

Примечание:

Для использования понятных имен сертификатов автоматическое копирование сертификатов в реестр должно быть отключено.

Копирование сертификатов центров сертификации

Если в памяти eToken, подключенного к компьютеру, содержится сертификат центра сертификации, отсутствующий в реестре, по умолчанию на экране появляется диалоговое окно, предлагающее пользователю скопировать этот сертификат в реестр. Появление этого окна можно отключить, изменив параметр `CACertMode` в разделе реестра `HKEY_CURRENT_USER\SOFTWARE\Aladdin\eToken\eTCertStore`. Всего предусмотрено три значения этого параметра:

- `0` — появляется диалоговое окно (значение по умолчанию);
- `1` — сертификаты центров сертификации копируются в реестр автоматически;
- `2` — сертификаты центров сертификации в реестр не копируются.

Для вновь создаваемых учетных записей пользователей параметр `CACertMode` принимает значение одноименного параметра из раздела реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCertStore`.

Кэширование PIN-кода

Обычно для получения доступа к защищенным данным в памяти eToken при работе пользователю достаточно ввести PIN-код лишь однажды, при первом обращении к таким данным. Если вы хотите, чтобы при работе с некоторыми приложениями ввод PIN-кода требовался при каждом обращении к защищенным данным, задайте эти приложения в параметре `ProcListModeX`, в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCAPI`. Имена приложений задаются с точками с запятой на конце, например, `iexplore;outlook;`.

Политика интерфейса пользователя в приложениях CryptoAPI

По умолчанию в интерфейсе рабочего стола аутентификации и других программах, использующих CryptoAPI, недоступны возможности принудительной смены PIN-кода, а также смены и разблокирования PIN-кода с участием удаленного администратора. Эти возможности определяются параметром реестра `UI_Policy`, размещающимся в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTCAPI`. Параметр представляет собой трехразрядное шестнадцатеричное число, каждый из разрядов которого определяет наличие той или иной возможности в приложениях, использующих CryptoAPI:

- младший разряд отвечает за возможность разблокирования заблокированного PIN-кода с участием удаленного администратора;
- средний разряд отвечает за возможность смены PIN-кода после неверного ввода с участием удаленного администратора;
- старший разряд отвечает за принудительную смену PIN-кода.

Принудительная смена PIN-кода может потребоваться в случаях:

- использования PIN-кода по умолчанию (`1234567890`);
- истечения срока действия PIN-кода.

В каждом из разрядов предусмотрены следующие цифры:

- `0` — возможность отключена;
- `1` — возможность доступна только на рабочем столе аутентификации;
- `2` — возможность доступна во всех приложениях, использующих CryptoAPI, кроме рабочего стола аутентификации;
- `3` — возможность доступна во всех приложениях, использующих CryptoAPI.

Например, если вы хотите сделать доступными во всех приложениях, использующих CryptoAPI, принудительную смену PIN-кода, а во всех приложениях CryptoAPI, кроме рабочего стола аутентификации — возможность после неудачных попыток ввода незаблокированного PIN-кода менять его с помощью удаленного администратора, назначьте параметру `UI_Policy` шестнадцатеричное значение 320.

Возврат из ждущего или спящего режима

При переводе компьютера в ждущий или спящий режим и последующем выходе из него по умолчанию в eToken RTE 3.66 требуется повторный ввод PIN-кода (в отличие от предыдущих версий eToken RTE до версии 3.60). Если вы хотите, чтобы в этом случае ввод PIN-кода не требовался (как в предыдущих версиях eToken RTE до версии 3.60), измените параметр `NoSmartcardLogonPinDlg` в разделе реестра `HKEY_LOCAL_MACHINE \SOFTWARE\Aladdin\eToken\Core`.

Если этот параметр отсутствует или имеет нулевое значение, то при возврате из ждущего и спящего режима требуется повторный ввод PIN-кода. Если же параметр принимает ненулевое значение, то при возврате из ждущего или спящего режима повторно вводить PIN-код не нужно.

eToken на предприятии

Выбор инструментов управления инфраструктурой eToken

Инфраструктура систем безопасности на базе eToken требует эффективного управления. Для этой цели необходимо принять ряд организационных мер, составить регламенты, отвечающие нуждам организации, и обеспечить их неукоснительное выполнение.

При большом количестве сотрудников, использующих eToken, управление инфраструктурой eToken лучше всего осуществлять мощными средствами автоматизации. Основным инструментом управления, рекомендуемым для крупных предприятий, является Token Management System (TMS).

Вместе с тем, если в вашей организации используются лишь несколько устройств eToken и вы не планируете существенного роста их количества, использование столь мощной системы, каковой является TMS, нецелесообразно с экономической, технической и организационной точек зрения.

Как правило, TMS рекомендуется внедрять, если в организации используется не менее 50—100 устройств eToken.

