Рост интереса к средствам аутентификации и увеличившееся их разнообразие является следствием общего перехода от паролей к более надежным технологиям.

Gartner, 2009

eToken®

YOUR KEY TO eSECURITY

РЕШЕНИЯ НА ОСНОВЕ USB-КЛЮЧЕЙ И СМАРТ-КАРТ

ДЛЯ ***аутентификации и хранения ключевой информации***

Aladdin®
SECURITY SOLUTIONS

Аутентификация или подтверждение подлинности — процедура проверки того, что пользователь является именно тем, за кого он себя выдает. Основой этой проверки является некая уникальная информация, доступная пользователю.

Наиболее надежным способом является многофакторная аутентификация – аутентификация, в процессе которой используются аутентификационные факторы нескольких типов. Например, пользователь должен предоставить смарт-карту или USB-ключ и ввести пароль. В этом случае злоумышленник не сможет получить доступ к данным, т.к. ему придется не только подсмотреть пароль, но и предъявить физическое устройство, кража которого, в отличие от кражи пароля, практически всегда быстро обнаружима.

eToken – персональное средство аутентификации и хранения ключевой информации

eToken компании Aladdin позволяет пользователям, IT-администраторам и администраторам безопасности более эффективно управлять процессом аутентификации, безопасно сохраняя в памяти eToken пароли, закрытые ключи, сертификаты открытого ключа, профили пользователя и другую информацию, нуждающуюся в безопасном хранении.

Использование eToken позволяет:

- повысить защищенность и обеспечить безопасный доступ к информации;
- эффективно управлять паролями;
- всегда иметь при себе персональные цифровые данные (сертификаты, ключи ЭЦП и шифрования, коды доступа), хранящиеся в защищенной памяти.

eToken обеспечивает двухфакторную аутентификацию пользователя

Фактор владения:
пользователь имеет «нечто» – ключ eToken

Фактор знания:
пользователь знает «нечто» – пароль ключа

Для чего нужен eToken?

Безопасный доступ к сети

Вход в сеть

eToken позволяет осуществлять двухфакторную аутентификацию пользователей при обращении к защищенным сетевым ресурсам. При этом могут использоваться как технология регистрации с использованием сертификатов инфраструктуры открытых ключей (PKI), так и стандартная аутентификация Microsoft (GINA API) с обычными паролями пользователей.

Безопасность виртуальных частных сетей (VPN) и безопасный удаленный доступ

eToken позволяет обеспечить двухфакторную аутентификацию пользователей при удаленном доступе к корпоративной сети. Он легко интегрируется с ведущими системами VPN и поддерживает различные методы аутентификации при доступе к VPN, включая одноразовые пароли и цифровые сертификаты.

Web - доступ

eToken позволяет обеспечить двухфакторную аутентификацию пользователей при доступе к защищенным Web-ресурсам и подпись конфиденциальных цифровых транзакций. eToken поддерживает несколько методов веб-аутентификации, включая одноразовые пароли и цифровые сертификаты.

Безопасность данных

Защита компьютера на этапе загрузки , шифрование данных

eToken интегрирован со многими системами защиты данных, обеспечивающих как аутентификацию пользователя до загрузки операционной системы и полное шифрование дисков (например, Secret Disk), так и отдельное шифрование выбранных папок и файлов.

Безопасная электронная почта

eToken позволяет шифровать и подписывать сообщения электронной почты, используя встроенные функции безопасности основных почтовых клиентов.

Цифровая подпись (предотвращение отказа от авторства)

С помощью eToken сообщения и документы можно снабжать электронной подписью, используя технологию PKI, обеспечивающую достоверность электронных сообщений.

Управление паролями

Благодаря eToken пользователям больше не нужно запоминать пароли для различных учетных записей. Все, что им нужно – это иметь устройство eToken и знать единственный пароль, необходимый для доступа к нему.

eToken управляет реквизитами пользователя и автоматически использует их для заполнения Web-форм, ввода данных ля прикладных приложений и входа в сеть.

Линейка продуктов eToken

Линейка продуктов eToken предоставляет широкие возможности интеграции со многими ведущими современными решениями в области информационной безопасности, позволяя решить любую задачу, связанную с аутентификацией и управлением паролями.

