Aladdin
SECURITY SOLUTIONS
www.aladdin.ru

eToken PKI Client 5.1 SP1

Руководство пользователя

Листов: 63

версия документа: 1.2

Содержание

1. Лицензионное соглашение

ВАЖНАЯ ИНФОРМАЦИЯ

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, ПРЕЖДЕ ЧЕМ ОТКРЫТЬ ПАКЕТ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И/ИЛИ ИСПОЛЬЗОВАТЬ ЕГО СОДЕРЖИМОЕ И/ИЛИ ПРЕЖДЕ, ЧЕМ ЗАГРУЖАТЬ ИЛИ УСТАНАВЛИВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ ПРОДУКТОВ с использованием электронных ключей и смарт-карт eToken (включая без ограничений библиотеки, утилиты, дискеты, CD ROM, ключи и смарт-карты eToken®, Руководства, описания и др. документацию) (далее ”Продукт”), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ ALADDIN (или любым дочерним предприятием – каждое из них упоминаемое как ”ALADDIN”), ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ.

ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (как определено далее по тексту) И/ИЛИ УСТАНАВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, **ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ**.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНАВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В ALADDIN, СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

Текст соглашения

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и компанией Aladdin Software Security R.D. (далее "Aladdin") относительно передачи неисключительного права на использование программного обеспечения (далее "ПО"), работающего с электронными ключами и смарт-картами eToken или ПО для eToken.

1. Права и Собственность.

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Это программное обеспечение, поддерживающее eToken, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как "Программное обеспечение"), и связанная с ней документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью компании Aladdin.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/ взаимосвязанные/ имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на Продукцию являются и будут являться собственностью исключительно компании Aladdin.

Данное соглашение не передает Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Aladdin от прав на интеллектуальную собственность по какому бы то ни было законодательству.

2. Лицензия.

После уплаты соответствующего вознаграждения Aladdin настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на

использование данного Программного обеспечения только в форме исполняемого кода, как описано в прилагаемой к Программному обеспечению документации и только в соответствии с условиями данного Соглашения:

Вы можете установить Программное обеспечение и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей документации компании Aladdin.

Вы можете добавить/присоединить Программное обеспечение к программам Вашего компьютера с единственной целью, описанной в данном Руководстве.

3. Требования к использованию.

Продукт должен использоваться и обслуживаться строго в соответствии с описаниями и инструкциями компании Aladdin, приведенными в данном и других документах Aladdin. За исключением указанного выше в разделах 1 и 2 Вы соглашаетесь:

- Не использовать, не модифицировать, и не выдавать сублицензии на данное Программное обеспечение и любую другую Продукцию компании Aladdin, за исключением явных разрешений в данном Соглашении и в Руководстве по интеграции.

- Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду, не передавать, не переводить на другие языки, не закладывать, не разделять Ваши права в рамках данного Соглашения с кем-либо или кому-либо ещё.

- Не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения.

- Не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть.

- Не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

4. Обслуживание и поддержка.

Aladdin не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного Программного обеспечения.

5. Ограниченная гарантия.

   Aladdin гарантирует, что:

- Данное Программное обеспечение с момента поставки его Вам в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с Руководством Пользователя (Администратора), при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

- Ключ (смарт-карта) eToken в течение 12 (двенадцати) месяцев с момента поставки будет в достаточной мере свободен от значительных дефектов в материалах, конструктивных характеристиках и качестве.

6. Отказ от гарантии.

ALADDIN НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБОЙ ИЗ ЕГО ПРОДУКТОВ БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, ALADDIN ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОГО ВИДА И ПРИГОДНОСТИ ИСПОЛЬЗОВАНИЯ ДЛЯ ОПРЕДЕЛЁННОЙ ЦЕЛИ.

НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ ALADDIN НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.

Если Вы произвели какие-либо модификации Программного обеспечения или любой из частей данного Продукта во время гарантийного периода, если ключ (смарт-карта) eToken подвергся повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если Продукт используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в данном Руководстве, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

7. Ограничение возмещения.

В случае нарушения гарантии, оговоренной выше, Aladdin может по собственному усмотрению:

- Заменить или бесплатно отремонтировать Продукт или его составляющие, если это не противоречит вышеупомянутому ограничению гарантии.

- Возместить стоимость, выплаченную Вами за Продукт или его компоненты. Любая замененная или отремонтированная компонента будет на гарантии или в течение промежутка времени, оставшегося от начального гарантийного периода, или в течение 30 дней, если срок начального гарантийного периода истекает ранее. Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Aladdin. Все Продукты должны быть возвращены дистрибьютору, через которого была совершена покупка (если покупка состоялась не непосредственно в Aladdin), и отправлена возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Продукты или их компоненты должны быть отправлены с копией платежных документов и накладных.

8. Исключение косвенных убытков.

Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. ALADDIN НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОЙ КОМПОЕНТЫ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ALADDIN ПИСЬМЕННО УВЕДОМЛЁН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

9. Ограничение ответственности.

В СЛУЧАЕ ЕСЛИ, НЕСМОТРЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, ALADDIN ПРИЗНАН ОТВЕТСТВЕННЫМ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ ALADDIN ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

10. Прекращение действия.

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено. После прекращения действия данного Лицензионного соглашения:

- Лицензия, предоставленная Вам данным Соглашением, прекращает свое действие, и Вы после ее прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- Вы незамедлительно вернёте в компанию Aladdin всё имущество, в котором используются права Aladdin на интеллектуальную собственность и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в них в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

11. Применимое законодательство.

Данное Соглашение должно быть истолковано и определено в соответствии с законами России (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Применение Конвенции Организации Объединённых Наций о Договорах международной купли-продажи товаров (the United Nations Convention of Contracts for the International Sale of Goods) однозначно исключается. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

12. Государственное регулирование и экспортный контроль.

Вы соглашаетесь с тем, что Продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом. Продукт является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт Продукта ограничения.

13. Программное обеспечение третьих сторон.

Если Продукт содержит в себе любое программное обеспечение, предоставленное какой-либо третьей стороной, такое программное обеспечение третьей стороны предоставляется "как есть" без какой-либо гарантии, и разделы 2, 3, 6, 8, 9-12 настоящего Соглашения применяются ко всем таким поставщикам программного обеспечения и к поставляемому ими программному обеспечению, как если бы это были Aladdin и Продукт соответственно.

14. Разное.

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

Авторские права и торговые знаки

eToken является зарегистрированным товарным знаком компании Aladdin Knowledge Systems Ltd.

ALADDIN KNOWLEDGE SYSTEMS LTD является зарегистрированным товарным знаком компании Aladdin Knowledge Systems Ltd.

Все другие товарные знаки, обозначения и названия изделий, используемые в данном документе, являются или могут быть товарными знаками соответствующих владельцев.

2. Введение

eToken PKI Client 5.1 – набор драйверов и дополнительных утилит, обеспечивающий работу с электронными ключами eToken в операционной системе Microsoft Windows.

Краткое содержание главы:

- Обзор
- Новые возможности в eToken PKI Client 5.1 SP1

2.1. Обзор

Инфраструктура открытого ключа (ИОК, PKI) – среда безопасного обмена данными с использованием ассиметричного шифрования. Основная задача ИОК – обеспечение защищенного обмена данными с использованием шифрования на открытом ключе. Каждый зарегистрированный конечный пользователь обладают уникальной парой ключей: открытым и закрытым ключом. Если первый может открыто передаваться от одного пользователя другому, то закрытый ключ должен храниться только у того пользователя, который является его владельцем, а соответственно для закрытого ключа должны быть обеспечены соответствующие меры и средства обеспечения сохранности. Таковыми являются электронные ключи и смарт-карты eToken, которые используются для генерации и хранения закрытых ключей, а также выполнения операций, требующих наличия закрытого ключа. Генерация, хранение и использование закрытых ключей RSA происходит в защищенном режиме на микросхеме смарт-карты eToken – сгенерированный закрытый ключ никогда не покидает память устройства. Для поддержки eToken в программном обеспечении ИОК требуется пакет eToken PKI Client, который включает в себя необходимые драйверы и утилиты для работы с устройствами eToken.

eToken PKI Client имеет широкий спектр применения в сфере информационной безопасности. Этот пакет обеспечивает взаимодействие устройств eToken с программным обеспечением Aladdin и сторонних разработчиков для реализации самых различных решений информационной безопасности. К числу таких решений можно отнести PKI-решения на базе интерфейсов PKCS#11 или CAPI, ПО для работы с eToken, (например eToken Single Sign-On), eToken Network Logon, систему централизованного управления eToken (Token Management System).

eToken PKI Client используется в процессе построения системы строгой двухфакторной аутентификации на базе цифровых сертификатов, а также реализации шифрования и электронной цифровой подписи (ЭЦП). Кроме того, eToken PKI Client обеспечивает возможность использования таких стандартных интерфейсов как Microsoft CAPI и PKCS#11 для доступа внешних приложений к устройствам eToken. Благодаря этому eToken может применяться для безопасного доступа в Интернет, VPN-сети, доступа к локальной сети, защиты данных, безопасного обмена электронными сообщениями, а также для работы с другими приложениями.

2.2. Новые возможности в eToken PKI Client 5.1 SP1

eToken PKI Client 5.1 SP1 обладает по сравнению с более ранними версиями следующими преимуществами:

Расширенная поддержка платформ Microsoft: добавилась поддержка Windows 7 и Windows Server 2008 R2. Кроме того, теперь также поддерживается браузер Internet Explorer 8.0

Поддержка новых моделей eToken: в нынешней версии утилиты eToken имеется возможность работать с устройствами eToken NG-Flash 4.50 CardOS, eToken NG-Flash 5.30 Java и eToken NG-Flash 5.30 Java Anywhere.

Поддержка новых алгоритмов хэширования: поддержка всей серии алгоритмов SHA-2.

Поддержка по умолчанию сертификатов в кодировке, отличной от DER: атрибут TolerantX509Attribute теперь имеет значение «Истина» по умолчанию.

При работе над этой версией помимо перечисленных усовершенствований были учтены отзывы и требования клиентов, полученные с момента выпуска предыдущих версий.

3. Интерфейс пользователя

Данная глава поможет вам лучше ориентироваться в интерфейсе eToken PKI Client.

Все функции eToken PKI Client доступны из основного интерфейса, а наиболее часто используемые – из меню, вызываемого из области уведомлений.

Краткое содержание главы:

- Обзор пользовательского интерфейса eToken PKI Client
- Значок eToken PKI Client в области уведомлений панели задач
- Главное окно утилиты PKI Properties

3.1. Обзор пользовательского интерфейса eToken PKI Client

Утилита Свойства eToken предоставляет администратору инструменты для работы с устройствами eToken, а также для задания политик использования устройств пользователями. Пользователи могут использовать эту утилиту для выполнения базовых операций с eToken, таких как: смена пароля, просмотр сертификатов, хранящихся в памяти устройства. Кроме того, утилита Свойства eToken позволяет пользователям и администраторам легко экспортировать и импортировать сертификаты между eToken и компьютером.

Это приложение также дает возможность администраторам инициализировать eToken в соответствии с определенной корпоративной политикой безопасности – утилита позволяет задавать гибкие настройки требований к качеству устанавливаемого пароля.

Примечание:

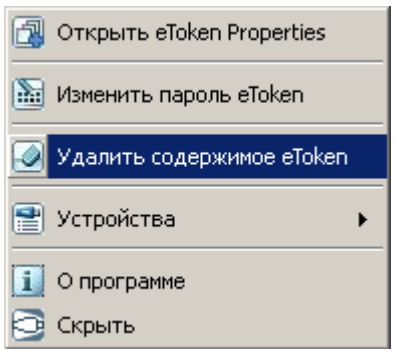
Во время выполнения операций с устройством eToken ни в коем случае не отсоединяйте его от USB-порта. Это может привести к потере данных на eToken.

eToken PKI Client Properties предоставляет информацию о eToken, включая серийный номер устройства и дополнительные параметры. Эта утилита имеет доступ к информации, хранящейся на eToken, такой как: ключи и сертификаты, и позволяет управлять информацией о пароле eToken.

3.2. Меню быстрого доступа

В области уведомлений находится значок eToken PKI Client, который открывает доступ к наиболее часто используемым функциям.

Чтобы открыть меню быстрого запуска, щелкните дважды на значке  в области уведомлений, и появится меню следующего вида:



3.3. Функции, доступные в меню быстрого запуска eToken PKI Client

Следующие функции доступны в меню быстрого запуска eToken PKI Client:

Открыть eToken Properties: открывает главное окно eToken PKI Client Properties

Сгенерировать одноразовый пароль: сгенерировать одноразовый пароль для eToken Virtual. Данная функция доступна, если конфигурация eToken Virtual поддерживает эту функцию.

Изменить пароль eToken

Удалить eToken: удаляет данные с eToken

Устройства eToken: выбор активного устройства из списка всех подключенных в данный момент устройств eToken

О программе: отображает информацию о продукте

Скрыть: скрывает иконку eToken PKI Client из панели задач

3.4. Скрытие и отображение иконки eToken PKI Client в панели задач

Чтобы скрыть иконку eToken PKI Client из панели задач, выберите в меню быстрого запуска пункт **Скрыть**.

Значок в области уведомлений появляется снова после подключения устройства eToken или при перезагрузке компьютера.

3.5. Главное окно утилиты eToken PKI Properties

Утилита eToken PKI Properties может работать в двух режимах:

Стандартный – в этом режиме доступны только базовые функции утилиты, см. Функции стандартного режима.

Расширенный – в этом режиме доступны все функции PKI Client и eToken, см. Функции расширенного режима.

Независимо от режима работы, главное окно утилиты разделено на две части:

В левой части окна представлен список доступных eToken (Стандартный режим) и устройств (Расширенный режим)

В правой панели представлены те действия, которые доступны для выбранного eToken

Панель инструментов вверху окна позволяет выполнять определенные действия в обоих режимах.

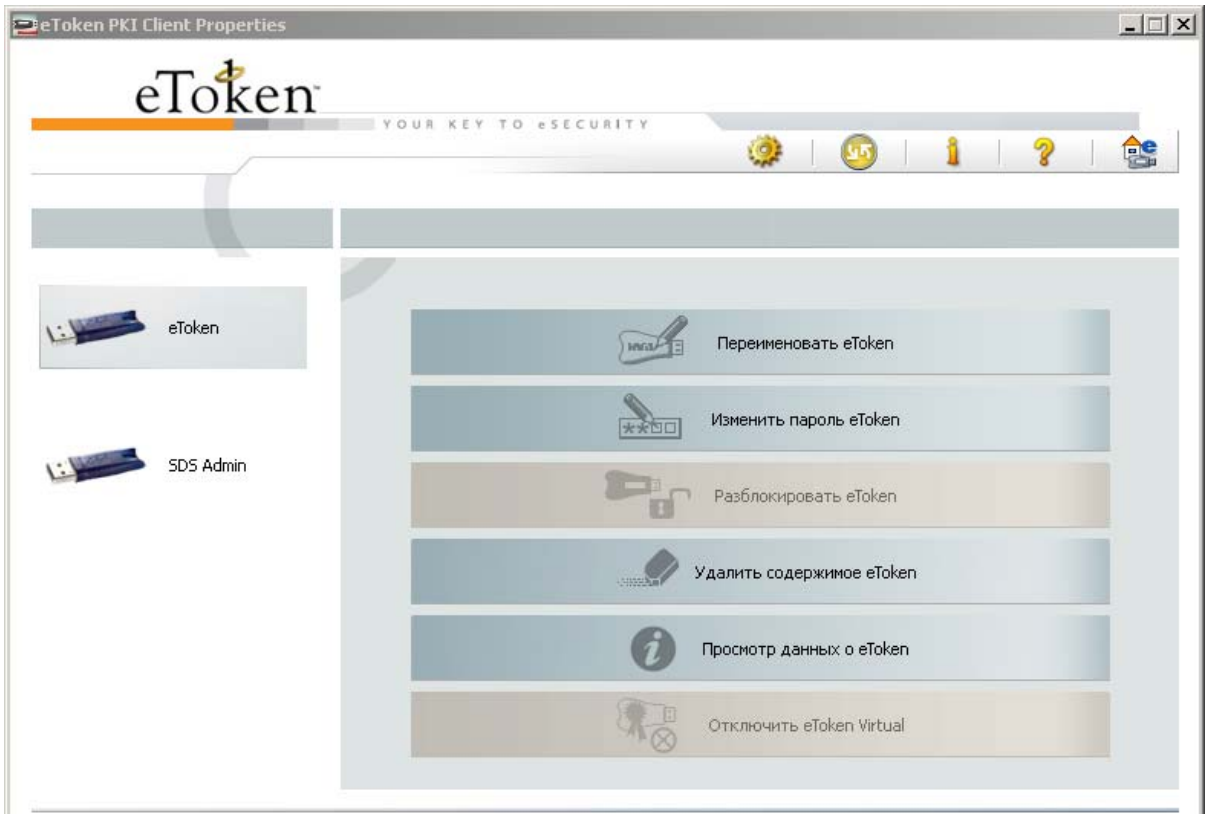
4. Панель инструментов eToken PKI Client Properties

Панель инструментов главного окна eToken PKI Client Properties отображается в стандартном и в расширенном режиме. Панель инструментов содержит следующие иконки:

Значок	Действие
	**Подробный вид** – переход от стандартного вида к расширенному.
	**Простой вид –** переход от стандартного вида к стандартному.
	**Обновить** – обновление данных всех подключенных eToken
	**О программе –** отображает информацию о версии eToken PKI Client
	**Справка** – открывает справку
	**Домашняя страница eToken** – открывает Web-сайт eToken

4.1. Стандартный режим

При запуске eToken PKI Properties окно eToken PKI Properties открывается в стандартном режиме.



При подключении аппаратного eToken или eToken Virtual, в левой панели окна отображается соответствующий значок.

Имя каждого eToken отображается справа от значка. Если имя устройства не было задано при инициализации или позднее, то для данного устройства будет отображаться имя по умолчанию - *eToken*.

Значок выбранного в данный момент устройства отмечен затененным прямоугольником.