Весь процесс работы с TMS подробно освещен в документе “eToken TMS: Справочное руководство”. Если в вашей организации не используется TMS, руководствуйтесь рекомендациями, приведенными в пункте “eToken на малом предприятии” настоящего раздела.

eToken на малом предприятии

Администратор eToken

Для эффективного управления инфраструктурой систем безопасности на базе eToken в штате компании должен быть сотрудник, наделенный полномочиями администратора eToken. В сферу ответственности администратора eToken могут входить:

- учет USB-ключей и смарт-карт;
- настройка критериев качества PIN-кодов eToken в соответствии с корпоративными правилами;
- распространение файлов `etpass.ini`, содержащих критерии качества PIN-кодов и словарей нежелательных/неприемлемых паролей;
- форматирование eToken;
- смена PIN-кодов eToken с использованием паролей администратора;
- настройка кэширования содержания закрытой области памяти eToken;
- выбор настроек паролей закрытых ключей;
- безопасное хранение PIN-кодов, паролей администратора и ключей форматирования.

Правила распределения доступа к eToken

Правила задания PIN-кодов, паролей администратора eToken и ключей форматирования следует составлять в соответствии с общекорпоративными принципами и критериями задания паролей и распределения полномочий.

Правила форматирования

Форматирование eToken уничтожает все хранящиеся в памяти eToken данные. Поэтому прибегать к форматированию следует только в случае, когда использовать eToken без переформатирования невозможно.

Используя ключ форматирования, можно разрешать, нормировать или запрещать переформатирование.

Форматирование разрешено

С помощью средств, доступных администратору, форматирование eToken может быть разрешено любому пользователю. При такой схеме форматирование должно регулироваться нормативными

документами. Для того чтобы разрешить форматирование eToken любому пользователю, следует задать ключ форматирования по умолчанию.

Форматирование нормировано

Для защиты eToken от несанкционированного форматирования следует при форматировании назначить новый ключ форматирования. Переформатировать eToken, не зная ключа форматирования, будет невозможно.

Форматирование запрещено

Если при форматировании eToken задать случайный ключ форматирования, последующее переформатирование будет невозможно.

Правила задания пароля администратора

При форматировании eToken можно либо задавать, либо не задавать пароль администратора. В случае если пароль администратора задан, администратор eToken может менять PIN-код, не зная его. Если пароль администратора не задан, возможности администратора ограничены лишь правилами форматирования.

Критерии стойкости PIN-кодов

Администратор eToken может нормировать длину и другие параметры используемых PIN-кодов, а также количество попыток ввода PIN-кода. При использовании сложных PIN-кодов оптимальным ограничением будет 15 попыток.

Работа с группами пользователей

Администратор eToken может устанавливать для разных групп пользователей разные критерии стойкости PIN-кодов. При этом для каждой группы администратор составляет файл `etpass.ini`, содержащий критерии качества PIN-кодов, и словарь нежелательных / неприемлемых паролей.

К разным группам пользователей могут применяться разные правила распределения доступа.

Разные группы пользователей могут использовать разные модели eToken.

Подготовка рабочего места администратора

Для организации рабочего места администратора eToken необходим персональный компьютер с наличием хотя бы одного свободного порта USB (если на предприятии используются USB-ключи eToken), устройства чтения смарт-карт (если на предприятии используются смарт-карты eToken) и установленным программным обеспечением для eToken. Для того чтобы подготовить рабочее место администратора:

- при необходимости установите драйвер устройства чтения смарт-карт;
- убедитесь в том, что устройство чтения смарт-карт и/или порт USB функционирует нормально;
- установите eToken RTE;
- при необходимости установите eToken RTE 3.66 RUI.

Подготовка рабочего места пользователя

Пользователь eToken должен обладать компьютером, в котором присутствует хотя бы один свободный порт USB (для USB-ключа eToken) или устройство чтения смарт-карт (для смарт-карты eToken). Для подготовки рабочего места пользователя:

- при необходимости установите драйвер устройства чтения смарт-карт;
- убедитесь в том, что устройство чтения смарт-карт (если используется смарт-карта eToken) или порт USB (если используется USB-ключ eToken) функционирует нормально;
- централизованно, удаленно или локально установите eToken RTE 3.66, а при необходимости — eToken RTE 3.66 RUI;
- скопируйте на компьютер пользователя в системную папку `%systemroot%\system32` файл `etpass.ini`, содержащий критерии качества PIN-кодов и паролей администратора eToken;

