Программно-аппаратные средства обеспечения информационной безопасности

Лекция № 5

Персональное средство аутентификации eToken. eToken API

Рахманенко И.А.

Сертифицированные USB-ключи и смарт-карты

- Сертифицированные электронные ключи eToken являются программно-аппаратным средством аутентификации и хранения ключевой информации и средством защиты информации от несанкционированного доступа.
- Сертифицированные электронные ключи eToken являются рекомендуемым носителем ключевой информации для сертифицированных СКЗИ российских разработчиков.
- Электронный ключ eToken ГОСТ соответствует требованиями ФСБ России к СКЗИ класса КС2 и может использоваться для защиты информации, не содержащей сведений, составляющих государственную тайну (Сертификат соответствия № СФ/124-1671 от 11 мая 2011 г.).

Двухфакторная аутентификация

- Электронные ключи eToken могут использоваться в любых приложениях для замены парольной защиты на более надежную двухфакторную аутентификацию.
- Например, если для аутентификации пользователю необходимо предоставить USB-ключ и ввести пароль, то злоумышленник не сможет получить доступ к данным, так как ему нужно не только подсмотреть пароль, но и предъявить физическое устройство, кража которого быстро обнаружима.

Особенности eToken

- **Строгая двухфакторная аутентификация** пользователей при доступе к защищенным ресурсам (компьютерам, сетям, приложениям)
- **Аппаратное выполнение криптографических операций** в доверенной среде (в микросхеме ключа: генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, выработка электронной подписи)

Особенности eToken

- **Безопасное хранение критически важных данных** – криптографических ключей, профилей пользователей, настроек приложений, цифровых сертификатов и пр. в энергонезависимой памяти ключа
- **Сертифицированные версии** для защиты информации в АС до класса защищенности 1Г включительно и для защиты персональных данных в ИСПДн до 1 класса включительно

Возможности кастомизации

- **Интеграция с системами контроля доступа** – все USB-ключи и смарт-карты могут выпускаться со встроенными пассивными радио-метками RFID для контроля доступа сотрудников в помещения.
- **Корпуса с логотипом** – возможно изготовление корпусов USB-ключей с объемным логотипом заказчика.
- **Печать логотипа заказчика** – на USB-ключи возможно нанесение логотипа заказчика методом тампопечати, на смарт-карты возможно нанесение фотографии сотрудника, либо логотипа организации.
- **Различные цвета корпуса** – по желанию заказчика USB-ключи могут быть выполнены в корпусе другого цвета.

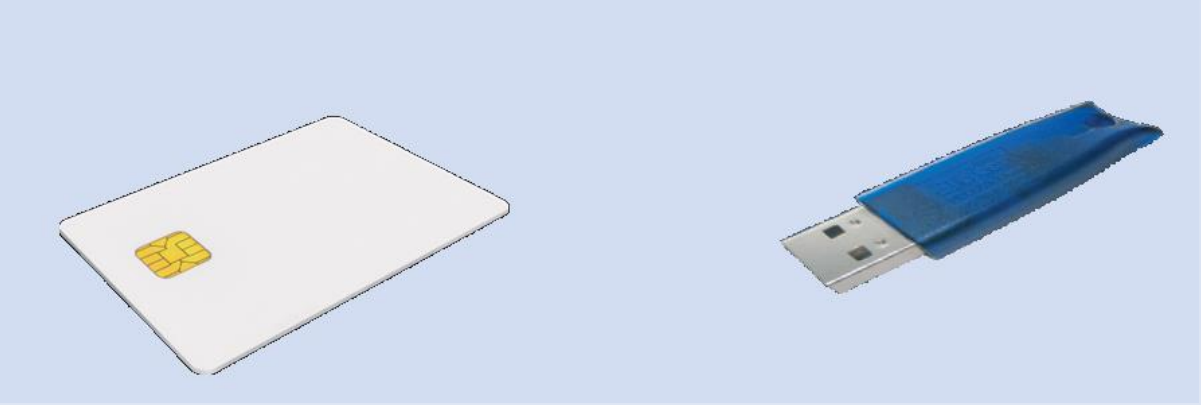
Технические характеристики

Харатеристика	Значение
Объем защищенной памяти	72 КБ на микросхеме смарт-карты
Поддерживаемые ОС	Microsoft Windows 2000/2003/XP/ Vista/2008/2008 R2/7 (32 и 64-битные версии); Linux; Mac OS Одноразовые пароли могут использоваться в любой операционной среде
Срок хранения данных в памяти	Не менее 10 лет
Количество циклов перезаписи памяти	Не менее 500,000

МОДЕЛЬНЫЙ РЯД

eToken PRO (Java)

- eToken PRO (Java) – персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью, выпускается в виде USB-ключа и смарт-карты.



eToken PRO (Java)