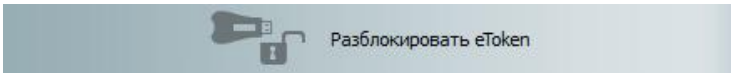
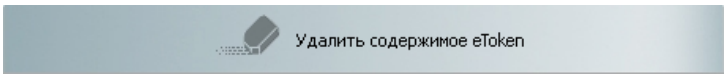
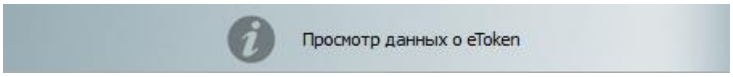
4.2. Значки устройств eToken

Значки, соответствующие различному типу подключаемых устройств:

Значок	Тип устройства
	eToken PRO
	eToken Virtual
	eToken Virtual (Emulated)
	eToken Rescue
	eToken Rescue (Emulated)
	eToken NG-OTP
	eToken NG-FLASH
	смарт-карт ридер без смарт-карты
	смарт-карт ридер с подключенной смарт-картой
	eToken или eToken Virtual с нарушенной структурой данных
	Неизвестное устройство

4.3. Функции стандартного режима

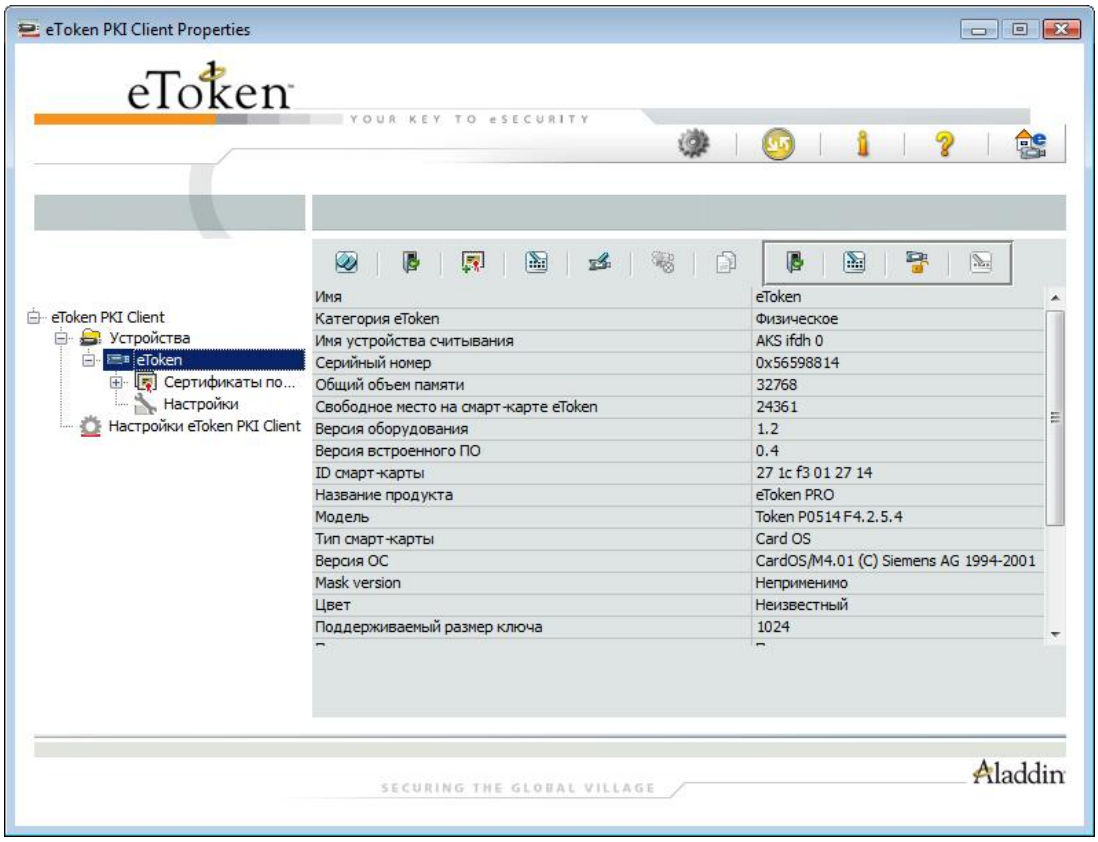
В правой части окна вы можете выбрать любую из следующих кнопок для выполнения описанных ниже действий.

Функция	Кнопка
Изменение имени eToken	
Изменение пароля пользователя eToken	
Сброс пароля пользователя с помощью механизма «запрос-ответ». Данная операция доступа только в том случае, если при инициализации eToken был установлен пароль администратора	
удаление данных с eToken	
Просмотр данных о eToken – просмотр подробной информации об eToken	
Отключение eToken Virtual или eToken Rescue. После отсоединения можно удалить файл eToken можно удалить.	

4.4. Расширенный режим

Расширенный режим утилиты Свойства eToken открывает доступ к дополнительным функциям управления eToken.

Для доступа к расширенному режиму щелкните левой кнопкой мыши на значке  - окно утилиты будет иметь следующий вид:



В левой части окна расположено дерево, где сгруппированы различные объекты управления. Если раскрыть все ветви дерева, можно увидеть информацию обо всех подключенных устройствах eToken.

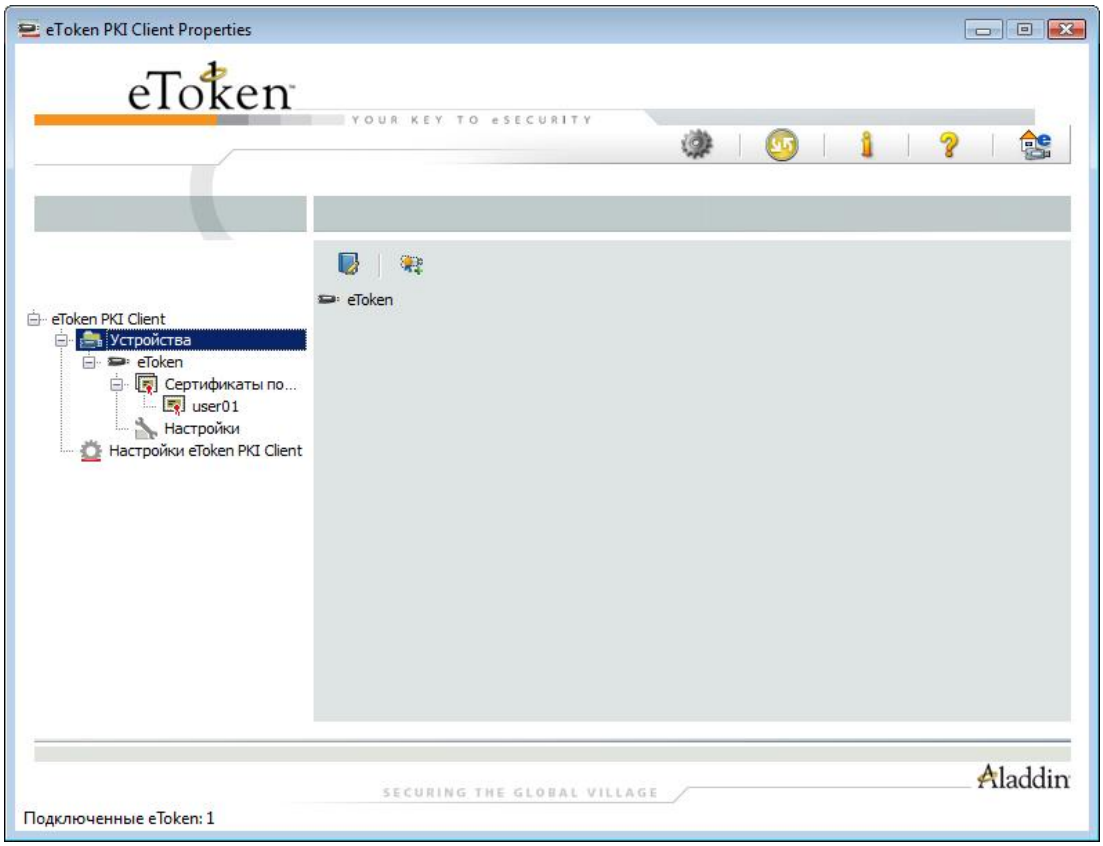
Доступ к функциям выбранного объекта можно получить, щелкнув на иконке устройства eToken в правой части окна, либо нажать правой кнопкой мыши на объекте и выбрать необходимую функцию из меню.

4.5. Функции расширенного режима

Доступ к функциям расширенного режима можно получить, выбрав необходимый объект в левой части окна.

4.5.1 Узел Устройства eToken

При выборе узла Устройства, список доступных устройств eToken будет отображен в правой части окна.

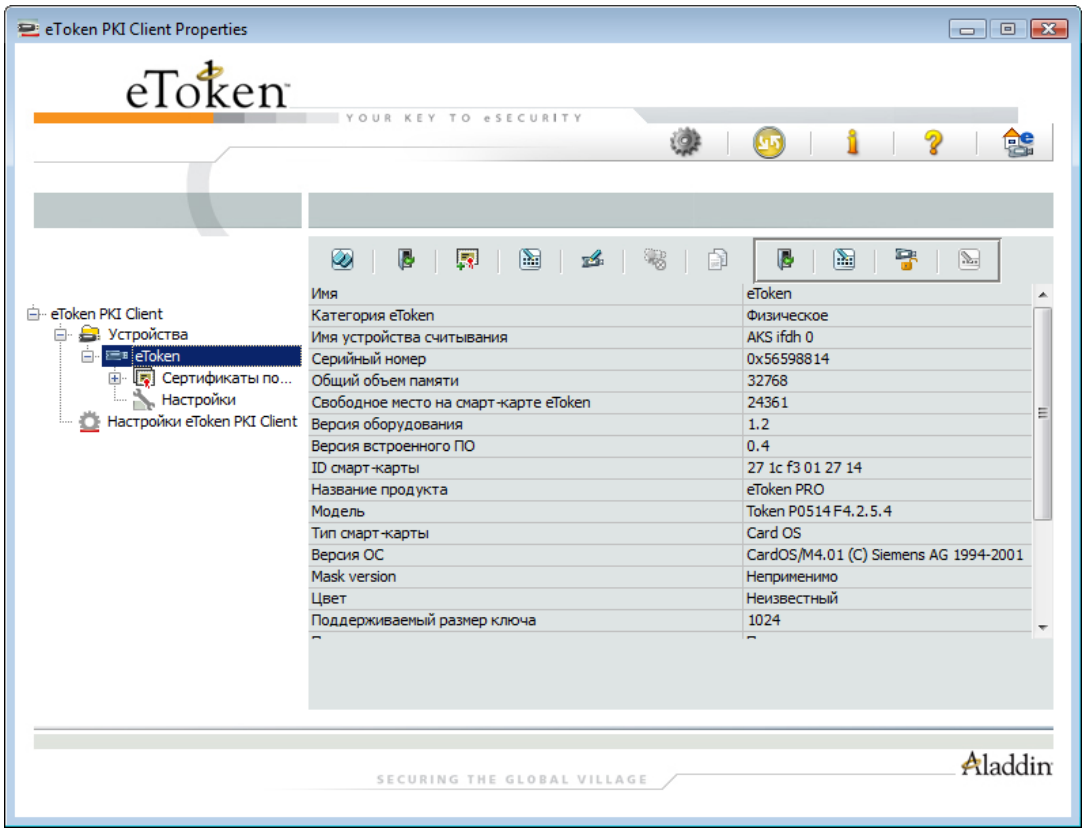


Следующие функции доступны при выборе узла Устройства:

Функция	Значок	Пункт меню
Управление считывателями См. Управление считывателями		Управление считывателями
Подключить eToken Virtual См. Подключение eToken Virtual или eToken Rescue		Подключить eToken Virtual

4.5.2 Просмотр данных об устройстве eToken

Устройства eToken отображаются в левой части окна. Информация о выбранном устройстве eToken доступна в правой части окна.



Пользователю доступны следующие функции:

Функция	Иконка	Пункт меню
Инициализировать eToken См. Инициализация eToken		Инициализировать
Авторизация См. раздел Авторизация с правами пользователя		Вход
Импорт сертификата См. Импорт сертификата		Импорт сертификата
Изменить пароль См. Смена пароля eToken		Изменить пароль
Переименовать eToken См. Переименование eToken		Переименовать
Отключить eToken Virtual (только для eToken Virtual или eToken Rescue)		Отключить

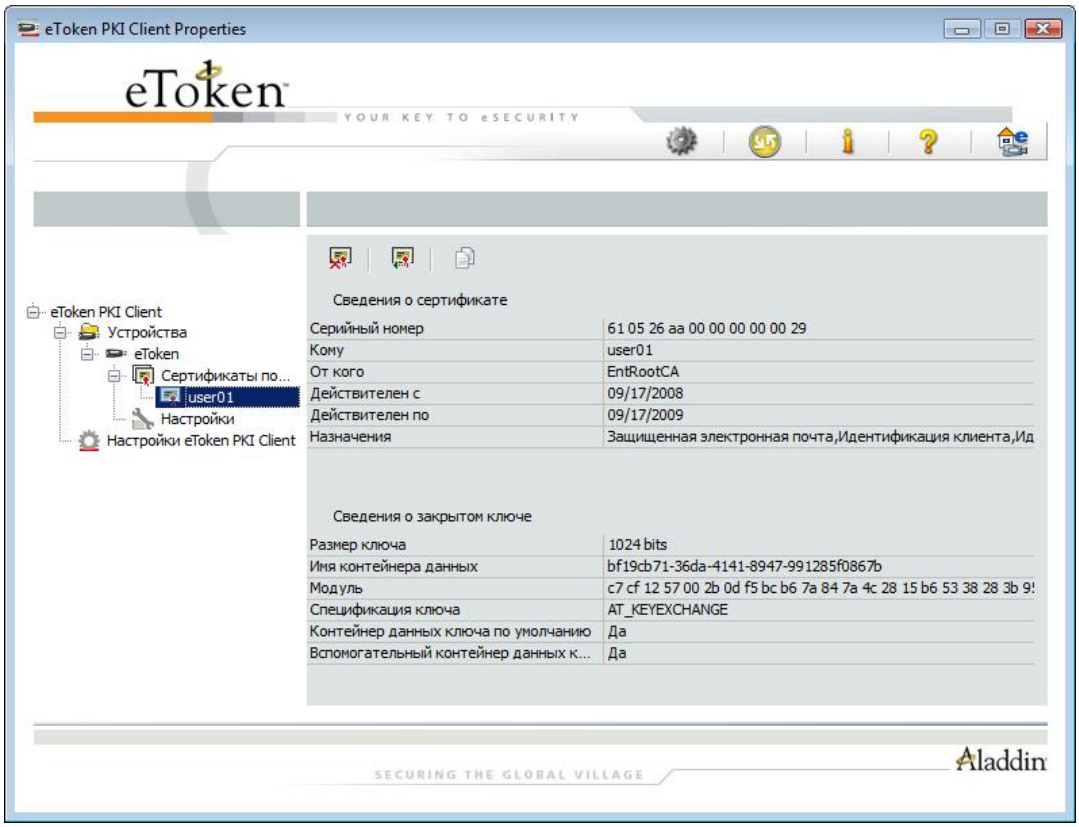
Функция	Иконка	Пункт меню
См. Отключение или удаление eToken Virtual или eToken Rescue		
Копировать в буфер обмена См. Просмотр сведений об eToken		Нет

Некоторые из функций доступны только после авторизации с паролем администратора eToken. Значки этих функций выделены в отдельную группу справа.

Функция	Иконка	Пункт меню
Вход с правами администратора См. Авторизация с правами администратора		Вход с правами администратора
Изменить пароль администратора См. Смена пароля eToken		Изменить пароль администратора
Разблокировать eToken См. Разблокирование eToken, используя механизм «запрос-ответ»		Разблокировать
Установить пароль пользователя (активно только в том случае если, был выполнен вход на eToken с правами администратора)		Установить пароль пользователя

4.5.3 Узел Сертификаты пользователей

Если eToken содержит сертификаты, то узел *Сертификаты пользователей* отображается в левой части окна под узлом *eToken*. Информация о сертификатах пользователей eToken отображается в правой части окна.

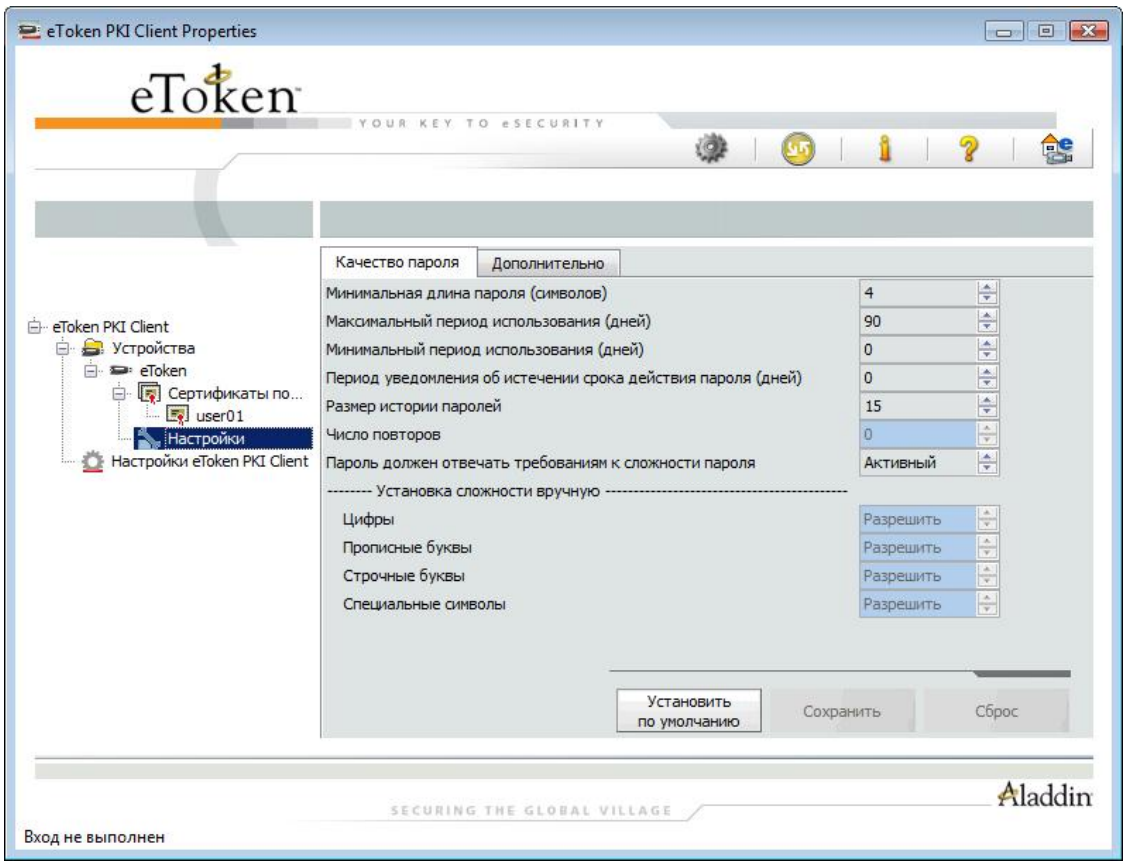


В данном окне доступны следующие функции:

Функция	Значок	Пункт меню
Импорт сертификата См. Импорт сертификатов в память eToken		Импорт сертификата
Экспорт сертификата См. Экспорт сертификатов из памяти eToken		Экспорт сертификата
Удалить сертификат по умолчанию См. Удаление атрибута «по умолчанию»		Удалить сертификат по умолчанию
Удалить сертификат См. Удаление сертификата		Удалить сертификат

4.5.4 Узел Настройки

Настройки подключенных устройств eToken представлены в правой части окна:



Окно узла Настройки содержит две вкладки:

Качество пароля (см. Настройка качества паролей eToken).

Дополнительно, см. Режим кэширования личных данныхи Режим вторичной идентификации с ключом RSA.