Модели eToken

eToken PRO

eToken PRO – смарт-карта с интегрированным ридером, выполненная в виде USB-ключа или смарт-карта, выполненная в виде обычной кредитной карты, предназначенная для чтения с помощью любого считывателя смарт-карт. Это доступное и простое устройство используется для реализации строгой двухфакторной аутентификации и в системах PKI.

Технические характеристики:

Операционные системы:	Microsoft Windows 2000/2003/XP/Vista/2008 (32 и 64-битные версии); Linux; Mac OS
Поддержка API и стандартов:	PKCS#11 v2.01, CAPI, CNG, команды APDU Siemens/Infineon, PC/CS; хранение сертификатов X.509 v3, SSL v3, IPSec/IKE
Объем защищенной памяти:	32КБ, 64КБ
Разъем:	USB типа A
Корпус (для USB-ключей):	твердая пластмасса, не поддающаяся необнаружимому вскрытию
Срок хранения данных в памяти:	не менее10 лет
Количество циклов перезаписи памяти:	не менее 500,000

eToken PRO (Java)

eToken PRO (Java) - новая модель USB-ключей и смарт-карт eToken, построенная на базе Java-карты. Обладает всей функциональностью eToken PRO, имеет увеличенный объем памяти для защищённого хранения пользовательских данных и предоставляет возможность расширения функционала за счет загрузки дополнительных приложений (апплетов).

Технические характеристики:

Операционные системы:	Microsoft Windows 2000/2003/XP/Vista/2008 (32 и 64-битные версии); Linux; Mac OS
Поддержка API и стандартов:	PKCS#11 v2.01, CAPI, CNG, команды APDU Athenna OS755, PC/CS; хранение сертификатов X.509 v3, SSL v3, IPSec/IKE
Объем защищенной памяти:	72КБ
Разъем:	USB типа A
Корпус (для USB-ключей):	твердая пластмасса, не поддающаяся необнаружимому вскрытию
Срок хранения данных в памяти:	не менее10 лет
Количество циклов перезаписи памяти:	не менее 500,000

Контроль доступа в помещения

eToken может использоваться в решениях на базе бесконтактных технологий контроля доступа. Радио-метки (RFID-метки) могут быть встроены как в USB-ключи, так и в смарт-карты eToken.

Примеры встраиваемых RFID-меток: HID, EM-Marin, Ангстрем, Indala, Mifare и др.

eToken NG-FLASH

Комбинированный ключ, сочетающий возможности модели eToken PRO и защищённого хранилища данных. Дополнительная Flash-память устройства может быть использована для загрузки операционных систем Microsoft Windows или Linux (образ операционной системы записывается в память устройства), для автоматического запуска приложений из памяти устройства, для безопасного хранения, транспортировки и резервного копирования данных.

Технические характеристики:

Операционные системы:	Microsoft Windows 2000/2003/XP/Vista/2008 (32 и 64-битные версии); Linux; Mac OS
Поддержка API и стандартов:	PKCS#11 v2.01, CAPI, CNG, команды APDU Athena OS755, PC/CS; хранение сертификатов X.509 v3, SSL v3, IPSec/IKE
Объем защищенной памяти:	64КБ
Объем Flash-памяти:	512МБ, 1ГБ, 2ГБ, 4ГБ
Разъем:	USB типа A
Корпус (для USB-ключей):	твердая пластмасса
Срок хранения данных памяти:	не менее10 лет
Количество циклов перезаписи памяти:	не менее 500,000
Количество циклов перезаписи Flash-памяти:	не менее 10,000

eToken NG-OTP

eToken NG-OTP – комбинация USB-ключа, обладающего всеми возможностями eToken PRO, и генератора одноразовых паролей (One-Time Password – OTP). При использовании eToken NG-OTP в режиме генератора одноразовых паролей безопасный доступ к корпоративным ресурсам возможен без установки дополнительного клиентского ПО и без физического подключения к компьютеру (также возможен доступ с мобильных устройств).

