Содержание:

ВВЕДЕНИЕ

Электронный ключ (также *аппаратный ключ*, иногда *донгл* от англ. *dongle*) — аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения.

Основой данной технологии является специализированная микросхема, либо защищённый от считывания микроконтроллер, имеющие уникальные для каждого ключа алгоритмы работы. Донглы также имеют защищённую энергонезависимую память небольшого объёма, более сложные устройства могут иметь встроенный криптопроцессор (для аппаратной реализации шифрующих алгоритмов), часы реального времени. Аппаратные ключи могут иметь различные форм-факторы, но чаще всего они подключаются к компьютеру через USB. Также встречаются с LPT- или PCMCIA-интерфейсами.

Принцип действия

Ключ присоединяется к определённому интерфейсу компьютера. Далее защищённая программа через специальный драйвер отправляет ему информацию, которая обрабатывается в соответствии с заданным алгоритмом и возвращается обратно. Если ответ ключа правильный, то программа продолжает свою работу. В противном случае она может выполнять определенные разработчиками действия, например, переключаться в демонстрационный режим, блокируя доступ к определённым функциям.

Существуют специальные ключи, способные осуществлять лицензирования (ограничения числа работающих в сети копий программы) защищенного приложения по сети. В этом случае достаточно одного ключа на всю локальную сеть. Ключ устанавливается на любой рабочей станции или сервере сети. Защищенные приложения обращаются к ключу по локальной сети. Преимущество в том, что для работы с приложением в пределах локальной

сети им не нужно носить с собой электронный ключ.

История

Защита ПО от нелицензионного пользования увеличивает прибыль разработчика. На сегодняшний день существует несколько подходов к решению этой проблемы. Подавляющее большинство создателей ПО используют различные программные модули, контролирующие доступ пользователей с помощью ключей активации, серийных номеров и т. д. Такая защита является дешёвым решением и не может претендовать на надёжность. Интернет изобилует программами, позволяющими нелегально сгенерировать ключ активации (генераторы ключей) или заблокировать запрос на серийный номер/ключ активации (патчи, крэки). Кроме того, не стоит пренебрегать тем фактом, что сам легальный пользователь может обнародовать свой серийный номер.

Эти очевидные недостатки привели к созданию аппаратной защиты программного обеспечения в виде электронного ключа. Известно, что первые электронные ключи (то есть аппаратные устройства для защиты ПО от нелегального копирования) появились в начале 1980-х годов, однако первенство в идее и непосредственном создании устройства, по понятным причинам, установить очень сложно.

eToken (от англ. electronic — электронный и англ. token — признак, жетон) — торговая марка для линейки персональных средств аутентификации в виде USB брелков и смарткарт а также программные решения с их использованием. Торговая марка была создана израильской компанией Aladdin Knowledge Systems (англ.)русск., впоследствии приобретённой SafeNet (англ.)русск.

Продуктами под этой торговой маркой в России торгует ЗАО «Аладдин Р. Д.»

Компания заявляет наличие сертификатов Гостехкомиссии и ФСТЭК России на продукты eToken,

1. Современные модели

1.1. Перечень современных моделей

- **eToken PRO** и **eToken PRO (Java)** — смарт-карты и USB-ключи, являющиеся полнофункциональными аналогами смарт-карт;
- **eToken GT** — недорогой аналог USB-ключей eToken PRO (Java), отличающийся лишь меньшим объёмом памяти;
- **eToken NG-FLASH** и **eToken NG-FLASH (Java)** — USB-ключи, сочетающие в себе возможности смарт-карт и USB флэш-накопителей;
- **eToken NG-OTP** и **eToken NG-OTP (Java)** — USB-ключи, сочетающие в себе возможности смарт-карт и генераторов одноразовых паролей;
- **eToken PASS** — OTP-токен (аппаратный генератор одноразовых паролей);
- **eToken Virtual** — программный эмулятор смарт-карты;
- **MobilePASS** — программный генератор одноразовых паролей.

1.2. Классификация

1.2.1. По функциональным возможностям

Функциями смарт-карт обладают все современные модели eToken, за исключением eToken PASS и MobilePASS.

eToken NG-FLASH с объёмом флэш-памяти 4 ГБ

Функциями USB флэш-накопителей обладают комбинированные устройства eToken NG-FLASH и eToken NG-FLASH (Java).

Функциями OTP-токенов (устройств для генерации одноразовых паролей) обладают eToken NG-OTP, eToken NG-OTP (Java), eToken PASS и MobilePASS.