4.5.5 Узел Настройки eToken PKI Client

Настройки eToken PKI Client относятся ко всем устройствам eToken, инициализированным после завершения конфигурирования настроек.

Окно узла Настройки eToken PKI Client содержит две вкладки: Качество пароля и Дополнительно.

См. Настройки eToken PKI Client.

5. Инициализация eToken

Процедура инициализации eToken подразумевает форматирование памяти устройства. В ходе этого процесса все созданные на eToken объекты с момента его выпуска удаляются, освобождается память, сбрасывается значение пароля.

Инициализация будет целесообразной, например, в том случае, когда увольняется сотрудник, чтобы этот eToken можно было передать другому сотруднику.

Примечание:

Вы не можете инициализировать eToken Virtual с помощью eToken PKI Client

Краткое содержание главы:

- Общие сведения об инициализации
- Инициализация eToken

5.1. Общие сведения об инициализации

Опция Инициализация eToken восстанавливает значения eToken к исходному виду. В ходе этого процесса все созданные на eToken объекты с момента его выпуска удаляются, освобождается память, сбрасывается значение пароля, что позволяет администратору инициализировать eToken в соответствии со спецификой организации или режимом безопасности.

Инициализация может применяться, например, в том случае, когда увольняется сотрудник. Что позволяет удалить сертификат и личные данные работника из памяти eToken, подготавливая eToken для использования другим сотрудником.

При инициализации могут меняться следующие параметры:

- Имя устройства eToken
- Пароль пользователя
- Пароль администратора
- Максимальное число попыток ошибочного ввода пароля пользователя и администратора
- Требование изменить пароль при первом сеансе авторизации
- Ключ инициализации

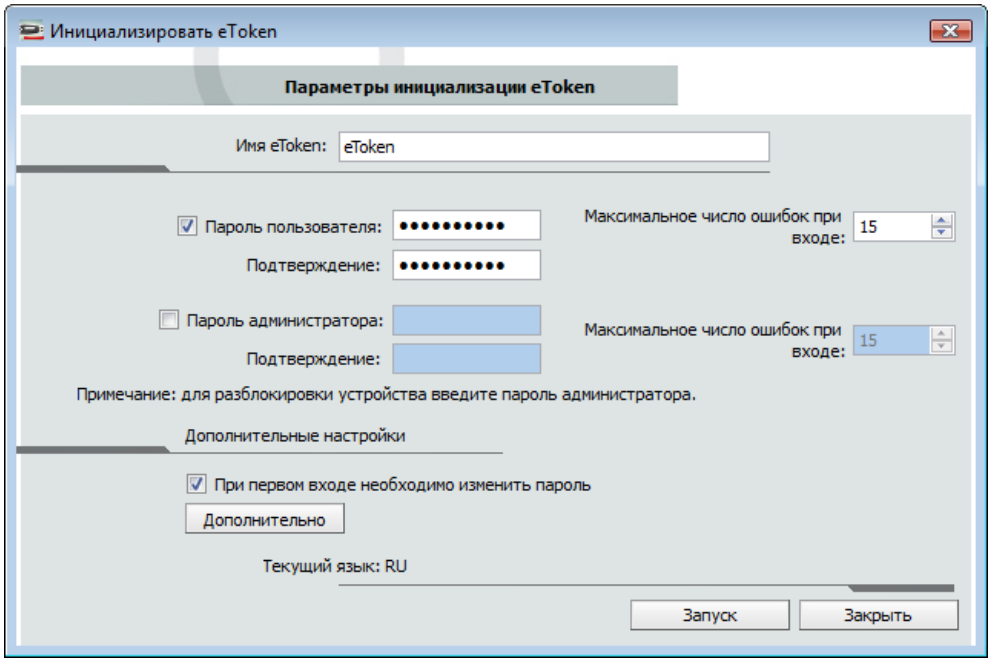
В процессе инициализации файловая система Aladdin eToken загружается на eToken. Используя настраиваемые параметры, Вы можете выбрать параметры, которые будут относиться к конкретному устройству eToken. Данные параметры могут быть необходимы, если Вы хотите использовать eToken для конкретных приложений или, если пароль администратора должен быть установлен на все устройства eToken.

5.2. Инициализация eToken

Для инициализации eToken выполните следующие действия:

1. Нажмите кнопку **Инициализировать eToken** на панели инструментов или щелкните правой кнопкой мыши на имени устройства eToken в левой части окна и выберите функцию **Инициализация** из меню.

   Откроется окно инициализации eToken.



2. Введите имя устройства eToken в поле Имя eToken. Если оставить это поле без изменений, то устройству будет присвоено стандартное имя –eToken.
3. Отметьте **Пароль пользователя** для инициализации eToken с паролем пользователя. Иначе eToken будет инициализирован без пароля, что приведет к невозможности его использования приложениями eToken.
4. Если поле **Пароль пользователя** заполнено автоматически, введите новый пароль пользователя eToken в поле напротив **Пароль пользователя**, **Подтверждение**.

Примечание:

По умолчанию для нового eToken установлен пароль 1234567890. Если Вы хотите использовать пароль и качество пароля пользователя по умолчанию, то снимите отметку напротив пункта **При первом входе необходимо изменить пароль**. Иначе инициализация eToken не удастся, так как пароль пользователя установленный по умолчанию не будет удовлетворять требованиям к качеству пароля (см. Настройка качества паролей). Если отмечен пункт **При первом входе необходимо изменить пароль**, то пользователь сможет ввести свой пароль при следующем входе на eToken. В этом случае пользователю необходимо ввести пароль, удовлетворяющий требованиям к качеству пароля (см. главу Настройки eToken)

5. Для инициализации eToken с паролем администратора, отметьте пункт **Пароль администратора**, и введите в поле напротив пароль администратора. Еще раз введите пароль администратора в поле **Подтверждение** (пароль должен содержать не менее четырех символов).

Примечание:

Создание пароля администратора позволяет выполнять определенные функции на eToken: сброс пароля пользователя на заблокированном eToken.

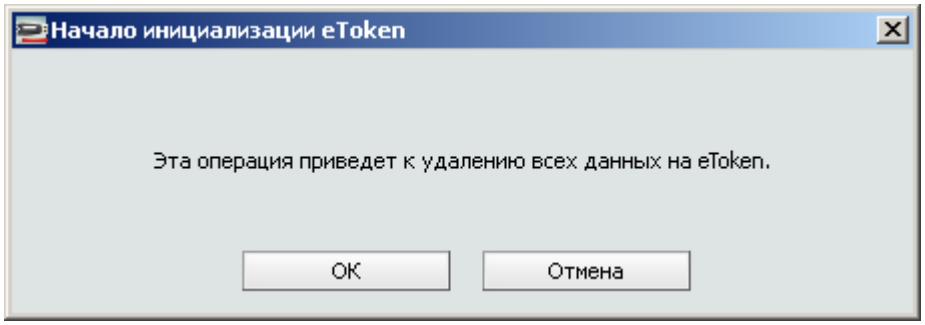
6. В поле **Максимальное число ошибок при входе** введите любое значение в пределах между 1 и 15. Это поле показывает, сколько раз подряд можно вводить неверный пароль пользователя или администратора. При достижении указанного значения счетчика eToken блокируется. Каждый раз после ввода корректного значения счетчик обнуляется. По умолчанию максимальное число попыток неверного ввода пароля равно 15.
7. При необходимости отметьте пункт **При первом входе необходимо изменить пароль**. Этот пункт отмечен по умолчанию.

Примечание:

Если eToken PKI Client был сконфигурирован таким образом, что пароль по умолчанию вводится автоматически при первом входе в систему, то пользователю требуется только ввести и подтвердить новый пароль, не вводя при этом пароль созданный по умолчанию.

8. Если Вы хотите настроить дополнительные параметры, продолжите процедуру инициализации в соответствии с указаниями следующего раздела (см. раздел Настройка дополнительных параметров инициализации), затем нажмите кнопку **ОК** для возврата в окно инициализации eToken.
9. Для начала процесса инициализации нажмите кнопку **Запуск**.

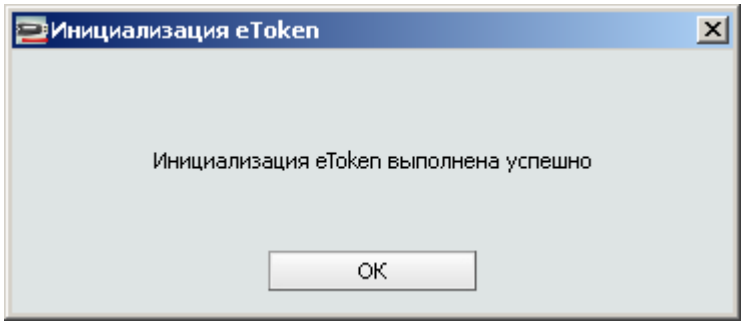
   На экране появится окно с повторным запросом на запуск инициализации.



10. Нажмите **ОК**.

    На экране появится шкала, показывающая степень выполнения процесса.

    По завершению инициализации на экране появится окно с подтверждением.



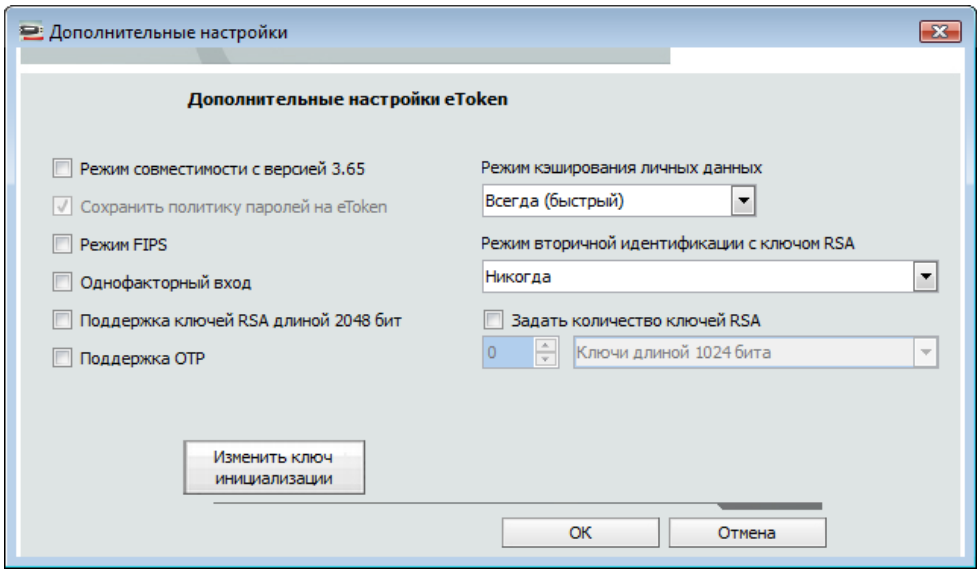
11. Закройте окно нажатием кнопки **ОК**. На этом инициализация eToken завершена.

5.3. Настройка дополнительных параметров инициализации

Для настройки дополнительных параметров выполните следующие действия:

1. В окне инициализации eToken нажмите кнопку **Дополнительно**.

Откроется окно дополнительных настроек eToken.



2. Установите необходимые настройки:

Настройка	Описание
Режим совместимости с версией 3.65	Выберите этот пункт для обеспечения возможности работы инициализированного устройства с eToken RTE 3.65
Сохранить политику паролей на eToken	Выберите этот пункт, если вы хотите хранить настройки качества паролей в памяти eToken
Режим FIPS	Выберите этот пункт для инициализации устройств в режиме соответствия стандарту FIPS. FIPS (Federal Information Processing Standards) – утвержденный правительством США набор стандартов, направленных на улучшение управления и использования компьютерных и телекоммуникационных систем связи. eToken PRO может быть сконфигурирован в соответствии со стандартом FIPS.
Однофакторный ввод	По умолчанию: отключено. При включенной функции однофакторного ввода, для входа в систему требуется только наличие устройства eToken. Пароль при этом не требуется. Примечание: По соображениям безопасности, однофакторный вход не используется в eToken PKI Client Properties
Поддержка ключей RSA длиной 2048 бит	Выберите этот пункт для поддержки 2048-битных ключей RSA (режим доступен не для всех моделей eToken)
Поддержка OTP	Выберите этот пункт для включения поддержки OTP (режим доступен не для всех моделей eToken)
Режим кэширования	В PKI Client в целях более эффективной работы

Настройка	Описание
личных данных	предусмотрено кэширование данных. Данная настройка определяет, когда личная информация (кроме закрытых ключей, аппаратно сгенерированных на eToken PRO/ NG OTP/ Smartcard) может быть кэширования вне памяти устройства eToken Выберите один из следующих вариантов: **Всегда (быстрый)**: режим по умолчанию. Личные данные всегда кэшируются в приложении. Этим ускоряется его работа, так как часть данных сохраняется на локальном компьютере, однако такой механизм менее безопасен, нежели когда данные не кэшируются **При входе пользователя**: данные остаются в КЭШе с момента авторизации с помощью eToken и до момента, пока сеанс авторизации не будет закрыт. После этого все закрытые данные будут удалены из КЭШа **Никогда**: в этом случае данные не кэшируются
Режим вторичной идентификации с ключом RSA	Данная настройка позволяет установить режим задания дополнительного пароля для ключей RSA. Если пароль задан, то помимо обладания собственно eToken и паролем, Вам так же необходимо будет знать пароль данного ключа PSA. Данная настройка определяет политику использования вторичной аутентификации с ключом RSA. **Всегда**: при создании ключа RSA, Вам будет предложено задать дополнительный пароль для доступа к ключу. При нажатии кнопки **ОК** генерируется ключ, введенный пароль используется в качестве дополнительного пароля RSA для этого ключа. Если в отдельном случае Вы этого делать не хотите, достаточно нажать кнопку **Отмена** **Всегда запрашивать у пользователя**: при генерации RSA ключа, каждый раз запрашивается дополнительный пароль RSA для доступа к этому ключу. Однако пользователь может и не задавать дополнительный пароль (нажав кнопку **Отмена**), при этом генерация ключа продолжится без использования дополнительного пароля RSA **Запрашивать по требованию приложения**: в этом режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность (при генерации ключа через Crypto API с флагом *User protected* **Никогда**: В этом режиме пароль для ключа RSA задать нельзя, для доступа к ключу используется пароль eToken
Задать количество ключей RSA	Данная настройка позволяет зарезервировать область памяти eToken под ключи RSA. Никакие другие данные не смогут быть помещены в эту

Настройка	Описание
	область
Изменить ключ инициализации	Ключ инициализации защищает от повторной инициализации и требует задания отдельного пароля до завершения инициализации

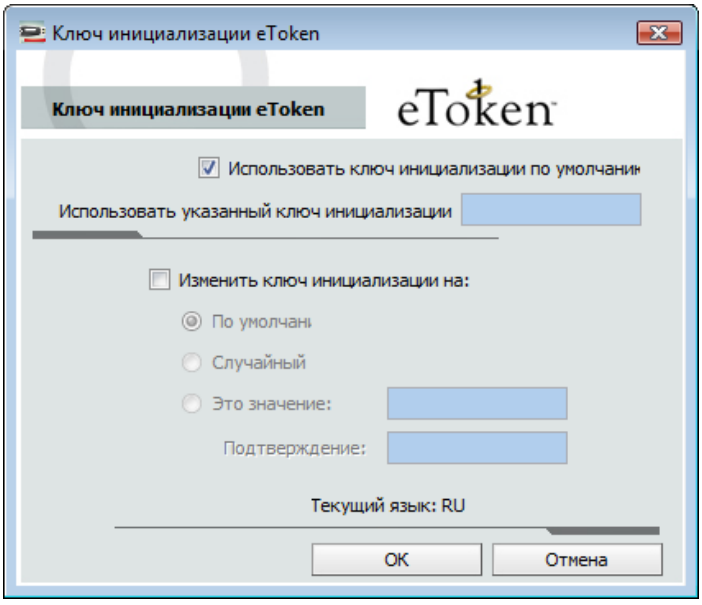
3. Если вы хотите изменить ключ инициализации eToken, выполните необходимые действия, описанные в главе Изменение ключа инициализации.
4. Закройте окно, нажав кнопку OK, и выполните остальные действия так, как описано в предыдущем параграфе.

6. Изменение ключа инициализации

Чтобы изменить ключ инициализации eToken выполните следующие действия:

1. В окне дополнительных настроек eToken нажмите кнопку **Изменить ключ инициализации**.

   Откроется окно ключа инициализации eToken



2. Установите необходимые настройки:

Поле	Описание
Использовать ключ инициализации по умолчанию	Использование стандартного значения ключа инициализации
Использовать указанный ключ инициализации	Введите то значение, которое было установлено в поле **Это значение**
Изменить ключ инициализации на:	**По умолчанию:** восстановить значение по умолчанию **Случайный**: в этом случае повторная инициализация eToken невозможна **Это значение**: введите и подтвердите новый ключ

3. Нажмите кнопку **OK** для возврата к окну дополнительных настроек eToken.

4. Закройте окно, нажав кнопку **OK**, и выполните остальные действия так, как описано в главе Инициализация eToken.

7. Управление устройствами eToken

Данный раздел посвящен описанию функций и настроек eToken.

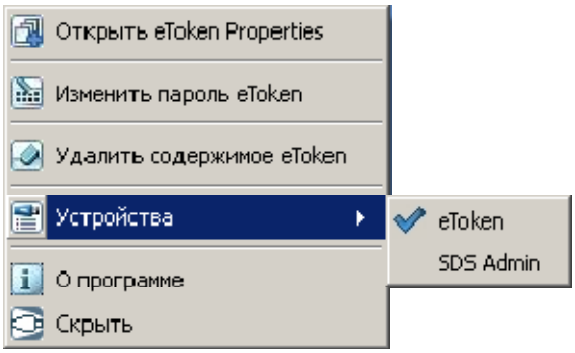
Краткое содержание раздела:

- Выбор активного eToken
- Смена пароля пользователя eToken
- Разблокирование eToken
- Удаление содержимого eToken
- Просмотр данных об устройстве eToken
- Копирование информации об eToken в буфер обмена
- Переименование eToken
- Авторизация в eToken
- Импорт сертификата в память eToken
- Выбор дополнительного сертификата и сертификата, используемого по умолчанию
- Управление считывателями
- Синхронизация паролей

7.1. Выбор активного eToken

Когда подключен не один eToken, а одновременно несколько, нужно выбрать из них тот, с которым будут выполняться все операции. Для этого выполните следующие действия:

1. Щелкните правой кнопкой мыши на значке в области уведомлений. На экране откроется меню eToken PKI Client.



2. Выберите пункт **Устройства** и в открывшемся дополнительном меню выберите то устройство, с которым вы собираетесь работать.

7.2. Смена пароля eToken

Каждое устройство eToken выпускается со стандартным паролем – `1234567890`. В целях

безопасности рекомендуется изменить стандартный пароль сразу после получения eToken.

Ответственность за сохранность пароля всецело лежит на владельце eToken.