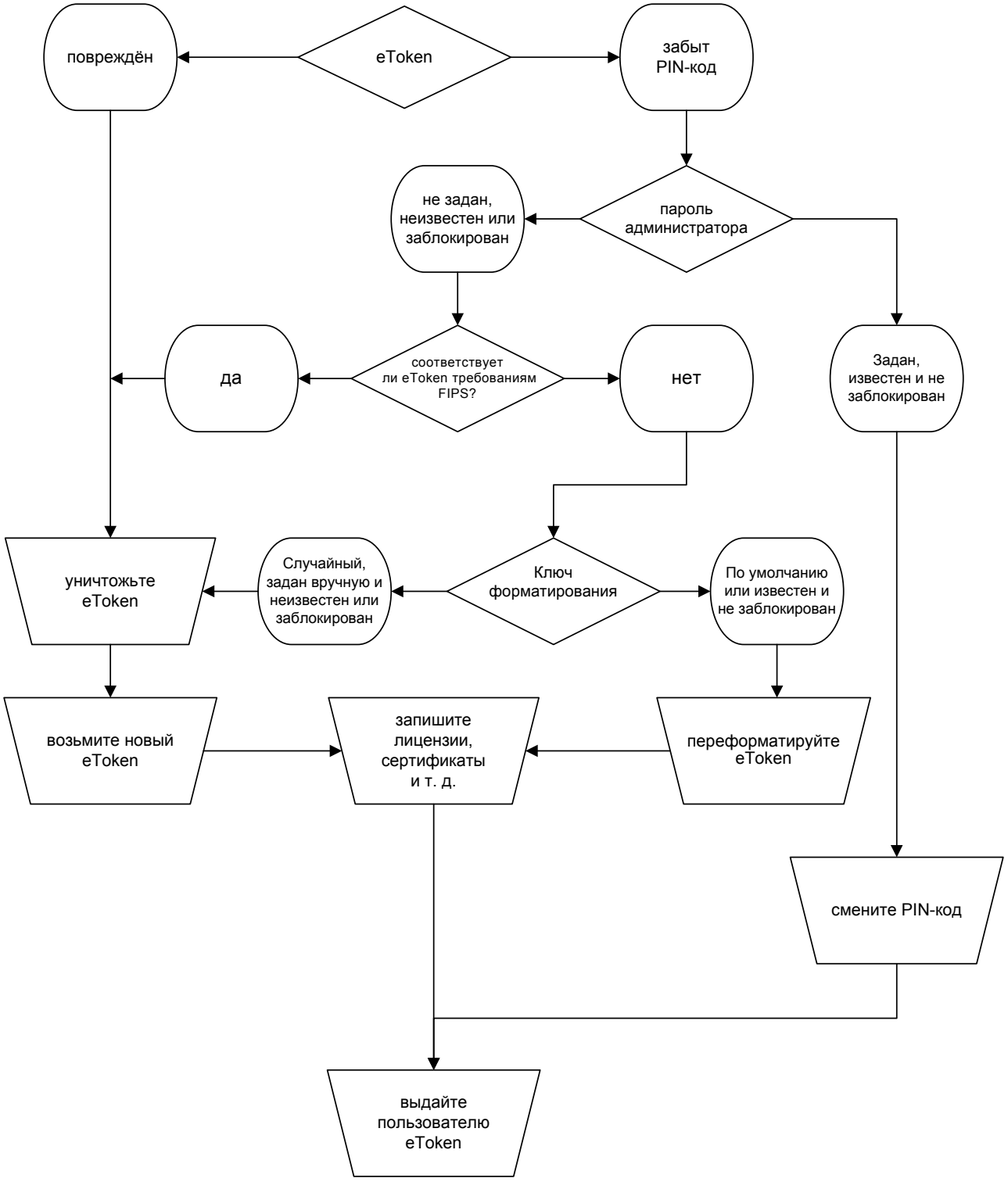
- скопируйте на компьютер пользователя словарь нежелательных/неприемлемых паролей.

Важно, чтобы путь к файлу словаря нежелательных/неприемлемых паролей, указанный в файле `etpass.ini`, соответствовал реальному расположению файла словаря на компьютере пользователя.

Замена eToken

Если eToken поврежден, уничтожьте его и выдайте пользователю новый.

Если пользователь забыл PIN-код, ваши действия зависят от состояния eToken.



Смена PIN-кода администратором eToken

Если при форматировании eToken был установлен пароль администратора, смените PIN-код и верните пользователю eToken.

Переформатирование eToken

Если пароль администратора не задан или утрачен, вы не можете сменить PIN-код, не зная его. Для того чтобы eToken можно было использовать, переформатируйте его. Вся информация, хранящаяся в памяти eToken, при этом будет потеряна. Если eToken защищен от переформатирования или/и соответствует требованиям FIPS, его PIN-код неизвестен, а пароль администратора не задан или утрачен, уничтожьте eToken и выдайте пользователю новый.

eToken уволенного сотрудника

После увольнения сотрудника необходимо выполнить следующее:

- сменить PIN-код;
- отозвать все сертификаты, изданные для увольняемого сотрудника, и удалить их из памяти eToken вместе с соответствующими ключевыми контейнерами и другими реквизитами.

Если PIN-код eToken уволенного сотрудника известен, сменить его не составит труда. Если же PIN-код неизвестен, попытайтесь осуществить те же действия, что и в случае, когда пользователь забыл PIN-код.

В случае удачной смены PIN-кода подготовьте eToken для использования другим сотрудником.

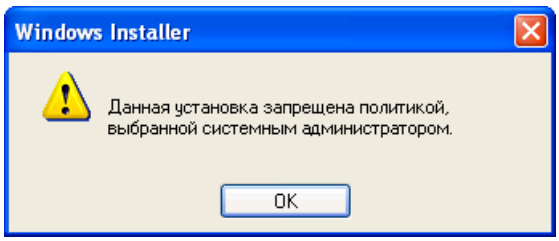
Известные проблемы и их решение

Ошибки при установке программного обеспечения

Проблема:

На экране появилось окно **Windows Installer** (Программа установки Windows) с сообщением:

`Данная установка запрещена политикой, выбранной системным администратором.`



Возможная причина:

Вы не обладаете полномочиями администратора.