Технические характеристики:

Операционные системы:	Microsoft Windows 2000/2003/XP/Vista/2008 (32 и 64-битные версии); Linux; Mac OS. Одноразовые пароли могут использоваться в любой операционной системе
Поддержка API и стандартов:	PKCS#11 v2.01, CAPI, CNG, команды APDU Siemens/Infineon, PC/CS; хранение сертификатов X.509 v3, SSL v3, IPSec/IKE
Алгоритм генерации OTP:	соответствующий архитектуре OATH (основан на HMAC/SHA1)
Срок жизни батарей:	14,000 сгенерированных паролей или 7 лет
Объем защищенной памяти:	64КБ
Разъем:	USB типа A
Корпус:	твердая пластмасса
Срок хранения данных в памяти:	не менее10 лет
Количество циклов перезаписи памяти:	не менее 500,000

eToken PASS

eToken PASS – автономный генератор одноразовых паролей, не предназначенный для подключения к компьютеру.

Технические характеристики:

Операционные системы:	любые
Алгоритм генерации OTP:	соответствующий архитектуре OATH (основан на HMAC/SHA1)
Срок жизни батарей:	14,000 сгенерированных паролей или 7 лет

Задачи обеспечения безопасности

Строгая двухфакторная аутентификация

Аутентификация с использованием PKI

В системах, использующих PKI, возможности eToken позволяют получать безопасный доступ к корпоративной сети, защищать свои персональные файлы и данные, осуществлять электронные сделки, подписывать и шифровать электронные письма и много другое – все это без ограничения мобильности и под надежной защитой.

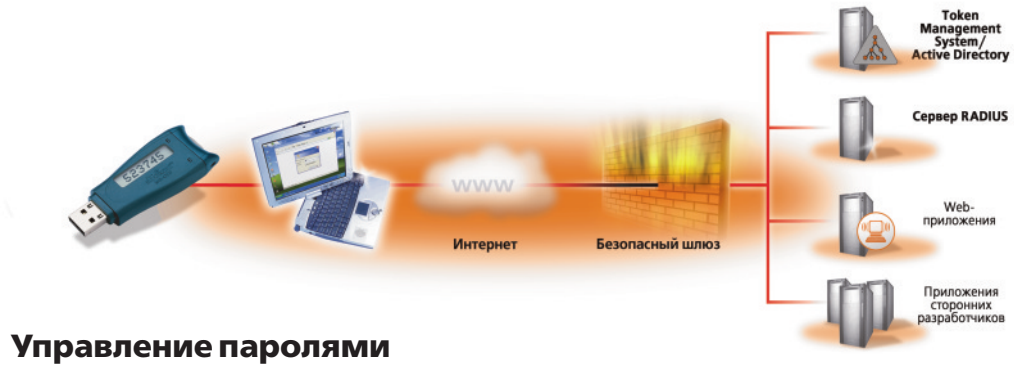
eToken позволяет с легкостью внедрить строгую аутентификацию пользователей и криптографические решения на основе PKI, приспособив их к конкретным условиям и требованиям организации. Ключевые пары генерируются в доверенной среде – защищенной памяти eToken. При этом закрытые ключи никогда не покидают память устройства, а сертификаты открытого ключа доступны для внешних приложений после ввода пароля eToken.

Аутентификация с использованием одноразовых паролей (One-Time Password – OTP)

Аутентификация с использованием одноразовых паролей подразумевает использование нового пароля для каждого нового сеанса доступа. Такой способ особенно актуален при доступе из ненадежной среды, например, из Интернет-кафе. Преимуществом решения компании Aladdin для работы с OTP является отсутствие необходимости использования дополнительного клиентского программного обеспечения, а также необходимости подключения специальных устройств к USB- порту. Это позволяет использовать решение в мобильных устройствах, а также в терминальных станциях, не оборудованных USB портами.

Компания Aladdin предлагает два вида устройств для работы с OTP – **eToken NG-OTP и eToken PASS.**

Архитектура eToken OTP предполагает наличие сервера аутентификации RADIUS, что делает возможным интеграцию с любыми VPN-шлюзами и приложениями, поддерживающими этот протокол. Сервер RADIUS использует для получения информации о пользователе инфраструктуру Active Directory (с использованием системы централизованного управления устройствами линейки eToken - TMS).