Если при инициализации eToken указать пароль администратора, то, в случае забытого или утерянного пароля, можно будет установить новый пароль без потери данных, хранящихся в памяти eToken. Исходя из этих соображений, рекомендуется инициализировать все устройства eToken с указанием пароля администратора.

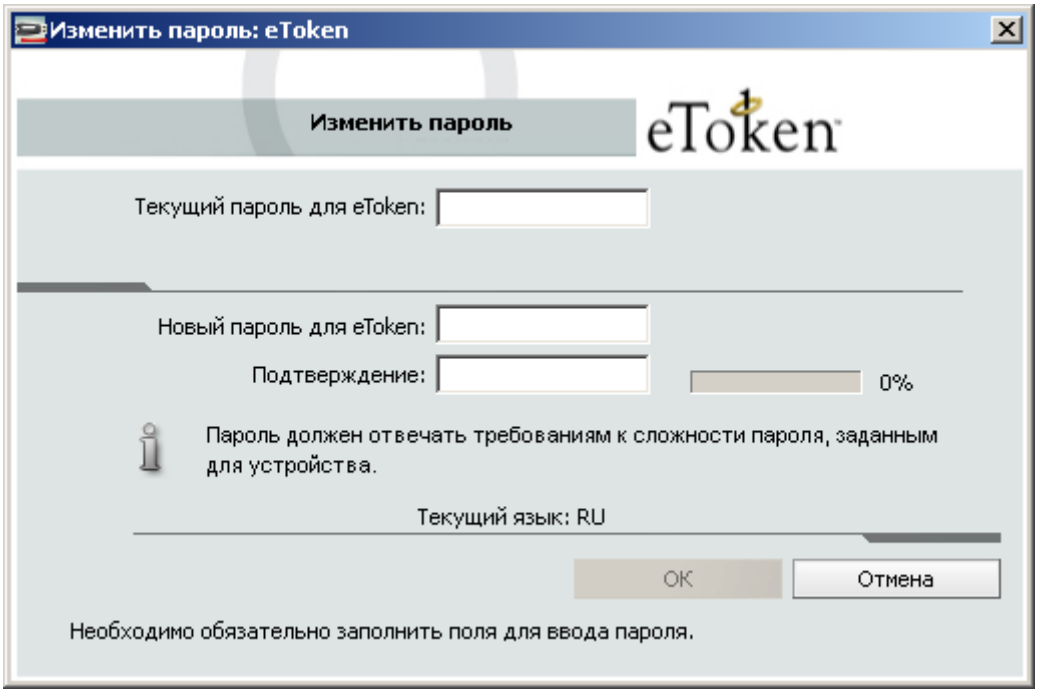
При смене пароля, новое значение должно соответствовать установленным администратором требованиям к качеству паролей. Более подробные сведения о политиках качества паролей изложены далее.

Примечание

От устойчивости и сохранности вашего пароля зависит безопасность данных вашей компании. Именно поэтому важно, чтобы пароль был как можно более надежным. В идеале PIN-код должен быть как минимум восьмизначным и представлять собой последовательность из символов в верхнем и нижнем регистрах, знаков препинания и цифр. Пароль должен быть максимально случайным и не содержать информацию, которую злоумышленник может знать – имя пользователя, дату рождения, номер телефона и т.д.

Для изменения пароля пользователя eToken выполните следующие действия:

1. Запустите утилиту «Свойства eToken» и в правой части окна нажмите кнопку **Сменить пароль**.
2. В открывшемся окне введите текущее значение PIN-кода в поле **Текущий пароль для eToken**.



3. Введите новое значение PIN-кода в полях **Новый пароль для eToken** и **Подтверждение**.

Примечание

По мере того, как вы вводите символы в поле для нового пароля, справа вы увидите шкалу, которая показывает, насколько введенный пароль соответствует установленным критериям качества.

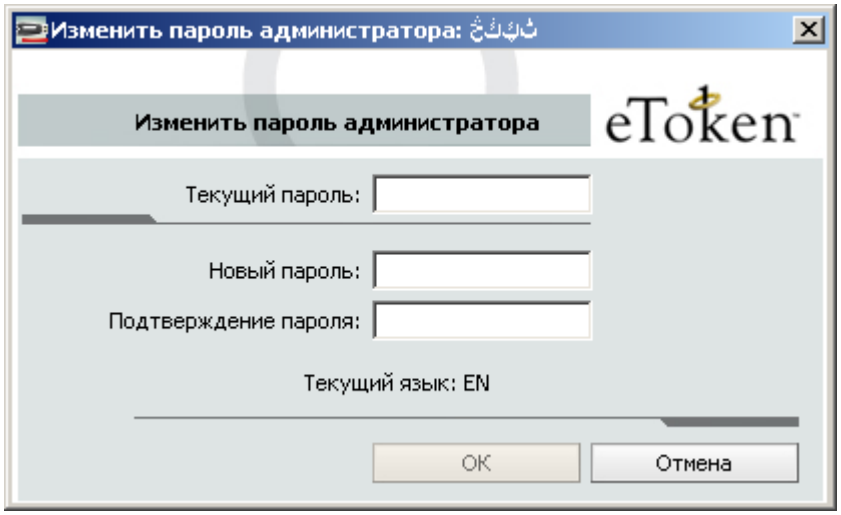
4. Нажмите **OK**. После этого пароль пользователя eToken будет обновлен.

Для изменения пароля администратора eToken выполните следующие действия:

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.

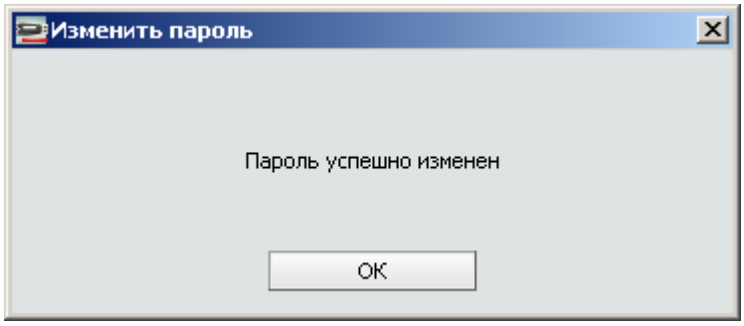
2. В панели меню сверху нажмите кнопку  . Она будет доступной только в том случае, если при инициализации eToken для него был задан пароль администратора.

   На экране откроется следующее окно.



3. Введите текущий пароль администратора в поле **Текущий пароль**.
4. В полях **Новый пароль** и **Подтверждение пароля** введите новый пароль.

   После того как пароль будет изменен, на экране появится окно с подтверждением.



5. Закройте окно, нажав кнопку **OK**.

7.3. Разблокирование eToken

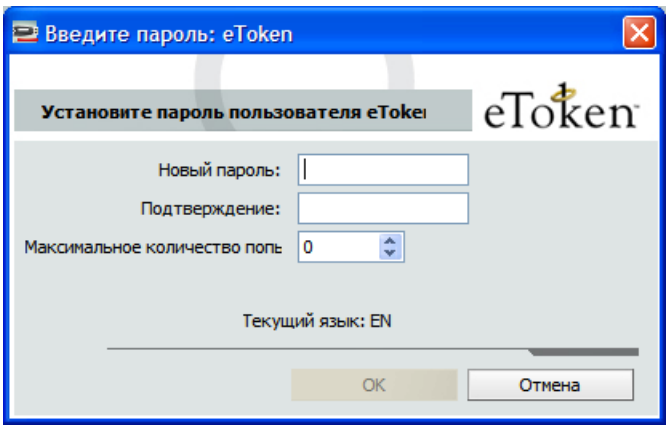
Если при инициализации устройства eToken был указан пароль администратора, это дает возможность разблокировать eToken. Такая необходимость возникает в тех случаях, если пользователь несколько раз подряд введет неправильный пароль.

Существует два способа разблокирования eToken: разблокирование eToken с использованием пароля администратора и разблокирование по схеме «запрос-ответ».

7.3.1 Разблокирование устройства eToken с использованием пароля администратора

1. Авторизуйтесь с правами администратора и щелкните правой кнопкой мыши на имени устройства eToken.

2. Выберите **Назначить пароль**. На экране откроется следующее окно.



3. Введите новый пароль в полях **Новый пароль** и **Подтверждение**:

4. Установите максимальное число последовательных вводов неверного PIN-кода, после которого eToken блокируется, в поле **Максимальное количество попыток.**

5. Нажмите кнопку **OK**. Теперь eToken разблокирован, и пользователь может использовать для авторизации новый пароль.

7.4. Разблокирование eToken по схеме «запрос-ответ»

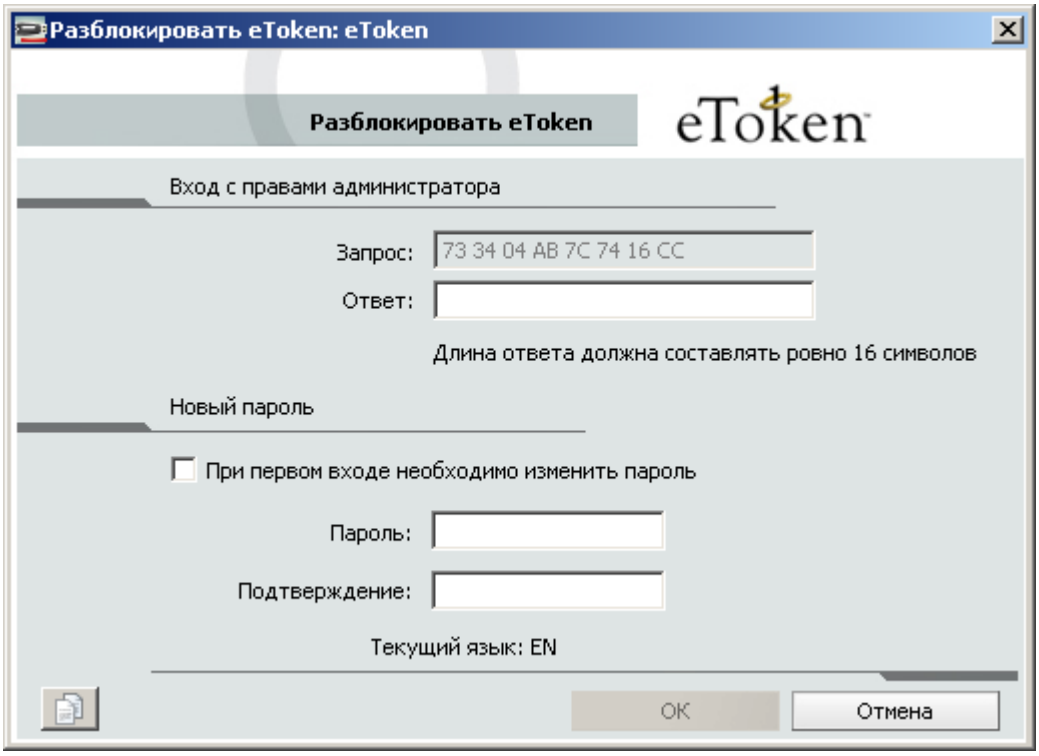
Для использования данной схемы на предприятии должна быть внедрена система централизованного управления eToken TMS версии 2.0 или выше. Заблокированное устройство eToken должно быть зарегистрировано и выпущено средствами системы.

При использовании данной схемы разблокирование устройства происходит удаленно и не требует физического подключения eToken к рабочей станции администратора. Пользователь с помощью утилиты «Свойства eToken» генерирует зашифрованный запрос, содержащий данные о заблокированном eToken, и отправляет его администратору. Администратор с помощью системы eToken TMS генерирует зашифрованный ответ на базе запроса и отправляет его пользователю. Пользователь вводит полученный ответ в утилите «Свойства eToken». В случае ввода корректных данных блокировка eToken снимается.

Важно отметить, что для аппаратных ключей eToken, также как для eToken Virtual, можно задать ограничение по количеству попыток ввода неверного значения пароля, в то время как для eToken Rescue такая возможность исключена.

Для разблокирования eToken по данной схеме необходимо выполнить следующие действия:

1. В правой части главного окна нажмите кнопку **Разблокировать eToken**. На экране появится следующее окно:



2. Свяжитесь с администратора и сообщите ему код из поля **Запрос**.

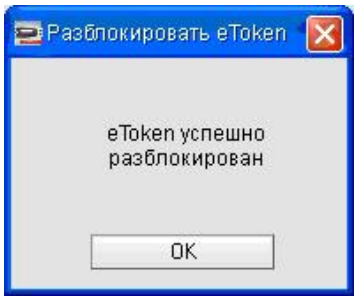
3. На ваш запрос администратор сообщит вам ответную комбинацию, которую нужно ввести в поле **Ответ**.

Примечание:

Генерация ответного кода осуществляется администратором с помощью системы централизованного управления eToken TMS. Процедура описана в документации к системе.

4. Введите новый пароль в поля **Пароль** и **Подтверждение**.

5. После нажатия кнопки **OK** в случае ввода корректного ответа eToken будет разблокирован и на него будет установлен новый PIN-код:



Примечание:

После запроса к администратору **НЕ СЛЕДУЕТ** выполнять никаких действий с устройством eToken до тех пор, пока вы не получите ответный код и не разблокируете eToken.

Несоблюдение этого правила может нарушить условия выполнения схемы «запрос – ответ», и в результате полученный вами код окажется недействительным.

7.5. Удаление содержимого eToken

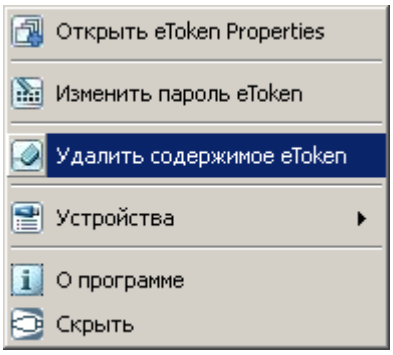
Данная функция позволяет освободить память eToken от всех содержащихся в ней объектов: объектов данных, криптографических ключей и сертификатов – как корневых, так и пользовательских. Данная операция однако не затрагивает объекты, в атрибутах которых установлен запрет на удаление. Для сравнения, процедура инициализации также удаляет все объекты в памяти eToken, однако при этом удаляются сразу все без исключения объекты, и при этом также происходит сброс значения пароля пользователя и также удаление пароля администратора, если этот пароль не задан явно при инициализации.

Примечание

Данная операция не затрагивает данных, сохраненных во Flash-памяти eToken.

Чтобы очистить память eToken, выполните следующие действия:

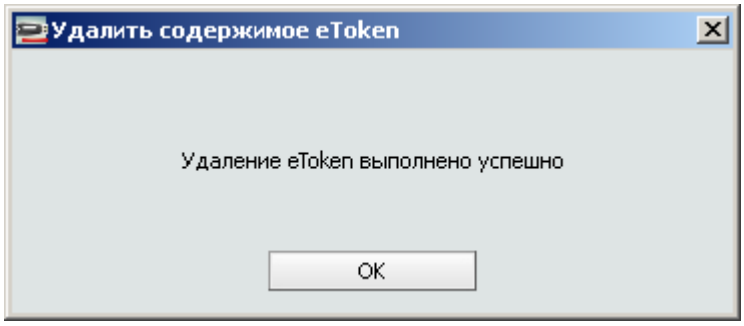
1. Выберите в меню быстрого запуска устройство, с которого вы хотите удалить данные.
2. Откройте меню быстрого вызова и выберите в нем пункт **Удалить содержимое eToken**.



На экране появится окно с предложением подтвердить удаление данных из памяти eToken.

6. Для продолжения нажмите кнопку **OK**.
7. В открывшемся окне введите пароль пользователя eToken и нажмите **OK**.

После того как данные из памяти eToken будут удалены, на экране появится соответствующие сообщения.



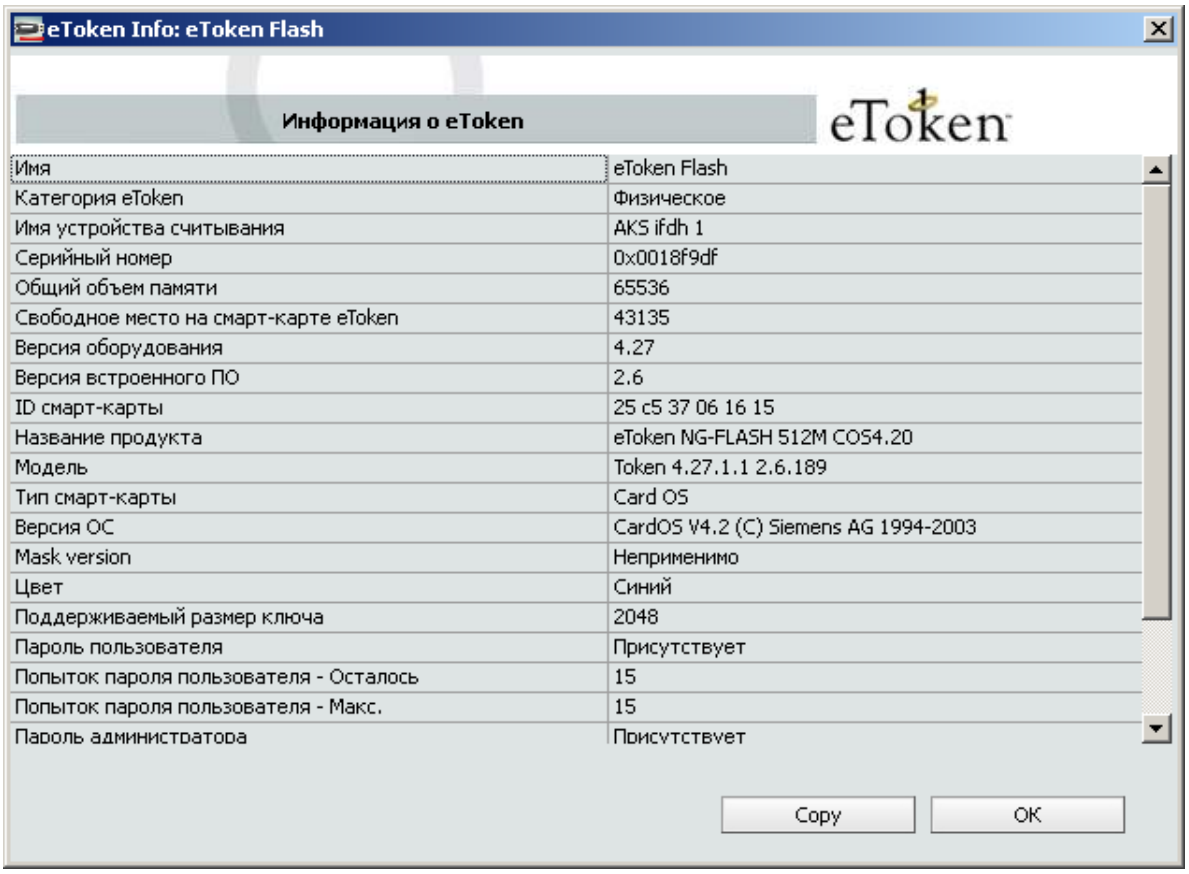
8. Закройте окно, нажав кнопку **OK**.