Решение:

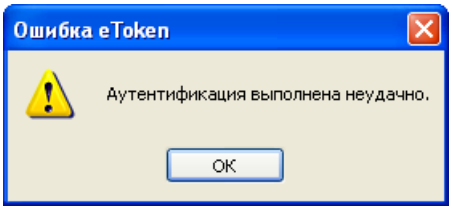
1. Нажмите **OK**.
2. Обратитесь к администратору

Ошибки при вводе PIN-кода и пароля администратора

Проблема:

На экране появилось окно **Ошибка eToken** с сообщением:

```
Аутентификация выполнена неудачно.
```



Возможная причина:

Вы неверно ввели PIN-код или пароль администратора.

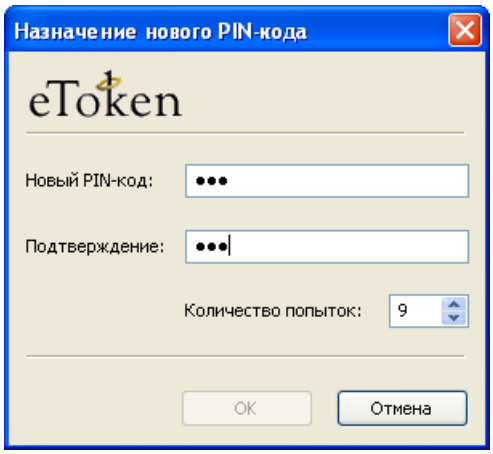
Решение:

Нажмите **OK** и повторите попытку.

Важно: число попыток ввода PIN-кода и пароля администратора eToken ограничено.

Проблема:

В окне назначения нового PIN-кода администратором или смены пароля администратора кнопка **OK** неактивна.



Возможная причина:

Для нового PIN-кода или пароля администратора вы ввели слишком короткую строку.

Решение:

Введите строку длиной не менее 4 символов.

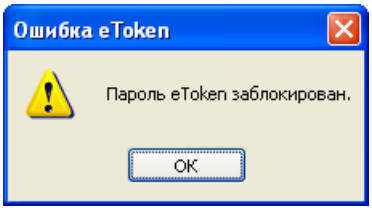
Примечание:

> критерии качества PIN-кодов в данном случае не применяются.

Проблема:

На экране появилось окно **Ошибка eToken** с сообщением:

```
Пароль eToken заблокирован.
```



Возможная причина:

PIN-код или пароль администратора eToken заблокирован, т.к. превышено количество попыток его неправильного ввода.

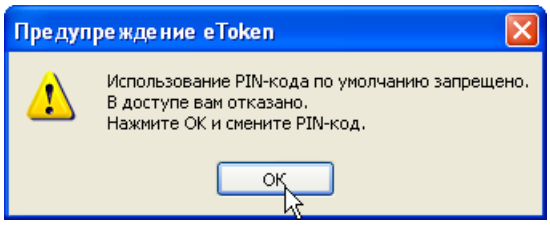
Решение:

1. Нажмите **OK**.
2. Обратитесь к разделу “eToken на предприятии”.

Проблема:

После ввода PIN-кода на экране появилось окно **Предупреждение eToken** с сообщением:

```
Использование PIN-кода по умолчанию
запрещено.
В доступе вам отказано.
Нажмите OK и смените PIN-код.
```



Возможная причина:

Данный eToken имеет PIN-код 1234567890. Согласно политике качества PIN-кодов запрещается использование PIN-кода по умолчанию.

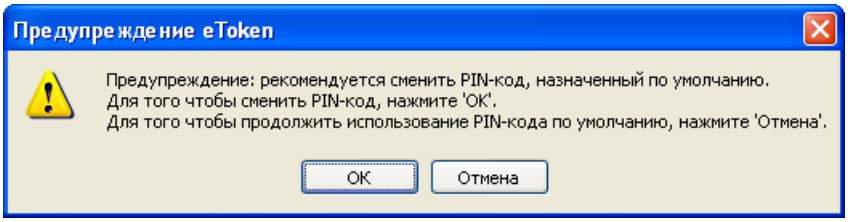
Решение:

1. Нажмите **OK**. На экране появится окно **Смена PIN-кода**.
2. Для смены PIN-кода следуйте инструкции из описания утилиты “Свойства eToken”.
3. Если вы не хотите менять PIN-код, нажмите **Отмена**. В этом случае для использования PIN-кода по умолчанию вам потребуется изменить критерии качества PIN-кодов. Для этого вы можете воспользоваться утилитой “Свойства eToken” (в некоторых режимах ее интерфейса).

Проблема:

После ввода PIN-кода на экране появилось окно **Предупреждение eToken** с сообщением:

```
Предупреждение: рекомендуется сменить PIN-код, назначенный по умолчанию.
Для того чтобы сменить PIN-код, нажмите ‘OK’.
Для того чтобы продолжить использование PIN-кода по умолчанию, нажмите ‘Отмена’.
```



Возможная причина:

Данный eToken имеет PIN-код 1234567890. Политика качества PIN-кодов не рекомендует использование PIN-кода по умолчанию.

Решение:

1. Для того чтобы сменить PIN-код:
   - нажмите **OK**;
   - следуйте инструкции из описания утилиты “Свойства eToken”.

2. Если вы не хотите менять PIN-код, нажмите **Отмена**.

Проблема:

eToken виден в диспетчере устройств, но не появляется в утилите eToken Properties.