Управление паролями

eToken Network Logon

eToken Network Logon предназначен для кардинального решения проблемы «слабых» паролей при работе на компьютерах под управлением Microsoft Windows. Сразу после установки продукта для входа в компьютер или в сеть можно начать использовать надёжные и стойкие к перебору пароли, либо цифровые сертификаты.

eToken Network Logon сгенерирует сложный пароль, установит его в системе и сохранит в памяти eToken. Пользователю больше не нужно запоминать и вводить новый пароль, что исключает возможность его подсматривания или перехвата злоумышленником.

eToken Web Sign-On

eToken Web Sign-On предназначен для сохранения данных, вводимых пользователем в различных формах на Web-сайтах. После сохранения данных в защищенной памяти устройства eToken, они будут автоматически подставляться при открытии Web-страниц, содержащих соответствующие формы. Для доступа ко всем сохраненным данным необходимо знание единственного пароля – пароля eToken.

В памяти eToken сохраняются не только регистрационные имена и пароли, но и любые другие конфиденциальные данные, которые пользователь хотел бы не вводить каждый раз вручную – номера счетов, телефонов, параметры кредитных карт и другие.

Web Sign-On поддерживается Microsoft Internet Explorer и Mozilla Firefox.

eToken Single Sign-On (SSO)

В любой компании доступ к тем или иным ресурсам и приложениям зависит от наличия соответствующих прав, однако до сих пор во многих случаях используется однофакторная аутентификация на базе паролей. В случае необходимости доступа к большому числу разных ресурсов и приложений пользователю становится крайне трудно помнить наизусть все нужные регистрационные данные. eToken SSO позволяет сохранять в защищенной памяти eToken все пароли и регистрационные данные для доступа к большому числу разных ресурсов и приложений: это и приложения Windows, и различные формы на Web-сайтах. Для доступа к ним будет необходимо знание единственного пароля – пароля устройства eToken.

Централизованное управление

Token Management System (TMS)

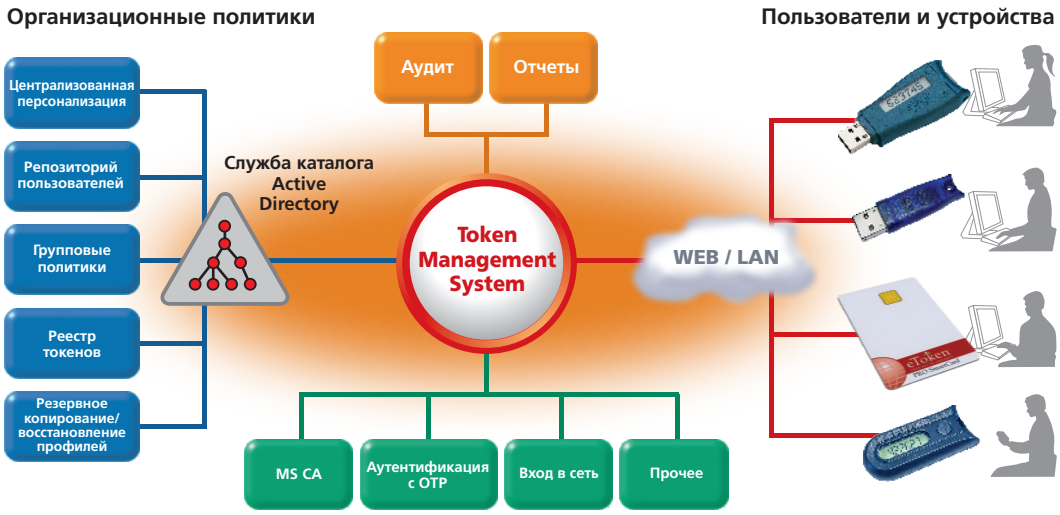
eToken TMS – это решение, предназначенное для построения инфраструктуры безопасного доступа к информационным ресурсам предприятия с централизованным управлением.