7.6. Просмотр сведений об eToken

Если вам необходимо просмотреть подробные сведения о подключенном устройстве eToken, то вы их можете просмотреть в утилите eToken Properties. Самый простой способ получить подробную сводку по интересующему устройству выглядит следующим образом:

1. Выберите в главном меню eToken Properties устройство в колонке справа.
2. Нажмите справа на кнопку **Просмотр данных о eToken**.

На экране появится окно следующего вида.



Если вы хотите скопировать все данные по устройству в буфер обмена, нажмите кнопку **Copy**.

9. После просмотра закройте окно, нажав кнопку **OK**.

Те же сведения вы можете просмотреть и скопировать в буфер обмена, выбрав необходимое устройство в расширенном режиме и нажав кнопку  .

7.7. Переименование eToken

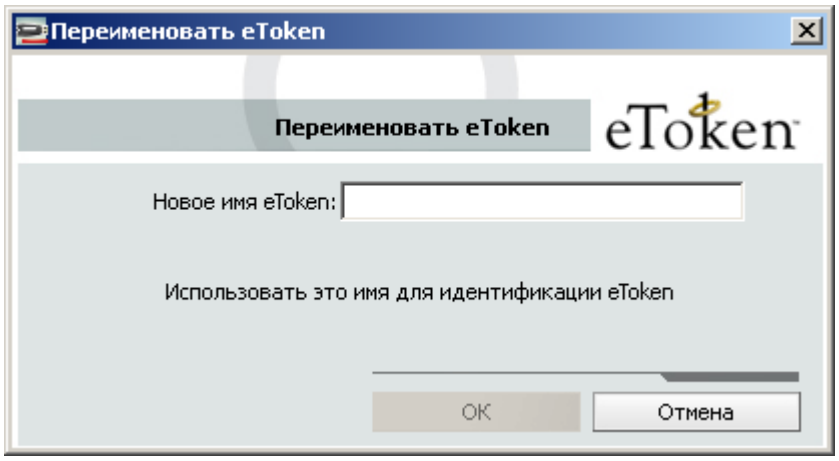
Для удобства различия устройств между собой имеет смысл сменить стандартное имя («eToken») на другое. Например, вы можете указать в имени инициалы пользователя или кратко указать область применения данного eToken.

Чтобы задать новое имя для eToken, выполните следующие действия:

1. В главном меню выберите то устройство, которое вы хотите переименовать.
2. В правой части окна нажмите кнопку **Переименовать eToken**. На экране появится окно авторизации.

3. В открывшемся окне введите пароль eToken и нажмите **OK**.

   На экране появится новое окно следующего вида:



4. Введите новое имя eToken, используя любые комбинации букв, цифр и специальных символов, и нажмите **OK**.

   Введенное имя сразу появится рядом со значком eToken в левой колонке.

Однако в меню быстрого запуска оно изменится только после повторного подключения устройства.

7.8. Режимы работы eToken

eToken предусматривает работу в двух режимах: в режиме пользователя и в режиме администратора. Основным режимом является режим пользователя, а режим администратора является второстепенным и возможен только в том случае, если при инициализации eToken был задан пароль администратора. Административные полномочия ограничены до изменения пароля администратора, задания значения пароля пользователя eToken, разблокирования eToken по схеме «запрос-ответ» и изменением требований к качеству паролей.

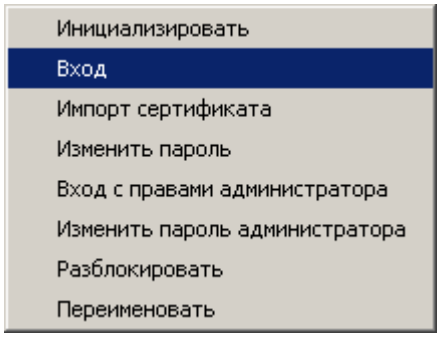
Без авторизации единственной функцией, доступной в eToken Properties, остается просмотр сведений об eToken.

7.9. Авторизация в режиме пользователя

При выполнении большинства функций в eToken Properties требуется авторизация пользователя. Такими функциями, например, являются Переименование eToken, изменение пароля пользователя, удаление содержимого из памяти eToken, импорт сертификатов и др.

Вместо того чтобы вводить пароль для каждой такой операции, удобнее выполнить авторизацию один раз. Процедура выглядит так:

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. Щелкните правой кнопкой мыши на устройстве в дереве слева и в открывшемся контекстном меню выберите пункт **Вход**.



3. В открывшемся окне введите пароль пользователя и нажмите **OK**.

Примечание:

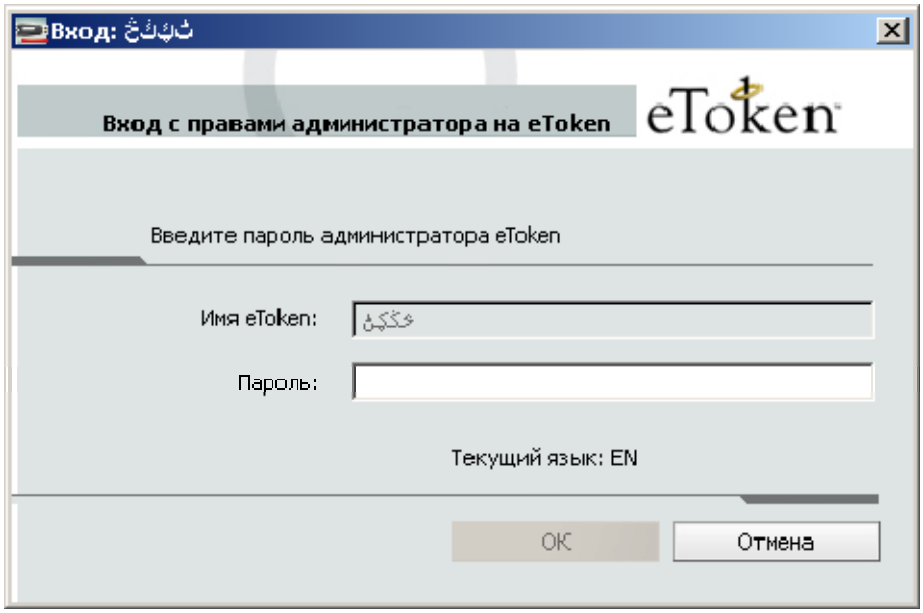
Длительность действия пароля с момента авторизации может быть ограничена в настройках eToken PKI Client. В таком случае по истечению определенного промежутка времени вам будет предложено ввести пароль снова при выполнении той или иной операции, требующей авторизации пользователя.

Для выхода из режима пользователя нажмите в расширенном режиме кнопку  или отключите eToken.

7.10. Авторизация в режиме администратора

Для доступа к административным функциям выполните следующие действия.

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. Выберите в дереве слева то устройство, на котором вы хотите выполнить авторизацию.
3. Нажмите кнопку  . Эта кнопка будет доступна только в том случае, если при инициализации eToken был задан пароль администратора.
4. В открывшемся окне введите пароль администратора и нажмите **OK**.



5. Для выхода из режима пользователя нажмите в расширенном режиме кнопку  справа или отключите eToken.

7.11. Импорт сертификатов в память eToken

В eToken PKI Client 5.1 SP1 имеется поддержка следующих форматов файлов сертификатов.

- PFX.
- P12.
- CER.

Если вы выбрали файл PFX, то закрытый ключ, соответствующий сертификат и сертификаты УЦ (если таковые имеются) будут скопированы на eToken. Если файл PFX защищен паролем, вам будет предложено ввести его.

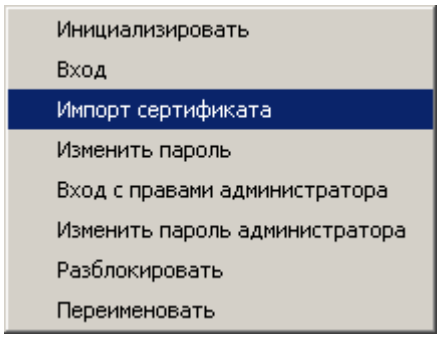
В случае с файлом CER (который содержит сертификаты X.509), программа проверяет, есть ли на eToken закрытый ключ, соответствующий данному сертификату.

Если закрытый ключ действительно есть, импортируемый сертификат будет связан с данным ключом. Если закрытый ключ не найден, вам будет предложено сохранить сертификат как сертификат УЦ. Ответив на запрос положительно, вы тем самым сможете сохранить сертификат.

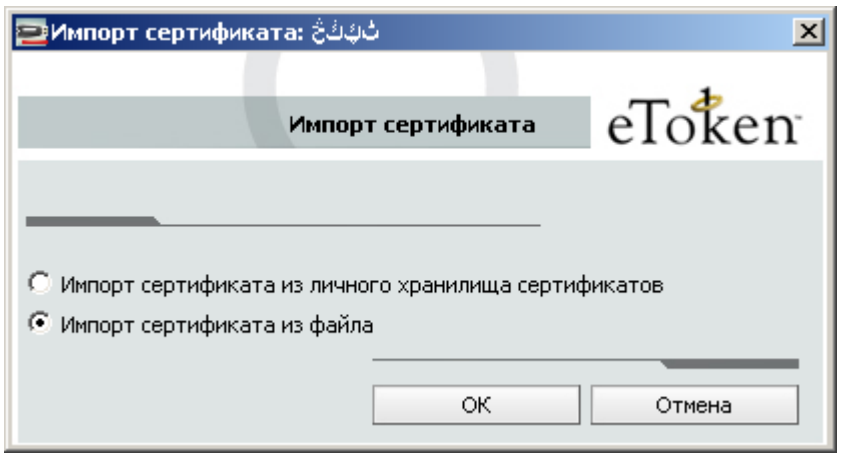
Для шифрования и использования цифровой подписи в электронных сообщениях после загрузки сертификата на компьютер и импортирования его на eToken, необходимо сначала удалить сертификат из локального хранилища, а затем повторно подключить eToken. Соблюдение этого условия гарантирует, что вы будете использовать именно те сертификаты и ключи, которые хранятся на eToken, а не в локальном хранилище компьютера.

Чтобы импортировать сертификат, выполните следующие действия:

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева щелкните правой кнопкой на устройстве, куда вы хотите импортировать сертификат и в открывшемся контекстном меню выберите пункт **Импорт сертификата**.



3. В открывшемся окне выберите место, где хранится сертификат – личное хранилище или файл – и нажмите **OK**.



Если вы указали в окне выше личное хранилище сертификатов, на экране откроется следующее окно со списком сертификатов, доступных для импорта из личного хранилища. Такими сертификатами могут быть:

- **Сертификаты, которым соответствует ключевая пара в памяти eToken**. Такая ситуация возможна в случае, если для выдачи сертификата на ЦС требуется подтверждение администратора. Тогда если на eToken сгенерирована ключевая пара, соответствующий ей сертификат можно импортировать позднее, выбрав пункт «Импорт сертификата из личного хранилища».
- **Сертификаты, которые изначально были созданы вместе с ключевой парой не на eToken, и имеющие необходимые атрибуты для экспорта**.

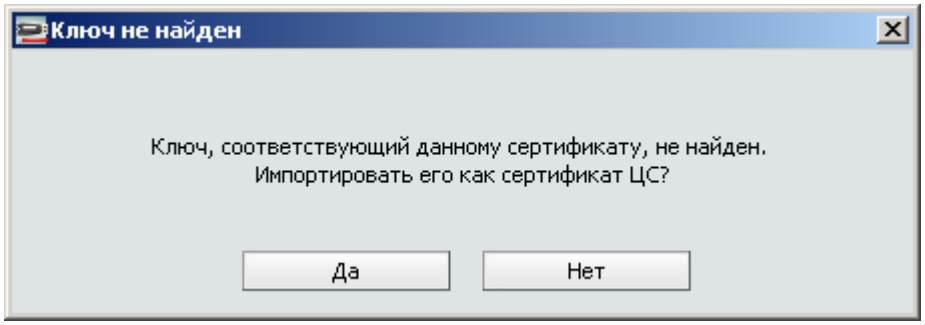
Если сертификат хранится во внешнем файле, то далее после нажатия кнопки **OK** вам будет предложено указать путь к этому файлу.

Если сертификат защищен паролем, появится соответствующее окно:

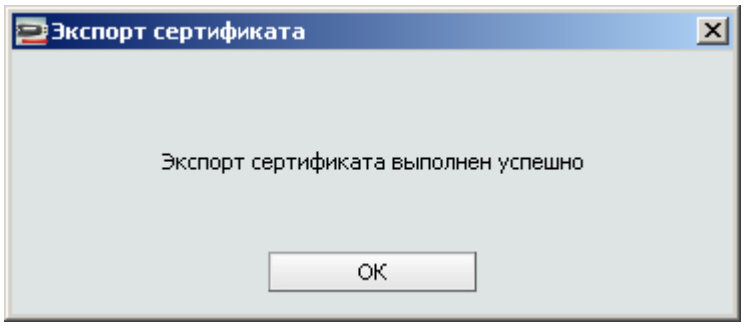
4. Введите пароль и нажмите **OK**.

Далее вам будет предложено сохранить все сертификаты данного ЦС в памяти eToken.

Если данному сертификату не будет найдено соответствующего закрытого ключа, на экране появится следующее сообщение.



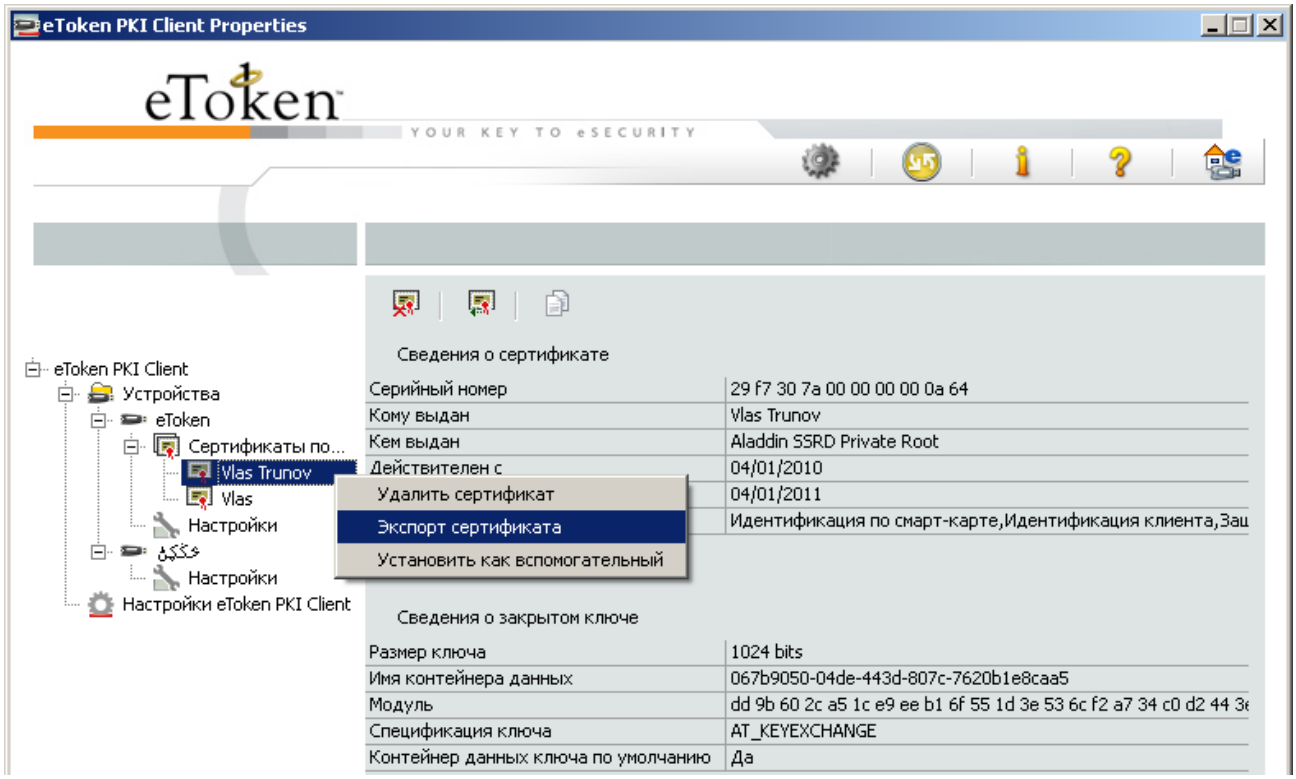
5. Нажмите **Да** или **Нет**.
6. После того как сертификат (или все сертификаты цепочки) будут импортированы, на экране появится окно с соответствующим подтверждением.



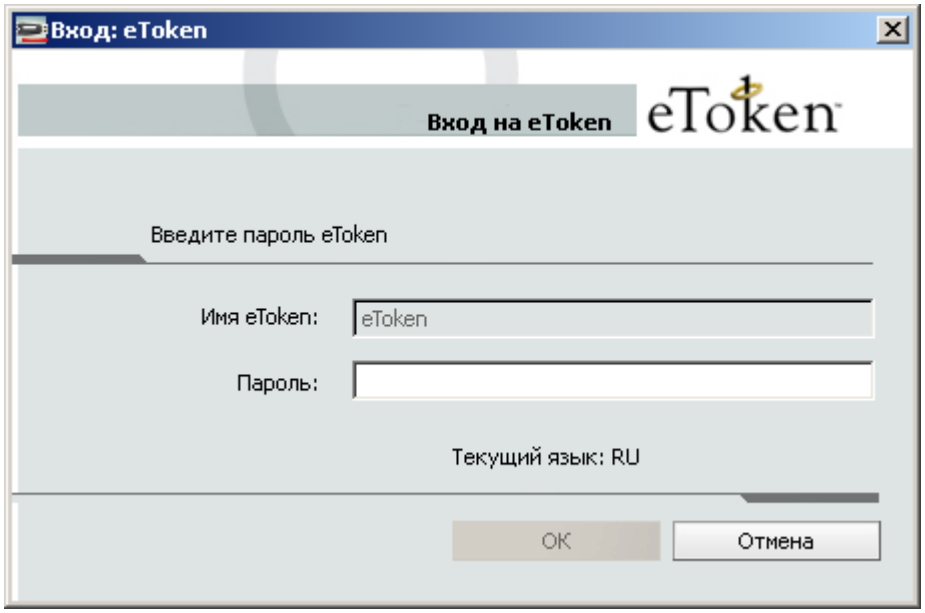
7.12. Экспорт сертификата с eToken

В случае с аппаратным eToken экспортируется только сертификат, тогда как в случае с eToken Virtual экспортируется сертификат вместе с закрытым ключом.

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева разверните ветвь устройства, на котором содержится сертификат, и щелкните правой кнопкой на сертификате, который вы хотите экспортировать.