Возможные причины:

1. Количество виртуальных считывателей установлено в 0.
2. Использование очень старой версии eToken Pro на компьютере, на котором установлен контроллер USB Open Host.
3. Использование eToken Pro 64K с версией RTE ниже 3.60.
4. Неисправный eToken либо некорректная установка RTE.

Решения:

1. Установите число считывателей равным 1 или 2 (см. раздел «Настройка параметров eToken RTE»).
2. Устройства eToken Pro, в которых последняя цифра версии встроенного ПО (firmware) меньше, чем 4 (т.е. 4.x.5.3 и ниже), вышли до появления контроллера USB Open Host. Поэтому eToken Pro некорректно работает на компьютерах с этим контроллером. Решением может быть использование на данном компьютере либо более новых eToken Pro, либо использование eToken R2, либо добавление на компьютер контроллера USB Universal Host.
3. eToken Pro 64K поддерживается начиная с RTE версии 3.60. Обновите RTE до версии 3.66.
4. Проверьте, доступны ли другие eToken на данном компьютере в утилите eToken Properties, а также работает ли данный eToken на других компьютерах. Если другие eToken на данном компьютере определяются, а данный eToken не работает и на других компьютерах, то, скорее всего, сам eToken функционирует некорректно и нуждается в замене. Если другие eToken также не определяются на данном компьютере, то попробуйте переустановить RTE 3.66.

Ошибки при форматировании eToken

Проблема:

Утилита форматирования не видит eToken.

Возможная причина:

Вы пытаетесь отформатировать eToken Pro 64K с помощью утилиты, входящей в комплект eToken Utilities

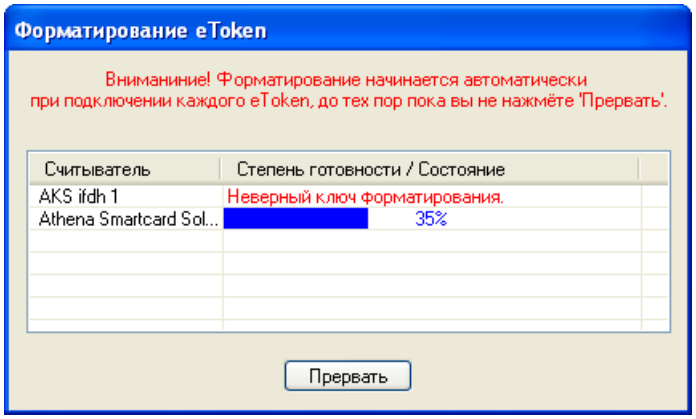
Решение:

Для форматирования eToken используйте утилиту форматирования, входящую в eToken Properties из состава RTE версии 3.66.

Проблема:

В окне **Форматирование eToken** (при автоматическом форматировании) или **Свойства eToken** (при форматировании вручную) появилось сообщение:

```
Неверный ключ форматирования.
```



Возможная причина:

Ключ форматирования указан неверно.

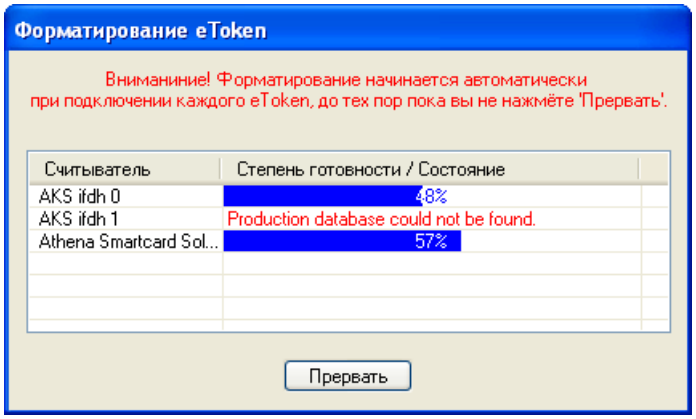
Решение:

1. Нажмите **Прервать** или **ОК**.
2. Уточните параметры форматирования.
3. Повторите попытку форматирования.

Проблема:

В окне **Форматирование eToken** появилось сообщение:

```
Production database could not be found.
```



Возможная причина:

В режиме автоматического форматирования вы подключили устаревшую модель eToken R2.

Решение:

Данная модель является устаревшей, форматировать eToken R2 нельзя. Если вам необходимо очистить память устройства, то следует удалить из его памяти ненужные объекты. В частности, для удаления сертификатов и ключевых контейнеров вы можете воспользоваться утилитой “Свойства eToken”.

Проблема:

При попытке форматирования eToken появилось сообщение:

`Объект безопасности смарт-карты заблокирован.`

Возможная причина:

Было предпринято 10 или более попыток форматирования данного eToken с указанием неверного ключа форматирования.

Решение:

Переформатировать данный eToken нельзя.

Проблема:

В окне **Параметры форматирования eToken** во вкладке **Настройки** флажок **Соответствие требованиям FIPS** неактивен.

Возможная причина:

Выбранный eToken не является USB-ключом eToken PRO со встроенным программным обеспечением (firmware) версии 4.x.5.4.

Решение:

Переформатировать данный eToken в режиме соответствия требованиям FIPS нельзя.

Проблема:

eToken NG-FLASH, отформатированный для использования в качестве загрузочного устройства, не виден на компьютере пользователя.