1.2.2. По видам обеспечения

Различные модели eToken являются аппаратными устройствами, за исключением программных средств eToken Virtual и MobilePASS.

1.2.3. По программно-аппаратным платформам

eToken NG-Flash, eToken NG-OTP и eToken PRO созданы на основе операционной системы Siemens CardOS и микросхем Infineon.

eToken GT, eToken NG-Flash (Java), eToken NG-OTP (Java) и eToken PRO (Java) построены на платформе eToken Java (операционная система Athena OS755 и микросхема Atmel), в которой реализована технология Java Card с учётом стандарта Global Platform.

1.2.4. По форм-факторам

Форм-фактор	Модели	Иллюстрация
USB-ключ	eToken GT eToken NG-FLASH eToken NG-FLASH (Java) eToken PRO[6] eToken PRO (Java)[6]	 USB-ключ eToken PRO

USB-ключ с генератором одноразовых паролей	eToken NG-OTP eToken NG-OTP (Java)	 eToken NG-OTP
OTP-токен	eToken PASS	 eToken PASS
смарт-карта	eToken PRO[6] eToken PRO (Java)[6]	 Смарт-карта eToken PRO

1.3. Среда функционирования

Программное обеспечение eToken PKI Client, обеспечивающее работу eToken с функциями смарт-карт, функционирует под управлением операционных систем:

- BlackBerry;
- GNU/Linux;
- Mac OS;
- Microsoft Windows.

Аппаратные OTP-токены eToken требуют для своей работы сервер управления TMS, функционирующий на платформе Microsoft Windows Server 2003 или 2008.

Программное средство eToken Virtual способно функционировать под управлением операционных систем:

- CentOS 5.2;
- Fedora 9;
- Mac OS X 10.4 и 10.5;
- Microsoft Windows Server 2003 и 2008, Vista и XP;
- openSUSE 10.3;
- Red Hat Enterprise Linux 5.2;
- Ubuntu 8.04 (32-bit).

Программное средство MobilePASS функционирует в следующей среде:

- сервер управления TMS 5.0 или SafeWord 2008;
- клиенты с программным обеспечением BlackBerry, Java ME, Symbian OS, Windows Mobile или поддерживающие технологию SMS (только при использовании сервера SafeWord 2008).

2. Приложения

2.1. Check Point VPN-1 SecuRemote и VPN-1 SecureClient

Check Point VPN-1 SecuRemote и VPN-1 SecureClient поддерживают аутентификацию, основанную на использовании сертификатов открытого ключа и закрытых ключей в памяти смарт-карт и их аналогов. При наличии на клиентском компьютере драйвера eToken[7] для установления VPN-соединения можно использовать eToken, в памяти которого имеется закрытый ключ и соответствующий ему сертификат открытого ключа, дающий владельцу право подключения.

2.2. eToken Network Logon

eToken Network Logon — разработанное компанией Aladdin Knowledge Systems приложение, позволяющее сохранять имя пользователя, пароль и имя домена Windows в памяти eToken и затем использовать eToken в процессе аутентификации. При назначении нового пароля и смене пароля может использоваться встроенный в eToken Network Logon датчик случайных чисел, в результате чего пользователь может даже не знать свой пароль и, следовательно, не иметь возможности входить в систему без eToken. Помимо аутентификации с использованием подставляемых из памяти eToken паролей, eToken Network Logon поддерживает имеющийся в Windows 2000-Server 2008 механизм аутентификации с использованием сертификатов открытого ключа и закрытых ключей в памяти смарт-карт и их аналогов.

2.3. eToken SafeData и «Крипто БД»

eToken SafeData[8] и «**Крипто БД**» — средства криптографической защиты информации (СКЗИ), разработанные российской компанией Aladdin. Они позволяют шифровать данные в отдельных колонках таблиц баз данных Oracle. При этом ключи шифрования хранятся в базе данных зашифрованными с использованием открытых ключей пользователей, а закрытые ключи пользователей хранятся в памяти eToken. В результате для обращения к зашифрованным данным пользователи должны задействовать свои eToken, в памяти которых хранятся закрытые ключи, соответствующие открытым ключам, с помощью которых зашифрованы ключи шифрования. Отличие eToken SafeData от «Крипто БД» состоит в используемых этими СКЗИ криптографических алгоритмах:

- eToken SafeData шифрует данные по алгоритмам DES, Triple DES, AES и RC4, а ключи шифрования — по алгоритму RSA;
- «Крипто БД» шифрует данные по алгоритмам, соответствующим ГОСТ 28147-89 и RFC 4357, защищает ключи шифрования с использованием алгоритмов, описанных в ГОСТ Р 34.10-2001 и RFC 4490.