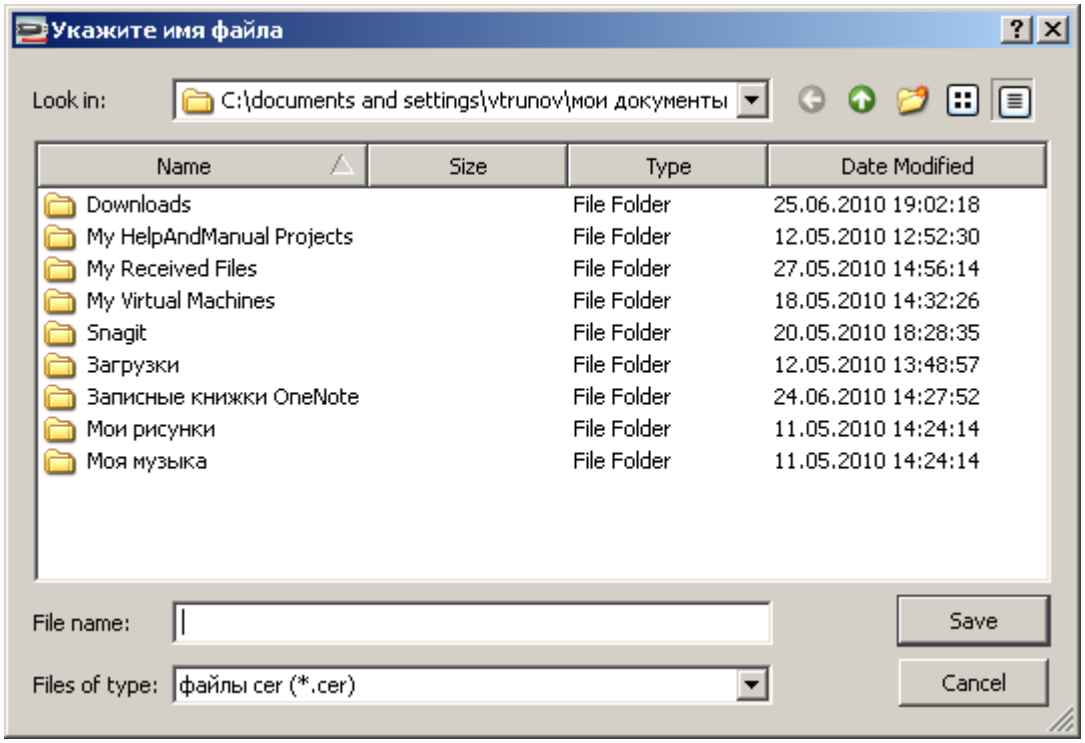


3. В открывшемся контекстном меню выберите пункт **Экспорт сертификата**. Вы увидите следующее окно:



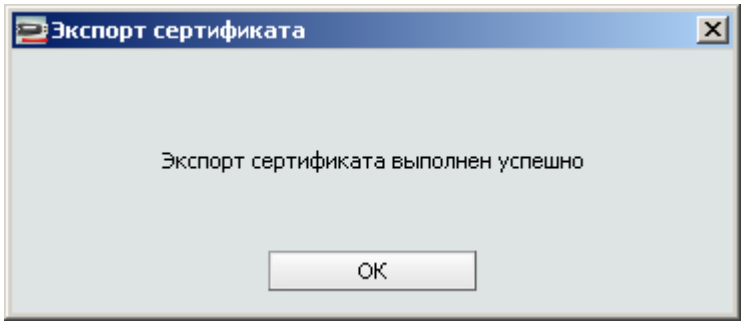
4. Выполните авторизацию, указав пароль пользователя eToken и нажав **OK**.

   На экране появится меню следующего вида.



5. Укажите имя и путь, по которому будет сохранен экспортированный сертификат, и нажмите **Save**.

   В подтверждение успешного завершения операции появится соответствующее сообщение.



6. Закройте окно, нажав кнопку **OK**.

Примечание:

Сертификат должен быть представлен в кодировке DER или в Base64 (но не в формате PKCS #7).

7.13. Определение для сертификата свойств «основной» или «вспомогательный»

В некоторых приложениях, использующих протокол CAPI, в явном виде не указывается, какой именно требуется сертификат (например, в клиенте для Microsoft VPN). При этом используется сертификат, заданный по умолчанию. Для указания одного из хранящихся в памяти eToken сертификатов, как сертификата по умолчанию, нажмите правой кнопкой мыши на соответствующем узле и выберите **По умолчанию**. Если сертификат по умолчанию явно не задан, то таковым считается первый сертификат, записанный в память eToken после инициализации.

Установка того или другого атрибута может быть недоступна для конкретного сертификата или ключа.

Пояснение к атрибутам представлено в следующей таблице.

Атрибут	Описание	Типовой сценарий
По умолчанию	При авторизации в системе по смарт-карте по умолчанию используется тот же сертификат, который использовался в предыдущий раз. Если вместо него нужен другой сертификат, то для такого сертификата необходимо установить атрибут «по умолчанию».	На вашем eToken есть два сертификата: один для доступа в домен А, а другой – в домен Б. В прошлый раз вы авторизовались в домене А, то есть в данный момент у вас по умолчанию используется первый сертификат – для доступа в домен А. Если же вы хотите после этого войти в домен Б с другого компьютера, аутентификация будет завершена с ошибкой, поскольку по умолчанию используется именно сертификат для доступа к домену А. Поэтому, чтобы войти в домен Б, вам нужно будет установить для второго сертификата атрибут «по умолчанию».
Вспомогательный	Во многих приложениях Microsoft используется механизм аутентификации по смарт-карте. Однако есть некоторые приложения, которые используют механизм аутентификации слиента. Он предоставляет более ограниченный доступ к ресурсам, нежели Smart Card Logon. Среди возможных применений этого механизма – доступ к VPN-сетям, и eToken PKI Client дает такую возможность, но если в eToken хранятся не один, а несколько сертификатов, предназначенных для аутентификации клиента, то из них нужно выбрать только один, задав для него атрибут «вспомогательный».	На вашем eToken есть сертификат, который используется для доступа к VPN-сети, но кроме него есть еще один сертификат, для которого при выпуске была задана возможность использования для аутентификации клиента. В этом случае для первого сертификата нужно установить атрибут «вспомогательный», и тогда аутентификация в VPN-сети будет выполняться корректно.

Чтобы установить для сертификата атрибут «по умолчанию» или «вспомогательный», выполните следующие действия:

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева разверните ветвь устройства, на котором содержится сертификат, и щелкните на нем правой кнопкой мыши.
3. В открывшемся контекстном меню выберите пункт **Установить как вспомогательный** или **Установить по умолчанию**.

Единовременно любой из этих атрибутов может иметь только один сертификат на eToken. Соответственно, если сертификат уже установлен как используемый по умолчанию, то соответствующий пункт контекстного меню будет отсутствовать. То же справедливо и для атрибута «вспомогательный».

7.14. Удаление атрибута «по умолчанию»

Если в eToken есть сертификат, для которого вы ранее задали атрибут «по умолчанию», и вместо него вы хотите использовать другой сертификат, достаточно выполнить для него те же действия, которые были описаны в предыдущем пункте. Если же вы просто хотите снять атрибут «по умолчанию», выполните следующие действия.

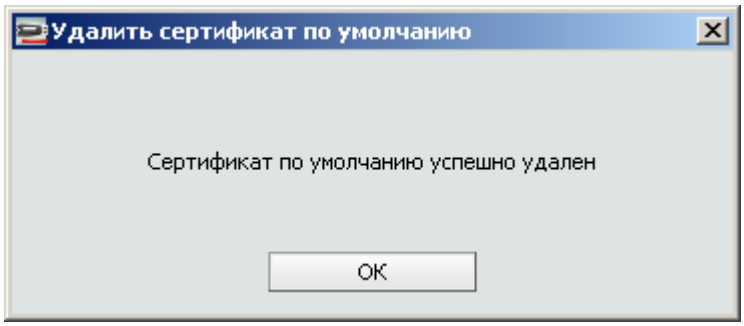
1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева разверните ветвь **Устройства** и затем выберите необходимое устройство, на котором находится сертификат.

3. Выделите пункт **Сертификаты пользователей**.

4. Выберите справа сертификат с атрибутом «по умолчанию».

5. Нажмите кнопку  вверху.

   На экране появится окно со следующим сообщением.

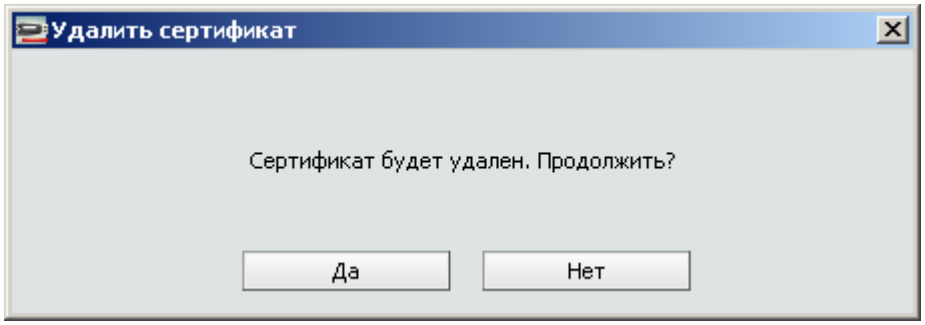


6. Закройте окно, нажав кнопку **OK**.

7.15. Удаление сертификата

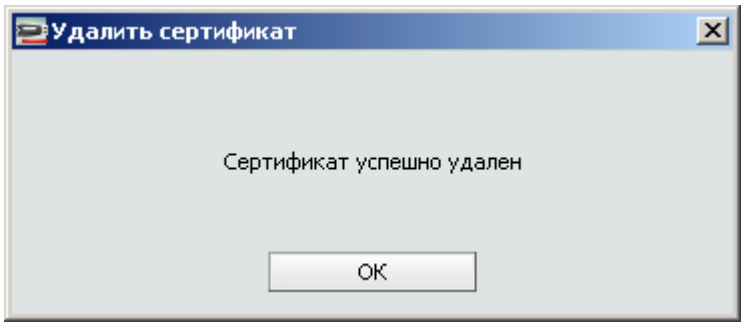
Чтобы удалить сертификат из памяти eToken, выполните следующие действия.

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева разверните ветвь **Устройства** и затем выберите устройство, содержащее сертификат, который вы хотите удалить.
3. Щелкните правой кнопкой мыши на узле, соответствующем нужному сертификату, и выберите **Удалить сертификат**. После этого на экране появится следующее окно.



4. Нажмите **Да**.

   После того как сертификат будет удален, на экране появится окно с подтверждением.



5. Закройте окно, нажав кнопку **OK**.

7.16. Управление считывателями

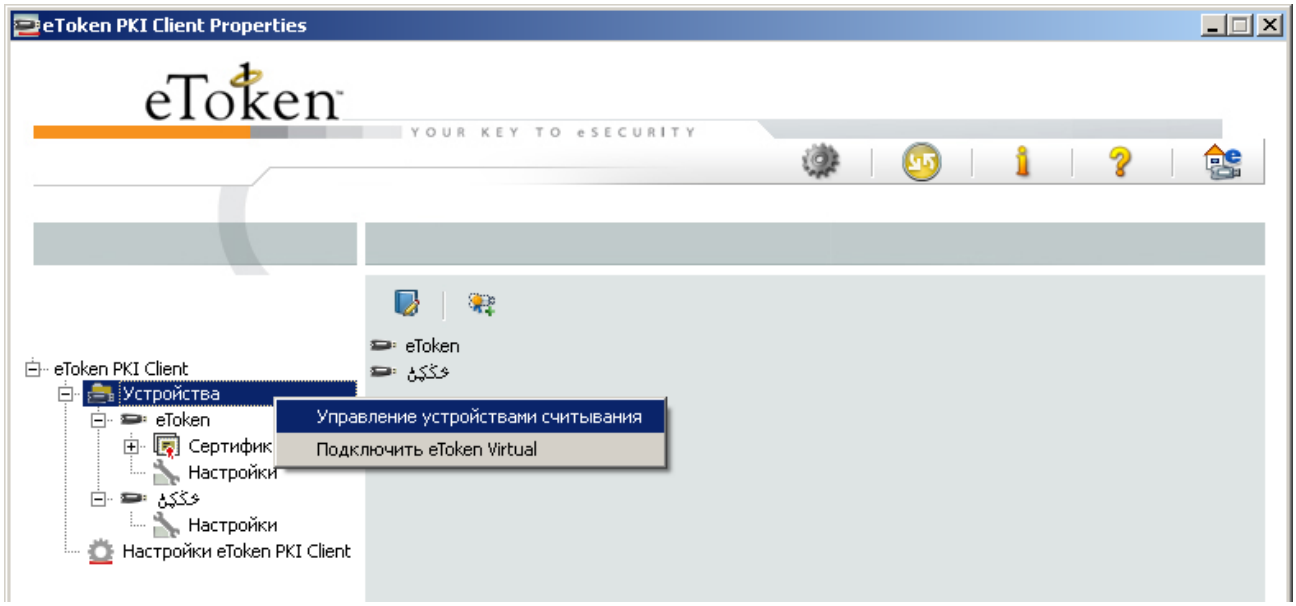
В исходной конфигурации утилиты eToken Properties предусмотрены два виртуальных считывателя для аппаратных устройств eToken и один – для eToken Virtual.

Количество занятых считывателей уменьшается каждый раз при подключении подключении USB-ключа или смарт-карты eToken или при подключении eToken Virtual.

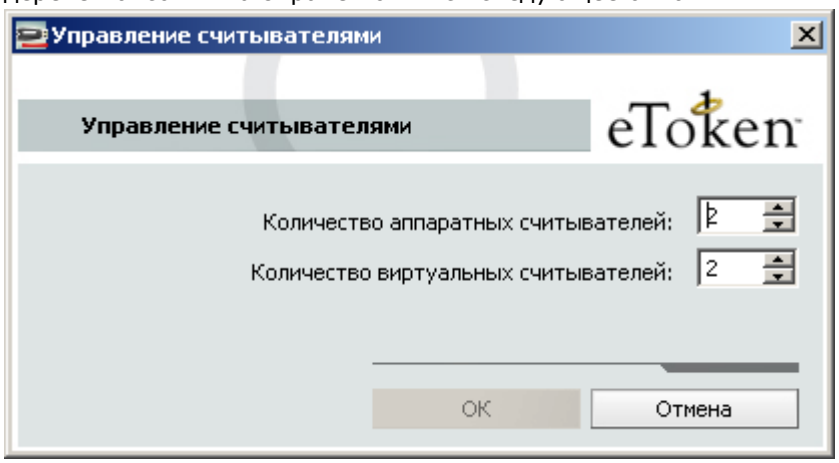
При наличии прав локального администратора, пользователь может вручную задать необходимое число виртуальных считывателей.

Для изменения количества считывателей выполните следующие действия:

1. Перейдите в расширенный режим, нажав кнопку  в главном окне.
2. В дереве слева щелкните правой кнопкой мыши в пункте **Устройства**.
3. В открывшемся контекстном меню выберите пункт **Управление устройствами считывания**.



4. Выберите пункт **Считыватели** на панели инструментов или **Управление считывателями** через контекстное меню, которое открывается правым щелчком в дереве консоли. На экране появится следующее окно:

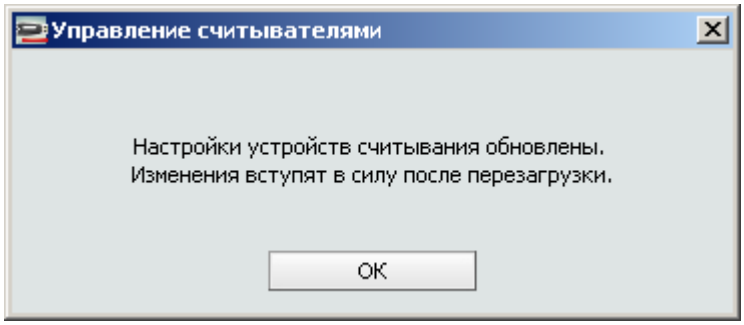


5. Установите количество считывателей для программных и аппаратных устройств в соответствующих полях.

   По умолчанию эти поля имеют следующие значения:

   - Количество аппаратных считывателей: 2
   - Количество виртуальных считывателей: 1

6. Закройте окно, нажав кнопку **OK**. После изменения количества считывателей необходимо перезапустить компьютер, чтобы изменения вступили в силу. Об этом будет дополнительно сообщено в отдельном окне:



7.17. Синхронизация пароля eToken и пароля для доступа к домену

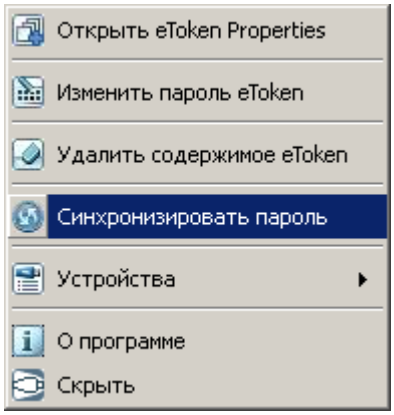
В eToken PKI Client предусмотрена возможность синхронизации пароля пользователя eToken и пароля для доступа к домену. Соответствующий пункт меню доступен только в том случае, если он был задан в настройках eToken PKI Client.

Синхронизация предполагает изменение пароля для доступа к домену в соответствии с заданным паролем пользователя eToken. При этом также контролируется, чтобы пароль пользователя удовлетворял требованиям к качеству паролей – как для домена, так и для eToken.

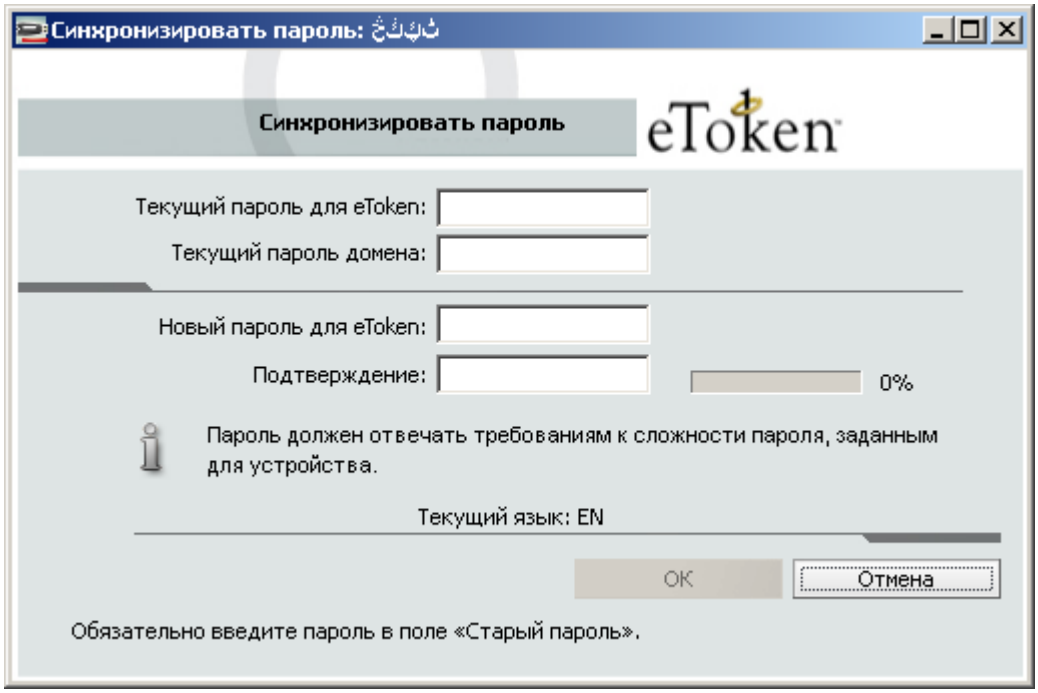
Для синхронизации паролей необходимо, чтобы домен заданный в настройках eToken PKI Client был доступен.