Возможная причина:

Выбранный eToken имеет модель 4.26, которая имеет ряд известных проблем с форматированием флеш-памяти, исправленных в версии 4.27. Модель устройства можно проверить в утилите «Свойства eToken».

Решение:

Использовать более новые eToken NG-FLASH модели 4.27 и выше.

Другие ошибки

Проблема:

Световой индикатор USB-ключа eToken не горит.

Возможные причины:

1. Вы впервые подключили данный eToken к данному порту USB.
2. Порт USB неверно настроен или неисправен.
3. eToken неисправен.

Решения:

1. Если вы впервые подключили данный eToken к данному порту USB, и eToken RTE на данном компьютере установлен, необходимо время для автоматической установки нового оборудования. Подождите немного.
2. Проверьте настройки порта USB в BIOS. Для этого:
   - перезагрузите компьютер, при перезагрузке откройте меню BIOS;

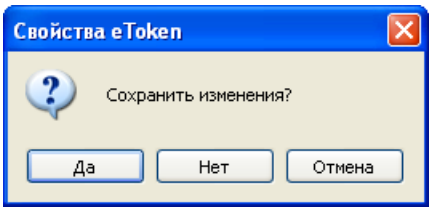
- назначьте параметру **Enable USB**, **USB Controller**, **USB Function**, и т.п. значение **Enable**, **Enabled**, **On**, и т.п.;
- назначьте параметру **Assign IRQ For USB**, **Assign USB IRQ**, и т.п. значение **Enable**, **Enabled**, **On**, и т.п.

3. Проверьте настройки порта USB в Windows. Для этого:
   - откройте **Control Panel (**Панель управления**)**;
   - если вы используете вид панели управления по категориям (category view), выберите **Performance and Maintenance** (Производительность и обслуживание);
   - дважды щелкните по значку **System (**Система**)**;
   - в окне **System Properties** (Свойства системы) откройте вкладку **Hardware (**Оборудование (Устройства));
   - в Windows 2000/XP/Vista нажмите **Device Manager** (Диспетчер устройств);
   - убедитесь в том, что в дереве консоли присутствует узел **Universal Serial Bus Controllers (**Контроллеры шины USB (Контроллеры универсальной последовательной шины USB)), а в нем — **USB Root Hub (**Корневой концентратор для USB (Корневой разветвитель для USB)).
4. Если проблема связана с аппаратной неисправностью порта USB или eToken, замените вышедшее из строя оборудование.

Проблема:

На экране появилось диалоговое окно **Свойства eToken** с вопросом:

```
Сохранить изменения?
```



Возможная причина:

Не сохранив изменения в одном разделе окна **Свойства eToken**, вы попытались перейти к другому разделу.

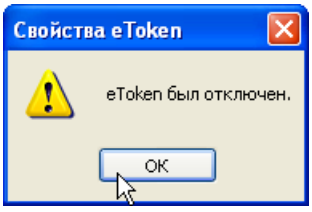
Решение:

Для сохранения изменений и перехода в другой раздел нажмите **Да**. Для того чтобы перейти в другой раздел без сохранения изменений, нажмите **Нет**. Если вы не хотите переходить к другому разделу, нажмите **Cancel**.

Проблема:

На экране появилось окно с сообщением:

```
eToken был отключен.
```



Возможная причина:

eToken отключен.

Решение:

Нажмите **OK** и подключите eToken.

Проблема:

Вы подключили eToken к компьютеру. На экране появилось сообщение **Found New Hardware** (Найдено новое оборудование, Поиск нового оборудования, Обнаружено новое оборудование) и окно **Found New Hardware Wizard** (Мастер нового оборудования, Мастер обнаружения нового оборудования, Установка оборудования).

Возможная причина:

На компьютере не установлен eToken RTE 3.66.

Решение:

Если eToken RTE не установлен или требуется обновление его версии

- в окне **Found New Hardware Wizard** (Мастер нового оборудования, Мастер обнаружения нового оборудования, Установка оборудования) нажмите **Cancel (**Отмена**)**;
- отключите eToken;
- установите/переустановите eToken RTE.

Проблема:

Несмотря на то, что ваш USB-ключ eToken подключен к компьютеру и его световой индикатор горит, приложение ведет себя так, как будто этот eToken не подключен

Возможная причина:

Количество подсоединенных к компьютеру USB-ключей eToken превышает количество виртуальных считывателей, присутствующих в системе.

Решение:

1. Отключите от компьютера все eToken, включая тот, что отсутствует в списке.
2. Подключите к компьютеру один или несколько eToken, но не более, чем количество виртуальных считывателей, присутствующих в системе (по умолчанию таких устройств два).
3. Убедитесь в том, что нужный eToken подключен (световой индикатор USB-ключа eToken должен гореть).
4. При необходимости обновите в приложении список подключенных eToken.

Проблема:

При подключении eToken NG-FLASH с эмуляцией CD-ROM производится автозапуск. Производится попытка чтения файла автозапуска, а при его отсутствии — вывод окна с предложением перечня возможных операций.