2.4. eToken SecurLogon для Oracle

eToken SecurLogon для Oracle — разработанное российской компанией Aladdin программное средство, в котором поддерживаемый в Oracle 8i Database Release 3 (8.1.7) Enterprise Edition и позднейших версиях СУБД Oracle механизм аутентификации с использованием сертификатов открытого ключа и закрытых ключей реализован с применением eToken в качестве ключевого носителя. Помимо отдельного продукта, eToken SecurLogon для Oracle представляет собой компонент средств криптографической защиты информации (СКЗИ) eToken SafeData и «Крипто БД», устанавливаемый на автоматизированном рабочем месте пользователей этих СКЗИ.

2.5. eToken SecurLogon для SAP R/3

eToken SecurLogon для SAP R/3 — разработанное компанией «АстроСофт» программное средство, позволяющее сохранять параметры подключения клиента к серверу приложений SAP R/3 в памяти eToken и в дальнейшем использовать eToken с сохранёнными реквизитами для аутентификации в системе SAP R/3.

2.6. eToken Single Sign-On

eToken Single Sign-On — разработанное компанией Aladdin Knowledge Systems приложение, позволяющее сохранять заполненные формы HTML и Windows в памяти eToken и затем автоматически подставлять в эти формы данные, сохранённые в памяти eToken. Благодаря этому eToken можно использовать как средство аутентификации во всех веб-приложениях, у которых интерфейс аутентификации представляет собой HTML-форму и во всех приложениях, у которых интерфейс аутентификации представляет собой диалоговое окно Windows. Работа с HTML-формами поддерживается только в Internet Explorer и Mozilla Firefox.

2.7. IBM Lotus Notes и Domino

Начиная с версии 6.0, IBM Lotus Notes и Domino поддерживают аутентификацию с использованием смарт-карт и их аналогов. При наличии на компьютере драйвера eToken[7] ID-файл, использующийся для аутентификации пользователя или сервера, может быть преобразован таким образом, чтобы его нельзя было применять, не подключая eToken и не вводя PIN-код.

При обращении к защищённому серверу Domino через веб-интерфейс по протоколу HTTPS eToken можно использовать для аутентификации клиента.

Помимо аутентификации, eToken можно использовать в Lotus Notes для подписи и расшифрования электронных писем.

2.8. Microsoft Windows

Аппаратные eToken с функциями смарт-карты можно использовать для интерактивной аутентификации в **домене Windows 2000-Server 2008**. При наличии на компьютере драйверов eToken[7] рабочий стол аутентификации позволяет не только вводить имя пользователя, пароль и имя домена, как обычно, после нажатия клавиш CTRL+ALT+DELETE, но и вместо нажатия этого сочетания клавиш подключать смарт-карту (eToken) и вводить PIN-код. Кроме того, начиная с Windows XP стало возможным использовать смарт-карты, в том числе eToken, для аутентификации при запуске приложений от имени другого пользователя.

Помимо использования eToken в качестве стредства аутентификации, он ещё может использоваться для обеспечения безопасности рабочего места в отсутствие пользователя. Windows 2000–Server 2008 можно настроить таким образом, что компьютер будет блокироваться при отсоединении eToken.

Для использования eToken в качестве средства аутентификации в домене Windows необходим развёрнутый и специально для этого настроенный центр сертификации предприятия (Microsoft Enterprise CA). Средствами eToken генерируется ключевая пара, и центр сертификации выпускает для пользователя сертификат открытого ключа, в котором в политику использования закрытого ключа включён пункт «вход со смарт-картой». После этого администратор может распространить на пользователя объект политики безопасности, запрещающий вход в систему без смарт-карты, в результате чего пользователь не сможет входить в систему без использования eToken, в памяти которого хранится подготовленный сертификат открытого ключа и соответствующий ему закрытый ключ.

2.9. Novell Modular Authentication Service

Novell Modular Authentication Service (**NMAS**) — это компонент Novell eDirectory, обеспечивающий механизмы аутентификации в различных системах

пользователей, зарегистрированных в этой службе каталогов. Начиная с версии 2.1, NMAS позволяет использовать eToken при аутентификации пользователей, на рабочих местах которых установлена операционная система Microsoft Windows 95 Service Release 2B, NT 4.0 SP 6a или позднейшие версии Windows.