Чтобы синхронизовать пароли eToken и домена, выполните следующие действия:

1. Откройте меню быстрого запуска, щелкнув на значке  в области уведомлений.
2. В открывшемся меню выберите пункт **Синхронизовать пароль** так, как показано на следующем рисунке.



На экране откроется следующее окно.



3. В первом поле сверху введите текущий пароль пользователя eToken.
4. В поле **Текущий пароль** домена введите пароля для доступа к домену.
5. В полях **Новый пароль для eToken** и **Подтверждение** введите пароль, который будет использоваться для доступа к eToken и домену.

Примечание

По мере того, как вы вводите символы в поле для нового пароля, справа вы увидите шкалу, которая показывает, насколько введенный пароль соответствует установленным критериям качества.

6. Нажмите **OK**. После этого пароль пользователя eToken будет обновлен.

8. Работа с eToken Virtual

eToken PKI Client, поддерживает все типы виртуальных аналогов eToken, а именно eToken Virtual, eToken Virtual Temp и eToken Rescue. Они могут храниться на жестком диске или на внешнем носителе. Основное предназначение виртуального eToken – замена утерянного USB-ключа или смарт-карты в случае, когда пользователь находится вне офиса, т.е. тогда, когда выдать ему новое аппаратное устройство не представляется возможным.

8.1. Общие сведения об eToken Virtual и eToken Rescue

Существует три типа eToken, которые заменяют собой аппаратные USB-ключи и смарт-карты.

- **eToken Rescue**: этот ключ призван решить проблемы, связанные с утерей eToken или выходом из его строя в то время, пока сотрудник находится за пределами офиса. eToken Rescue предназначен только для чтения, то есть в отличие от своего аппаратного аналога в него никаких сертификатов записать нельзя. Кроме того, данный тип ключа отличает ограниченный срок действия.

- **eToken Virtual**: имеет тот же функционал, что и eToken NG-OTP. В нем можно хранить те же данные, в т.ч. профили eToken Single Sign-On, ключевые пары и сертификаты. eToken Virtual имеет привязку к определенному компьютеру или носителю, то есть это значит, что его нельзя копировать и использовать на каком-либо другом компьютере.

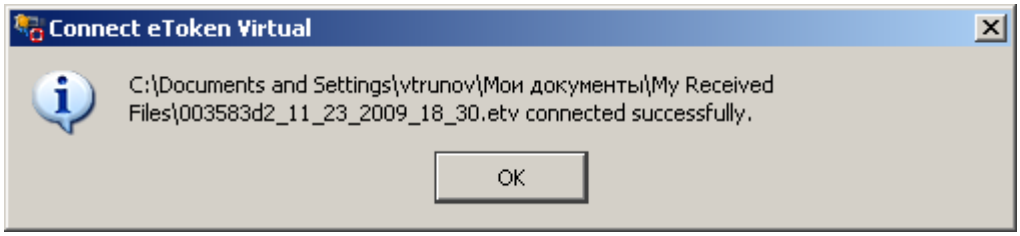
Примечание

Возможность выработки одноразовых паролей может быть ограничена настройками eToken PKI Client.

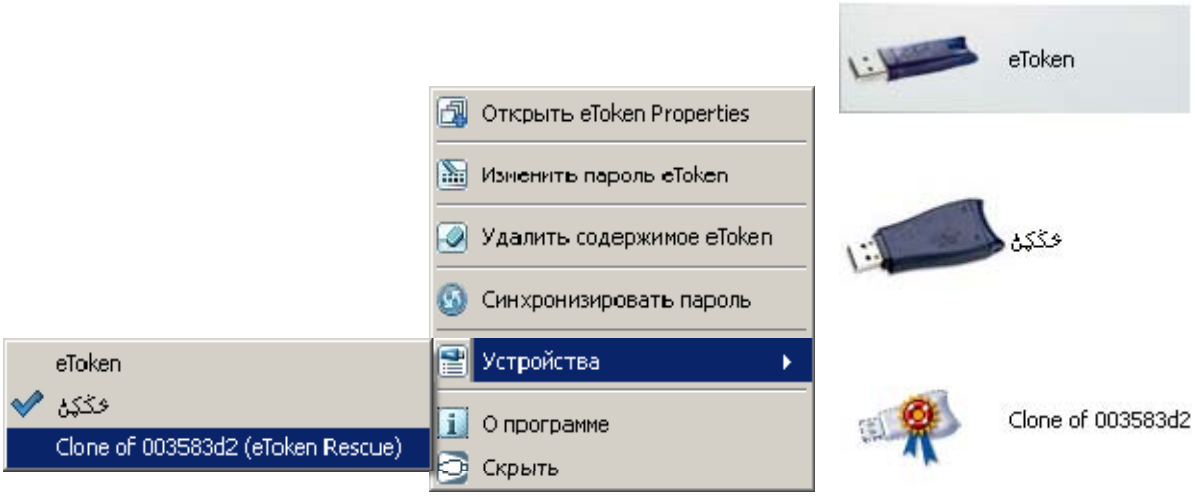
- **eToken Virtual Temp**: этот тип ключа отличается от eToken Virtual тем, что содержит сертификаты с ограниченным сроком действия.

8.2. Подключение eToken Virtual или eToken Rescue

Чтобы подключить eToken Virtual или eToken Rescue, запустите файл с расширением .etv. После этого на экране должно появиться соответствующее подтверждение.



При этом вы увидите имя eToken в главном окне утилиты eToken Properties и в меню быстрого запуска.

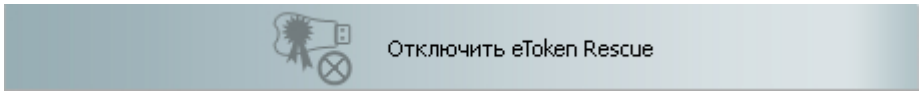


8.3. Отключение или удаление eToken Virtual или eToken Rescue

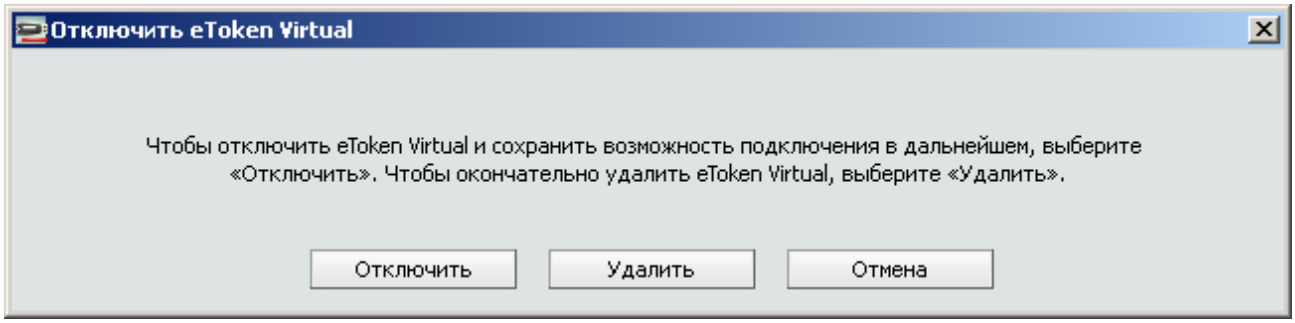
Если вы не собираетесь пользоваться eToken Virtual в течение некоторого времени, вы можете отключить его и подключить позднее, выполнив действия, описанные в предыдущем пункте. Если же вы совсем не собираетесь пользоваться данным ключом или срок его действия истек, вы можете также удалить сам файл. Кроме того, в тех случаях когда eToken Rescue был выпущен как замена утраченному аппаратному eToken, после выдачи пользователю нового USB-ключа или смарт-карты необходимо не только отключить, но и удалить eToken Rescue.

Чтобы отключить и/или удалить eToken Virtual, выполните следующие действия:

1. В главном окне утилиты eToken Properties выберите в колонке слева тот eToken, который вы хотите отключить.
2. Нажмите кнопку Отключить eToken Rescue.

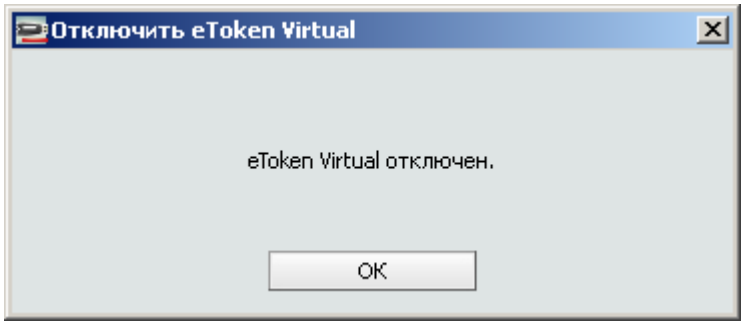


На экране появится окно с предложением отключить или удалить eToken.



3. Выберите необходимое действие, нажав соответственно кнопку **Отключить** или **Удалить**.

   После того как eToken будет отключен или удален, на экране появится соответствующее подтверждение.



4. Закройте окно, нажав кнопку **OK**.

8.4. Выпуск eToken Virtual/eToken Virtual в качестве замены утраченному аппаратному eToken

Для выпуска eToken Virtual и eToken Rescue в организации должна быть установлена система eToken TMS. Общую информацию и документацию по этой системе вы можете найти Раздел TMS на сайте Aladdin.

8.5. Разблокирование eToken Virtual

При достижении определенного ограничения по количеству последовательно введенных ошибочных значений пароля пользователя, eToken Virtual блокируется. Чтобы разблокировать его, выполните действия, описанные в главе Разблокирование eToken по схеме «запрос-ответ».

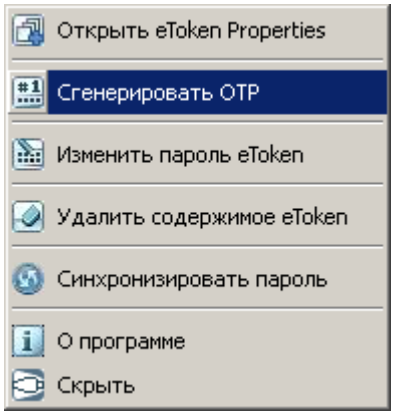
Важно отметить, что для аппаратных ключей eToken, также как для eToken Virtual, можно задать ограничение по количеству попыток ввода неверного значения пароля, в то время как для eToken Rescue такая возможность исключена.

8.6. Выработка одноразовых паролей

Данный пункт относится только к ключам eToken Virtual и eToken Rescue, для которых при выпуске была задана возможность выработки одноразовых паролей.

Для выработки одноразового пароля выполните следующие действия:

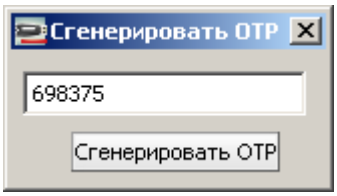
1. Щелкните правой кнопкой на значке  в области уведомлений.
2. Выберите пункт **Сгенерировать OTP**.



На экране появится окно с единственным полем для вывода одноразовых паролей.

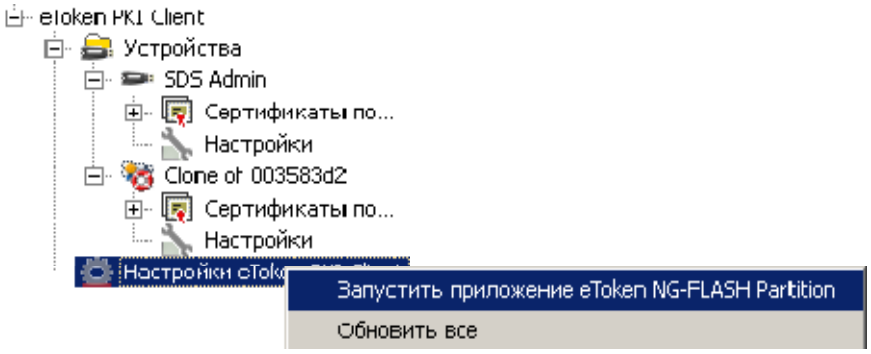
Если вы подключили eToken Virtual / eToken Rescue первый раз, то на экране может появиться окно, где вам будет предложено сменить установленный по умолчанию пароль пользователя.

5. Нажмите кнопку Сгенерировать OTP, и вы увидите значение одноразового пароля.

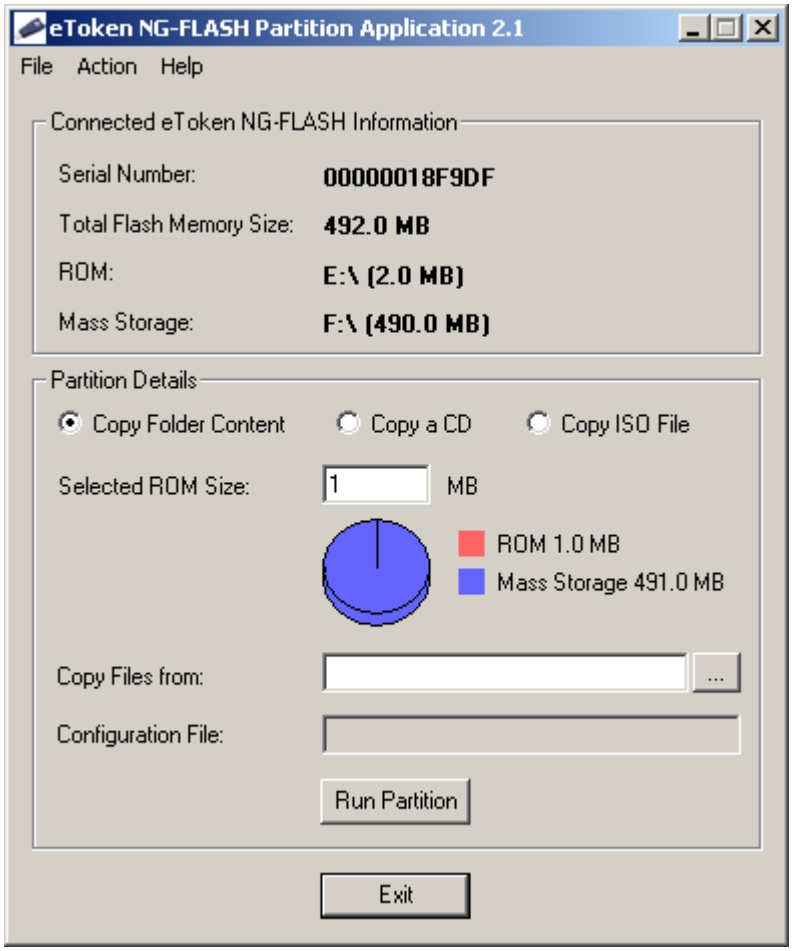


9. Утилита NG-Flash Partition

В состав eToken PKI Client входит утилита NG-Flash Partition, которая предназначена для управления разделами памяти устройств eToken NG-FLASH и eToken NG-FLASH (Java). Для вызова утилиты в расширенном режиме eToken Properties щелкните правой кнопкой мыши в пункте Настройки eToken PKI Client в дереве слева и выберите пункт Запустить приложение eToken NG-FLASH Partition.

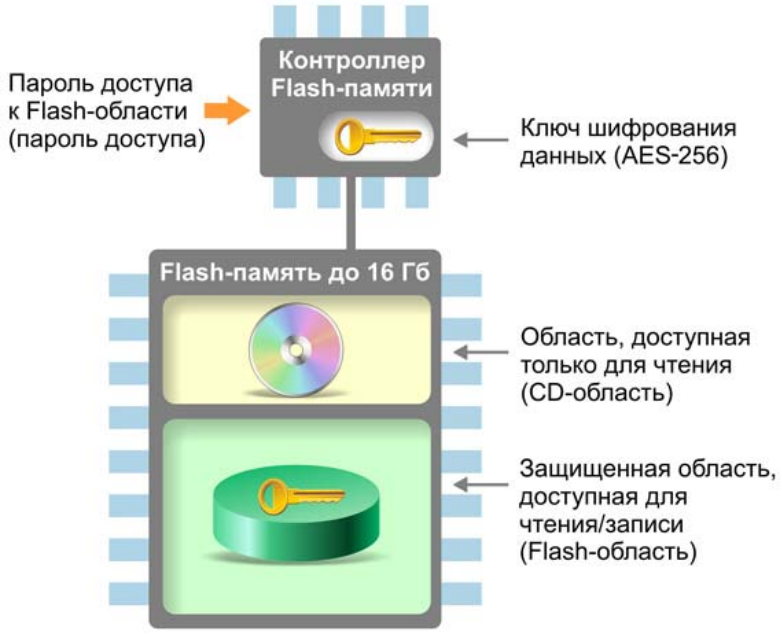


Все операции выполняются из главного окна утилиты.



9.1. Память электронных ключей eToken NG-FLASH / eToken NG-FLASH (Java)

Прежде чем говорить о возможностях eToken NG-FLASH и eToken NG-FLASH (Java), важно иметь представление о том, как организована их память.



В названных моделях eToken имеется встроенный модуль Flash-памяти, в которой помимо собственно перезаписываемой области для хранения любых данных может быть выделена ROM-область для автоматического запуска программ при подключении eToken. Для разметки Flash-памяти используется утилита eToken NG-FLASH Partition.

Данные в области для чтения и записи могут быть зашифрованы. Операции шифрования (зашифрование данных при их записи, расшифрование при считывании) выполняются контроллером Flash-памяти, расположенным внутри устройства. Ключ шифрования данных также хранится в контроллере Flash-памяти. Для защиты доступа к ключу шифрования данных используется пароль доступа.

Если пароль доступа не установлен, ключ шифрования данных хранится в памяти контроллера в открытом виде. Если пароль установлен, то ключ шифрования данных хранится в памяти контроллера в зашифрованном виде (для шифрования ключа шифрования данных также используется алгоритм шифрования AES, в качестве ключа выступает пароль доступа).

9.2. Функциональные возможности и ограничения различных моделей электронных ключей eToken

Версия используемого ПО и модели eToken накладывает определенные функциональные ограничения. Требования к ПО и доступные функции для разных моделей eToken сведены в следующей таблице по критерию установленной в электронном ключе операционной системы.

Версия аппаратного обеспечения	ОС	Макс. объем Flash-памяти	Шифрование Flash-области	Версия eToken NG-FLASH Partition	eToken NG-Flash Secure Drive	Создание загрузочной ROM-области
4.27	Siemens CardOS 4.2b	4 ГБ	–	1.0.15	–	–
				2.0		+
				2.1		
5.01	OS755	4 ГБ	AES-128	2.0	1.0	+
				2.1		
5.30	OS755	16 ГБ	AES-256	2.1	2.1	+

9.3. Управление разделами eToken NG-FLASH / eToken NG-FLASH (Java)

Для демонстрации работы утилиты предлагаем вам типовой сценарий, в котором вам необходимо подготовить новый USB-ключ eToken NG-FLASH для автозагрузки приложения из ROM-памяти устройства. Для этого выполните следующие действия.