Возможная причина:

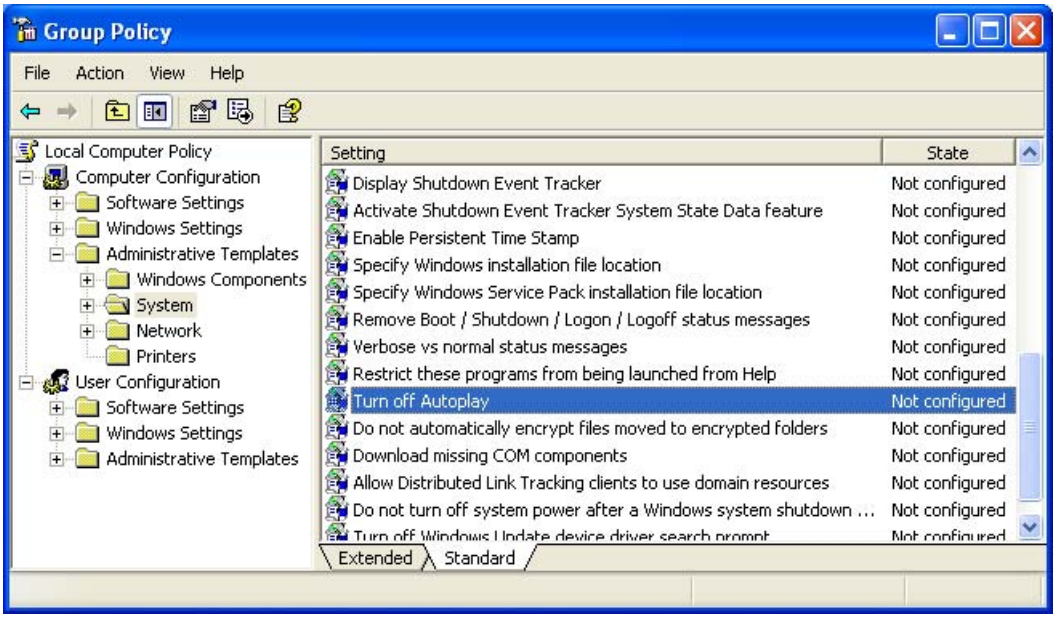
Не отключена функция автозапуска

Решение:

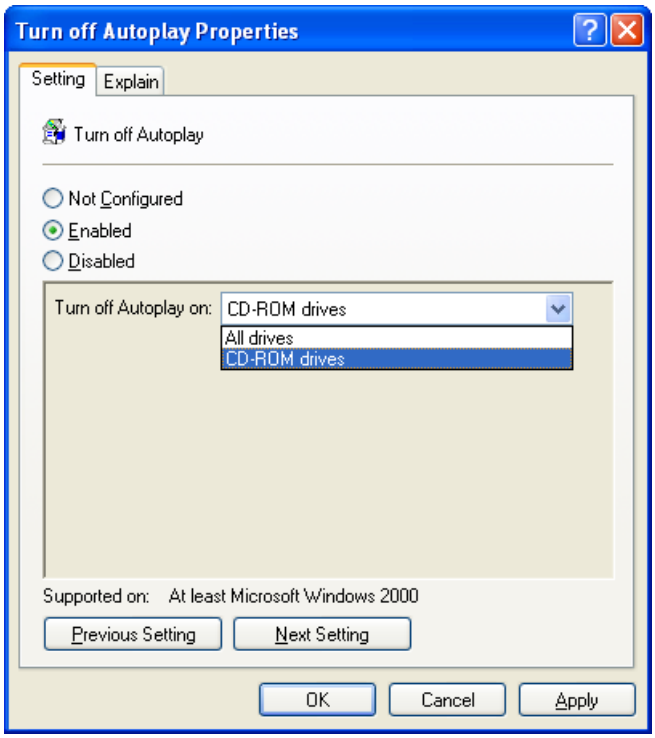
Для отключения данной функции выполните следующие действия:

1. Запустите редактор групповых полисов с помощью команды **Start > Run > gpedit.mmc** (Пуск > Выполнить > gpedit.mmc).

2. В окне редактора выберите **Computer Configuration > Administrative Templates > System > Turn off Autoplay** (Конфигурация компьютера > Административные шаблоны > Система > Отключить автозапуск) и нажмите ENTER.



3. В окне **Turn off Autoplay Properties** (Свойства отключения функции "Автозапуск") выберите значение **CD-ROM** (для отключения функции автозапуска на устройствах CD-ROM) или **All drives** (для отключения функции автозапуска на всех дисках).



4. Нажмите **Apply** (Применить) и закройте окно.

Проблема:

При подключении eToken NG-FLASH сетевые диски становятся недоступными.

Возможная причина:

Программа Mount Manager, присваивающая имена дискам, не распознает сетевые диски и присваивает новому диску или разделу следующую доступную букву. При этом возможна ситуация, когда секции ROM или Mass Storage устройства eToken NG-FLASH присваивается буква существующего (подключенного) в системе сетевого диска.

Решение:

Чтобы предотвратить возникновение данной ситуации, необходимо сетевому диску при подключении присвоить самую последнюю букву. Для этого выполните следующие действия:

1. Щелкните правой кнопкой мыши на значок **My Computer** (Мой компьютер) и выберите **Manage** (Управление).
2. В группе **Computer Management (Local)** (Управление компьютером (локальное)) выберите пункт **Disc Management** (Управление дисками).
3. В списке дисков в правой области просмотра правым щелчком мыши выберите новый диск и в раскрывающемся меню выберите команду **Change drive letter and Paths** (Изменить букву диска или путь к диску).
4. Нажмите **Change** (Изменить) и в раскрывающемся меню выберите букву диска, которая не присвоена подключенному сетевому диску.