2.10. Oracle Application Server

Oracle Application Server поддерживает механизм аутентификации с использованием сертификатов открытого ключа и закрытых ключей. Размещая закрытые ключи пользователей в памяти eToken, можно применять eToken для аутентификации пользователей в Oracle Application Server без использования eToken Single Sign-On.

2.11. Oracle E-Business Suite

Oracle E-Business Suite поддерживает интеграцию с механизмом аутентификации Oracle Application Server Single Sign-On. При использовании такой интеграции возможна аутентификация пользователей Oracle E-Business Suite на основе сертификатов открытого ключа и закрытых ключей в памяти eToken.

Если интеграция с Oracle Application Server Single Sign-On не задействуется, то решение по аутентификации пользователей в Oracle E-Business Suite строится следующим образом:

- аутентификация пользователей на веб-сервере — на основе сертификатов открытого ключа и закрытых ключей в памяти eToken;
- аутентификация пользователей на сервере Forms — с помощью eToken Single Sign-On.

2.12. Token Management System

Token Management System (**TMS**) — разработанное компанией Aladdin Knowledge Systems приложение, позволяющее осуществлять учёт и управление жизненным циклом eToken в масштабах предприятия. TMS интегрируется с Active Directory, связывает учётные записи пользователей с выданными им eToken, а также с выпущенными сертификатами открытого ключа и иными реквизитами. Политики

использования eToken назначаются и применяются точно так же, как политики безопасности в домене Windows. Разработчики различных поддерживающих eToken приложений могут создавать так называемые коннекторы TMS, благодаря которым использование eToken в их приложениях может управляться средствами TMS.

3. Конкурирующие продукты

В зависимости от набора своих функциональных возможностей, разные модели eToken конкурируют на рынке с продукцией различных производителей: ActivIdentity, Arcot, Entrust, Eutron, Feitian, Gemalto, Kobil Systems, MultiSoft, RSA Security (подразделение EMC), Vasco, Актив, БИФИТ, ОКБ САПР и других.

Модели eToken	**Конкурирующие продукты**
USB-ключи eToken GT, eToken PRO и eToken PRO (Java)	ActivIdentity ActivKey SIM USB Token, Entrust USB Tokens, Feitian ePass, Eutron CryptoIdentity, Kobil mIDentity, MS Key, Rutoken ЭЦП, Vasco Digipass Key 1, ПСКЗИ «Шипка», Kaztoken
eToken NG-FLASH	Rutoken Flash
eToken NG-OTP	ActivIdentity ActivKey Display USB Token, Feitian OTP c400, Vasco Digipass 860
eToken PASS	ActivIdentity Mini OTP Token, Entrust IdentityGuard Mini Token, Feitian OTP c100–c300, Kobil SecOVID Token III, RSA SecurID 700, Vasco Digipass Go
смарт-карты eToken PRO и eToken PRO (Java)	ActivIdentity Smart Cards, Feitian PKI card, Gemalto TOP, iBank 2 Key
eToken Virtual	ArcotID

MobilePASS	ActivIdentity Soft Tokens, ArcotOTP, Kobil SecOVID Soft Token, RSA SecurID software tokens, Vasco Virtual Digipass

4. Устаревшие модели

- **eToken R1** — прототип первого USB-ключа eToken, не выпускавшийся серийно
- **eToken R2** — USB-ключ с защищённым микроконтроллером, выпускавшийся фирмой Aladdin Knowledge Systems до 2005 года;
- **eToken RIC** — USB-ключ с защищённым микроконтроллером, выпускавшийся российской компанией Aladdin до 2002 года.

5. Недостатки

Моделям eToken с функциями смарт-карт присущи недостатки, свойственные всем устройствам, в которых PIN-код вводится не с собственной клавиатуры устройства, а с клавиатуры терминала, к которому устройство подключено: с помощью троянской программы злоумышленник может перехватить PIN-код и произвести неоднократное несанкционированное подписывание или шифрование любой информации от имени владельца устройства.

Заключение

В заключение, хочется сказать, что любой здравомыслящий хозяин старается защитить свое жилище от проникновения грабителей. С этой целью, в частности, на входную дверь устанавливается комплект прочных замков. Так неужели компьютеры, содержащие важную и ценную информацию, не нуждаются в надежной защите от возможных нападений недобросовестных сотрудников? Ответ очевиден: нуждаются. И здесь неплохую службу могут сослужить аппаратно-программные средства контроля доступа к компьютерам.

СПИСОК ИСТОЧНИКОВ

https://wreferat.baza-referat.ru/EToken

https://ru.wikipedia.org/wiki/Электронный_ключ