1. В группе переключателей Partition Details выберите необходимый пункт

- Copy Folder Content – копировать данные из папки (копирование отдельных файлов невозможно).

- Copy a CD – копировать данные с диска.

- Copy ISO file – копировать образ ISO-файла.

  В зависимости от выбранного выше пункта в поле **Copy Files from** будет доступен выбор файла или литеры диска, откуда будут копироваться данные в eToken.

2. Выберите файл или литеру диска, щелкнув на кнопке  справа от поля **Copy Files from**.

   После этого в поле Selected ROM Size вы увидите, какой объем ROM-памяти будет выделен для записи указанных данных. В круговой диаграмме этот объем будет также выделен красным сектором.

3. Если во Flash-памяти eToken есть какие-либо данные и в защищенной памяти хранятся сертификаты, прежде всего позаботьтесь о том, чтобы у вас была сохранена резервная копия этих данных на случай их необходимости в будущем.

4. Нажмите кнопку **Run Partition**.

   На некоторое время в окне появится сообщение Please Wait (Подождите, пожалуйста), и затем появится сообщение с предложением переподключить eToken.

   Отключите и снова подключите eToken к USB-порту.

   После того как инициализация будет завершена, на экране появится соответствующее подтверждающее сообщение.

5. Закройте окно, нажав кнопку **OK**.

Описанная процедура позволяет загрузить в ROM-память приложения, управляющие доступом к Flash-памяти. Подробнее об этом читайте в следующем пункте.

9.4. Блокирование доступа к Flash-памяти устройств eToken NG-Flash (Java)

В дистрибутив eToken PKI Client входит утилита eToken NG-Flash Secure Drive для управления доступом к памяти eToken NG-FLASH (Java). Используя описанную выше процедуру, вы можете записать эту утилиту в ROM-память устройства с тем, чтобы задать пароль и заблокировать доступ к содержимому Flash-памяти. Для этого выполните следующие действия.

1. Откройте утилиту eToken NG-Flash и выполните инициализацию, указав в настройках путь к файлам eToken NG-Flash Secure Drive (по умолчанию – c:\Program Files\Aladdin\eToken\PKIClient\NG-FLASH Partition\NG-FLASH_Secure_Sample, где c: - диск, куда был установлен eToken PKI Client).

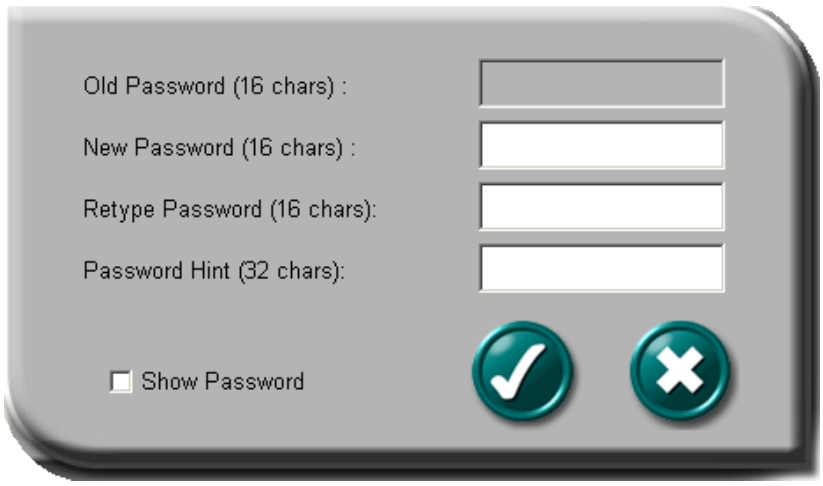
   В этой папке вы найдете три файла:

- Lock.exe – исполняемый файл утилиты eToken NG-Flash Secure Drive.
- eTFlash – значок eToken NG-Flash Secure Drive в области уведомлений.
- autorun.inf – конфигурационный файл для автоматического запуска утилиты eToken NG-Flash Secure Drive.

   Инициализированный eToken будет отображаться как два устройства: CD-ROM и Съемный диск.

2. Откройте ROM-диск и запустите утилиту lock.exe. На экране появится следующее окно.

3. Нажмите кнопку с ключом в правом верхнем углу окна. На экране появится следующее окно.



4. Введите новый пароль в полях **New Password** и **Retype Password**. На случай, если вы забудете пароль, вы можете ввести подсказку в поле **Password Hint** (необязательное поле). Отметьте пункт Show Password, если вы хотите, чтобы значение пароля отображалось в открытом виде.

5. Сохраните новый пароль, нажав кнопку  .

Теперь для доступа к содержимому Flash-памяти вам необходимо будет выполнить авторизацию с помощью той же утилиты eToken NG-Flash Secure Drive. Если в вашей системе включен автозапуск съемных носителей, то утилита запустится сразу при подключении eToken.

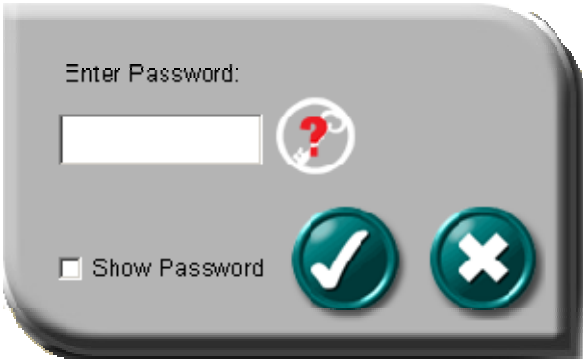
Ограничение вступит в силу сразу после отключения eToken или после нажатия кнопки  .

9.5. Разблокирование доступа к Flash-памяти устройств eToken NG-Flash (Java)

Чтобы разблокировать доступ к Flash-памяти устройства, выполните следующие действия.

1. Запустите утилиту eToken NG-Flash Secure Drive (если она не запускается автоматически при подключении eToken).

2. Нажмите кнопку  . На экране появится следующее меню.



3. Введите пароль в поле **Enter Password**. Если вы забыли пароль, и при установке пароля была задана подсказка, вы можете воспользоваться ей, щелкнув на значке со знаком вопроса справа от поля **Enter Password**.

4. Нажмите кнопку  . Если пароль был введен правильно, на экране появится сообщение о том, что устройство разблокировано.

5. Закройте окно, нажав кнопку  .

9.6. Снятие пароля для доступа к Flash-памяти устройств eToken NG-FLASH (Java)

Если вы хотите сделать Flash-память eToken NG-FLASH (Java) доступной без ограничений, выполните следующие действия.

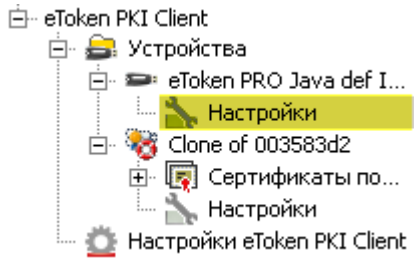
1. Запустите утилиту eToken NG-Flash Secure Drive (если она не запускается автоматически при подключении eToken).
2. Нажмите кнопку  . На экране появится следующее меню.

3. Введите пароль в поле **Enter Password**. Если вы забыли пароль, и при установке пароля была задана подсказка, вы можете воспользоваться ей, щелкнув на значке со знаком вопроса справа от поля **Enter Password**.
4. Нажмите кнопку  . Если пароль был введен правильно, на экране появится сообщение о том, что устройство разблокировано.

Закройте окно, нажав кнопку  .

10. Настройки устройств eToken

В этой главе описаны настройки, которые относятся только к отдельным устройствам. Чтобы задать такие настройки, в расширенном режиме утилиты eToken Properties выберите устройство и пункт Настройки, как показано на следующем рисунке.



Краткое содержание главы:

- Настройка качества паролей
- Настройка режима кэширования закрытых данных
- Защита ключей RSA дополнительным паролем

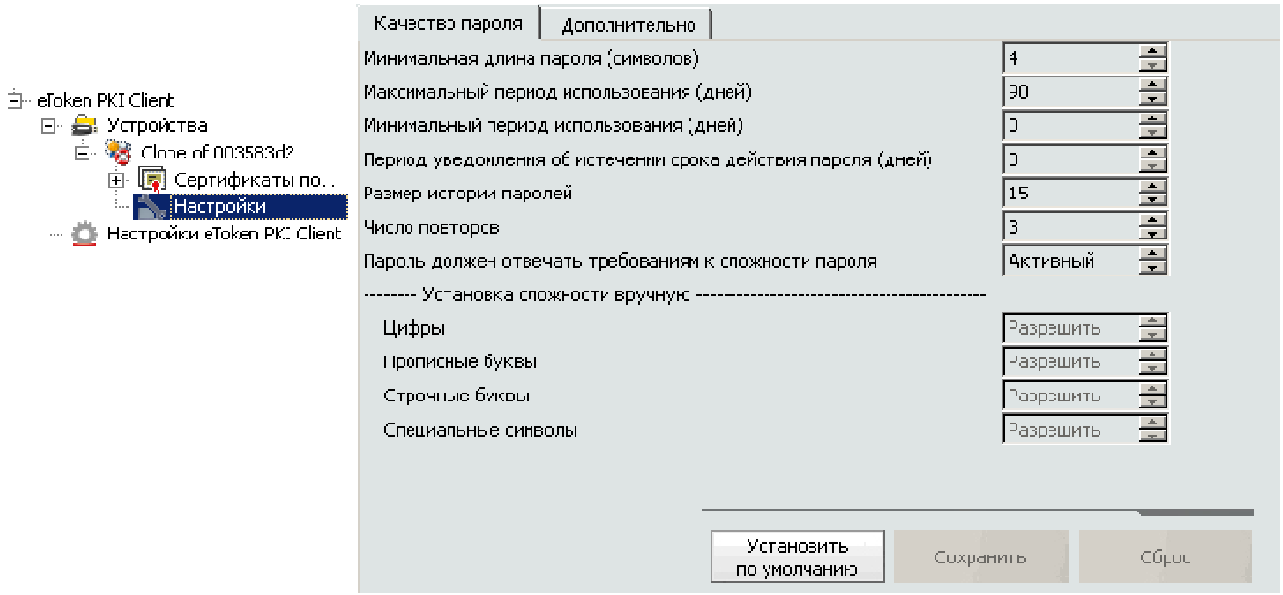
10.1. Настройка качества паролей

Параметры качества пароля пользователя и пароля администратора (далее – паролей) достаточно настроить один раз. Тогда при установке пароля будет выполняться обязательная его проверка на стойкость согласно заданным критериям. В eToken RTE 3.66 и более ранних версиях все настройки качества паролей хранились на локальном компьютере в файле `etpass.ini`. Начиная с eToken PKI Client версии 4.0, эти настройки хранятся в памяти eToken.

Если eToken был инициализирован с помощью eToken RTE, параметры качества паролей на нем сохранить будет нельзя.

Чтобы настроить политику качества паролей, выполните следующие действия:

1. Откройте утилиту Свойства eToken.
2. Перейдите в расширенный режим, нажав кнопку  в главном окне.
3. В дереве слева раскройте ветвь, соответствующую устройству, и выберите пункт **Настройки**.
4. На вкладке **Качество паролей** установите необходимые параметры, руководствуясь следующей таблицей.



Настройки качества паролей включают в себя следующие:

Название параметра на вкладке Качество пароля	Пояснения
Минимальная длина пароля (символов)	по умолчанию – 6.
Максимальный период использования (дней)	максимальный срок действия пароля в днях (по умолчанию равен 0 – срок действия пароля не ограничен).
Минимальный период использования (дней)	время действия пароля до того момента, когда его можно будет впервые изменить.
Период уведомления об истечении срока действия пароля (дней)	значение этого поля показывает, когда пользователь получит предварительное уведомление об истечении срока действия пароля (по умолчанию – 0 – уведомления пользователю не выдаются).
Размер истории паролей	этот параметр определяет количество сохраненных ранее использовавшихся паролей (по умолчанию – 10). Новый пароль не может совпадать с одним из тех паролей, которые на текущий момент хранятся в журнале.
Число повторов	Максимальное число повторов каждого символа в значении пароля. По умолчанию: 3.
Пароль должен отвечать требованиям к сложности пароля	Данный параметр указывает на необходимость проверки сложности пароля, а именно присутствия в значении различных типов символов: заглавных и прописных букв, цифр и специальных символов). Возможные значения: • Активный (по умолчанию): в значении пароля должны обязательно присутствовать символы всех типов. • Вручную: в значении пароля должны быть указаны те символы, которые выбраны в следующих полях (**Цифры, Прописные буквы, Строчные буквы, Специальные символы**). • Нет: контроль сложности пароля отключен.

5. Чтобы сохранить заданные параметры, нажмите кнопку **Сохранить**.

10.2. Настройка режима кэширования данных

В целях повышения производительности в PKI Client имеется возможность кэшировать открытые данные, которые хранятся в памяти eToken.

Чтобы включить режим кэширования закрытых данных, выполните следующие действия:

1. Откройте утилиту Свойства eToken.
2. Перейдите в расширенный режим, нажав кнопку  в главном окне.
3. В дереве слева раскройте узел, соответствующий устройству, для которого вы хотите настроить параметры кэширования.
4. Выберите пункт **Настройки** и справа раскройте вкладку **Дополнительно**.
5. В поле **Режим кэширования личных данных** выберите требуемое значение.

   Возможны три варианта:

- **Всегда (быстрый)** – режим по умолчанию Закрытые данные кэшируются в приложении всегда. Этим ускоряется его работа, так как часть данных сохраняется на локальном компьютере, однако такой механизм менее безопасен, нежели когда данные не кэшируются.

- **Во время сеанса пользователя.** Данные остаются в кэше с момента авторизации с помощью eToken и до момента, пока сеанс авторизации не будет закрыт. После этого все закрытые данные будут удалены из кэша.

- **Никогда.** В этом случае закрытые данные не кэшируются.

10.3. Защита ключей RSA дополнительным паролем

Этот режим позволяет установить режим задания дополнительного пароля для генерируемых ключей RSA. Если пароль задан, то помимо обладания собственно eToken и PIN-кодом, вам также необходимо будет знать пароль для данного ключа RSA.

Чтобы установить режим защиты ключей RSA, выполните следующие действия.

1. Откройте утилиту Свойства eToken.
2. Перейдите в расширенный режим, нажав кнопку  в главном окне.
3. В дереве слева раскройте узел, соответствующий устройству, для которого вы хотите настроить параметры кэширования.
4. Выберите пункт **Настройки** и справа раскройте вкладку **Дополнительно**.
5. В поле **Режим кэширования личных данных** выберите требуемое значение.

   Возможны следующие варианты:

- **Всегда**. Перед генерацией ключа RSA всегда предлагается задать дополнительный пароль; если в отдельном случае вы этого делать не хотите, достаточно нажать кнопку Отмена

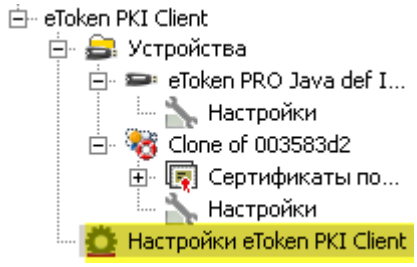
- **Всегда запрашивать пользователя**. Перед генерацией ключа RSA пользователю предлагается выбрать, задавать дополнительный пароль или нет

- **По требованию приложения**. В этом режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность (при генерации ключа через Crypto API с флагом «User protected»).

- **Никогда не спрашивать**. В этом режиме пароль для ключа RSA задать нельзя (режим по умолчанию).

11. Настройки eToken PKI Client

В этой главе представлены настройки, которые отвечают за работу eToken PKI Client. Найти их в утилите eToken Properties можно, щелкнув в расширенном режиме на узле Настройки eToken PKI Client.



Здесь представлены не все настройки, поскольку некоторые из них задаются только в процессе установки (см. eToken PKI Client 5.1 SP1. Руководство администратора).

Все настройки eToken PKI Client можно разделить на две части – так, как они представлены на вкладках в правой части окна. Первая группа параметров – это параметры качества паролей. Все они дублируют те же параметры, что действуют применительно к отдельным устройствам, и более подробно они были описаны выше. Разница здесь лишь в том, что параметры, установленные в разделе Настройки eToken PKI Client, не имеют привязки к конкретному устройству, а действуют в отношении всех устройств eToken при смене пароля и инициализации.

Вторая группа – это параметры, которые отвечают за хранение и управление сертификатами. Эти параметры представлены на вкладке **Дополнительно**.

11.1. Качество паролей

См. Настройка качества паролей.

11.2. Прочие настройки

В данном разделе задаются настройки качества паролей, используемые при инициализации устройств eToken с помощью утилиты «Свойства eToken». Данные настройки можно изменить в процессе инициализации. После инициализации настройки сохраняются в памяти устройства. Подробное описание всех возможных настроек приведено в разделе «Качество паролей» на странице 62.

Настройки, представленные в разделе «Прочее»:

11.2.1 Копировать сертификаты в локальное хранилище

Этот режим включен по умолчанию. Когда вы подключаете eToken, все хранящиеся на нем сертификаты копируются в хранилище сертификатов Windows. После отключения eToken эти сертификаты либо автоматически удаляются, либо остаются в хранилище.

Так как eToken PKI Client 5.1 SP1 передает все сертификаты в реестр, то дополнительного подтверждения об удалении сертификатов не требуется. Сертификат удаляется только из реестра и остается в памяти eToken. Когда вы подключите eToken в следующий раз, сертификат снова будет скопирован. При необходимости можно удалить сертификаты при отключении eToken. Для этого воспользуйтесь утилитой Свойства eToken.

Копирование закрытых ключей, сгенерированных на eToken, не производится.

11.2.2 Управление сертификатами ЦС

По умолчанию этот режим отключен. Включение режима позволяет загружать сертификаты ЦС, хранящиеся в памяти eToken, в локальное хранилище на компьютере.

11.2.3 Включить режим единого входа

По умолчанию этот режим отключен. При включении этого режима введенный один раз PIN-код кэшируется и автоматически отправляется во все приложения, которым необходима аутентификация в eToken. При отключении и подключении устройства заново, PIN-код будет необходимо ввести повторно.

11.2.4 Возможность настройки после инициализации

Данный параметр определяет возможность настройки паролей после инициализации eToken. По умолчанию такая возможность включена.

11.2.5 Возможность настройки для администратора

Этот параметр действует только тогда, когда предыдущий параметр включен. Если этот пункт отмечен, то параметры качества паролей может менять администратор. Если снять флажок в этом пункте, параметры качества паролей сможет менять также и пользователь.

Тел: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 2683Р от 02.09.05, №№ 4205П, 4206Х, 4207Р от 22.06.07 и № 4898П от 14.12.07