Назначение

- Централизованное управление средствами аутентификации в течение всего жизненного цикла (инициализация/выпуск сертификата, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование).;
- Учет средств аутентификации, аудит их использования;
- Автоматизация типовых операций и сценариев администрирования в соответствии с политиками безопасности, принятыми в организации.
- Быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

eToken TMS является связующим звеном между пользователями, средствами аутентификации, приложениями информационной безопасности – основанных как на PKI, так и на традиционной аутентификации с применением регистрационных имен и паролей – и политикой безопасности.

Для разработки дополнений к TMS доступен комплект разработчика eToken TMS Connector SDK, позволяющий добавить возможность работы со сторонними приложениями в процессе стандартных операций с устройствами eToken (добавление, назначение, отзыв и т.д.).



Интероперабельность

Компания Aladdin уделяет пристальное внимание обеспечению совместимости своих продуктов и технологий с решениями ведущих производителей. Это, в первую очередь, подтвержденная сертификатами совместимость с такими мировыми вендорами, как Microsoft, IBM, Novell, Cisco. Кроме этого компанией Aladdin были выполнены работы по совместимости и совместные тестирования корректности работы eToken с ведущими российскими разработчиками СКЗИ (компаниями «КРИПТО-ПРО», «Инфотекс», «Сигнал-КОМ», «ЛИССИ»), систем защиты информации, а также множества прикладных систем: электронного документооборота, биллинга, банковского ПО, медицинских и ряда других.

Исследования совместимости решений eToken с решениями разработчиков СКЗИ проводятся на постоянной основе по мере выхода новых моделей eToken или новых версий СКЗИ.

Отзывы клиентов

Первый Республиканский Банк (ОАО «ПРБ»)
Коханько Сергей, Начальник Отдела информационной защиты и безопасности

**«Внедрение технологичных и прозрачных в управлении средств аутентификации на базе смарт-карт eToken позволило нам решить ряд задач по снижению влияния человеческого фактора на уровень информационной безопасности.
Использование eToken позволило свести к нулевому показателю случаи разглашения паролей и использования чужих учётных записей для доступа к компьютерам и данным».**

Объединенная Система Мобильных Платежей
Дмитрий Уханов, Директор департамента по разработке IT

«Защиту аутентификационных данных пользователей с помощью eToken мы расцениваем как значительное конкурентное преимущество, что уже успели оценить наши агенты. На данный момент не зарегистрировано ни одного случая несанкционированного доступа к системе online-транзакций агентов, использующих eToken, что лишний раз убеждает нас в правильности выбора».

Сертифицированные продукты на базе eToken

USB-ключи и смарт-карты eToken

Сертифицированные электронные ключи eToken являются программно-аппаратным средством аутентификации и хранения ключевой информации и средством защиты информации от несанкционированного доступа (сертификат ФСТЭК России №1883 от 11.08.2009 г.).

В соответствии с рекомендациями руководящих документов сертифицированные электронные ключи eToken могут использоваться в ИСПДн до 2 класса включительно и для создания автоматизированных информационных систем до класса защищенности 1Г включительно.

Сертифицированные электронные ключи eToken являются рекомендуемым носителем ключевой информации для сертифицированных СКЗИ российских разработчиков.

eToken Windows Logon

Программно-аппаратный комплекс eToken Windows Logon предназначен для входа на рабочую станцию и в домен Windows с использованием USB-ключей и смарт-карт eToken.

eToken Windows Logon обеспечивает двухфакторную аутентификацию пользователей и администраторов рабочих станций, а также автоматически блокирует рабочую станцию при отсоединении eToken. Применение eToken Windows Logon позволяет решить проблему «слабых» паролей и автоматизировать исполнение пользователями требований регламентов по ИБ.

Сертифицированный eToken Windows Logon следует применять для аутентификации пользователей в автоматизированных системах, обрабатывающих конфиденциальную информацию, до класса защищенности 1Г включительно (сертификат ФСТЭК России №925/3 от 14.02.2007 г.).

ID: M02101-0909

Aladdin SECURITY SOLUTIONS

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
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner

Microsoft CERTIFIED Partner

IBM Business Partner

ORACLE PARTNER