Подтвердите изменение настроек, два раза нажав кнопку **OK**.

Проблема:

При запуске утилиты eToken Properties выдается сообщение:

`Smartcard resource manager has been stopped`

Возможные причины:

1. Вы работаете в режиме терминальной сессии и хотите получить доступ к eToken, подключенному непосредственно к серверу.
2. Служба смарт-карт запущена от имени другой учетной записи, либо у текущей учетной записи пользователя не хватает прав на создание виртуальных считывателей смарт-карт.

Решения:

1. Необходимо помнить, что все ресурсы смарт-карт берутся с клиентского компьютера. Получить доступ к eToken, подключенному непосредственно к серверу в терминальной сессии невозможно. Для работы с eToken, установленному на стороне клиента, в этом случае необходима установка RTE как на клиенте, так и на сервере.
2. • Войдите в систему от имени локального администратора.

   • Отключите eToken.

   • Удалите eToken RTE через панель управления/Установка и удаление программ.

   • Запустите редактор реестра (regedit).

   • Откройте следующий раздел реестра:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Calais`

   Щелкните по `Calais` правой кнопкой мышки и выберите **Разрешения**.

   • Проверьте, существуют ли ниже перечисленные группы с указанными разрешениями. Если какой-то из групп нет, либо же разрешение стоит некорректно, внесите соответствующие изменения:

   - `Administrators – Full Control`

   - `CREATOR OWNER – Special Permissions (Full Control)`

   - **LOCAL SERVICE - (Read и Special Permissions все кроме Full control и Create Links)**

- Power Users - Read
- SYSTEM - Full Control
- Users - Read

• Закройте редактор реестра.

• Откройте консоль mmc «Службы» (Панель управления/Администрирование/Службы или Control Panel/Administrative Tools/Services). Остановите и заново запустите службу Смарт-карты (Smart Card).

• Если есть проблемы с запуском службы, то запустите редактор реестра еще раз.

• Откройте следующий раздел реестра:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SCardSvr

Создайте строковый параметр ObjectName со значением "NT AUTHORITY\LocalService".

• Перезапустите компьютер.

• Откройте консоль mmc «Службы».

• Проверьте, что служба запускается от имени "NT AUTHORITY\LocalService".

• В случае если служба запускается от другого имени, то проверьте значение параметра ObjectName в следующем разделе реестра:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SCardSvr

• Перезагрузите компьютер и еще раз проверьте, от какого имени запускается служба.

Подробная информация доступна также по этому адресу: http://support.microsoft.com/?kbid=832082 (на английском).

Проблема:

Не виден eToken при доступе через удаленный рабочий стол.

Возможная причина:

В терминальной сессии работа с eToken, который подключен непосредственно к серверу, невозможна, это ограничение службы терминалов.

Решение:

При работе через удаленный рабочий стол eToken необходимо подключать к клиентской станции. При этом и на сервере, и на клиенте должно быть установлено RTE, а в настройках клиента удаленного доступа (RDP) необходимо включить перенаправление локальных смарт-карт в терминальную сессию.

Часто задаваемые вопросы

Вопрос:

Как отформатировать eToken?

Ответ:

в утилиту eToken Properties уже встроена возможность форматирования, но она по умолчанию недоступна в пользовательском интерфейсе. Для активации возможности форматирования задайте параметру Advanced значение 1f в следующем разделе реестра: HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\eTProperties

После этого в утилите eToken Properties появится кнопка "Форматирование". При форматировании eToken вся информация с него удаляется.

Вопрос:

Как задать пароль администратора?

Ответ:

Пароль администратора можно задать только при форматировании eToken. При форматировании eToken вся информация с него удаляется.

Вопрос:

Как сбросить PIN-код eToken или разблокировать eToken, используя пароль администратора?

Ответ:

Для того чтобы изменить PIN-код eToken или разблокировать eToken, нужно аутентифицироваться в утилите eToken Properties с помощью пароля администратора, а затем на вкладке «Администратор» нажать кнопку «Задать PIN-код»

Вопрос:

Что делать, если пользователь забыл PIN-код своего eToken?

Ответ:

Если при форматировании был установлен пароль администратора, то достаточно выбрать пункт Administration в контекстном меню ключа утилиты eToken Properties и сменить пользовательский PIN-код.

Если при форматировании не был установлен пароль администратора, то поможет только новое форматирование ключа с полной потерей всей хранимой информации.

Вопрос:

Можно ли каким-либо образом сохранить копию сертификата с закрытым ключом, хранящегося на eToken?

Ответ:

Если сертификат генерировался непосредственно на eToken, то создать резервную копию сертификата и закрытого ключа нельзя, так как закрытый ключ никогда не покидает eToken.

Если резервная копия сертификата необходима, то можно создать сертификат вне eToken, потом сохранить резервную копию, а затем поместить сертификат и закрытый ключ на eToken.

Предметный указатель