- eToken PRO (Java) является следующим поколением электронных ключей eToken PRO. По сравнению с ними eToken PRO (Java) имеет увеличенный объем памяти для защищенного хранения пользовательских данных и предоставляет возможность расширения функционала за счет загрузки дополнительных приложений (Java - апплетов).

eToken PRO (Java)

- **Рекомендуется для решения следующих задач:**
- обеспечение строгой двухфакторной аутентификации пользователей в операционных системах и бизнес-приложениях (Microsoft, Citrix, Cisco Systems, IBM, SAP, Check Point), защищенное хранение ключевой информации российских СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.);

eToken PRO (Java)

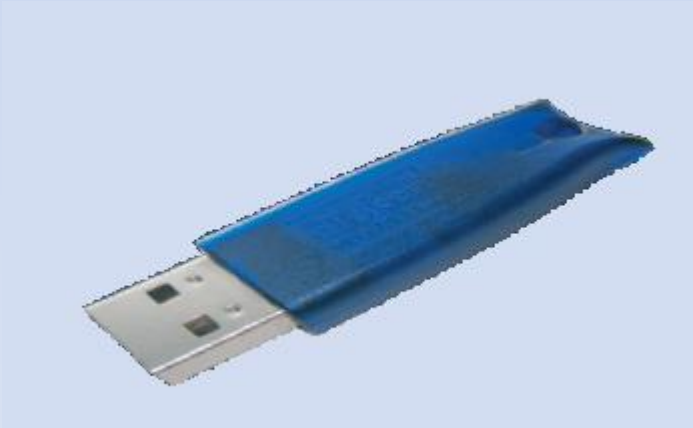
- **Рекомендуется для решения следующих задач:**
- защита ключей электронной подписи пользователей в системах электронного документооборота, формирование электронной подписи документов и транзакций, обеспечение безопасной работы с электронной почтой;
- защита закрытых ключей электронной подписи пользователей систем дистанционного банковского обслуживания.

eToken PRO (Java)

- Смарт-карты eToken PRO (Java) со встроенными радио-метками RFID, напечатанным логотипом компании, фотографиями сотрудников могут использоваться в качестве единых карт для контроля физического доступа в помещения и контроля логического доступа к информационным ресурсам.

eToken PRO Anywhere

- eToken PRO Anywhere – USB-ключ для безопасного доступа к Web-ресурсам с любого компьютера без предварительной установки ПО.



eToken PRO Anywhere

eToken PRO Anywhere предоставляет следующие сервисы безопасности:

- автоматический запуск браузера и открытие заранее заданных Web-сайтов, адреса которых хранятся в защищенной памяти устройства;
- аутентификация пользователя в рамках протокола SSL/TLS и защита всех данных, передаваемых по сети Интернет;
- защита от фишинга и атак «человек посередине».

eToken PRO Anywhere

Рекомендуется:

- поставщикам on-line услуг для предоставления клиентам безопасного доступа к Web-ресурсам без установки клиентского ПО;
- организациям – для предоставления своим сотрудникам удаленного доступа к корпоративным порталам и электронной почте с возможностью использовать электронной подписи с любых компьютеров;
- для снижения нагрузки на службы технической поддержки по вопросам удаленного доступа.

eToken NG-FLASH (Java)

- eToken NG-FLASH (Java) – комбинированный USB-ключ, обладающий функциональными возможностями eToken PRO (Java), и оснащенный дополнительным модулем Flash-памяти объемом до 16 ГБ.

eToken NG-FLASH (Java)

Дополнительная Flash-память устройства позволяет хранить данные в зашифрованном виде и может быть использована для:

- доверенной загрузки операционных систем Microsoft Windows или Linux (образ операционной системы записывается в память устройства);
- хранения и запуска предварительно сконфигурированной виртуальной машины (VMWare, Virtual PC) с предустановленным набором ПО и настроенными параметрами безопасности;
- автоматического запуска приложений из памяти устройства;
- безопасного хранения, транспортировки и резервного копирования данных;
- запуска безопасного предварительно настроенного браузера.

eToken NG-FLASH (Java)

Рекомендуется:

- администраторам безопасности, аудиторам ИБ – для создания временных центров по оценке защищенности информационных систем, оценке их соответствия требованиям нормативных документов;
- компаниям, работающим через агентскую сеть (страхование, кредитование) – для создания агентских рабочих мест по обслуживанию клиентов;
- разработчикам ПО – для распространения / тиражирования программного обеспечения;
- всем пользователям – для безопасного хранения, транспортировки и резервного копирования данных.

eToken NG-OTP (Java)

- eToken NG-OTP (Java) – комбинированный USB-ключ с генератором одноразовых паролей (One-Time Password – OTP). Обладает всем функционалом eToken PRO (Java) для использования в PKI-системах, а также может работать без подключения к компьютеру как автономный генератор одноразовых паролей.

eToken NG-OTP (Java)

Одноразовый пароль может быть использован для:

- аутентификации пользователей при удаленном VPN-доступе, доступе к Web-серверам, опубликованным Web-приложениям;
- подтверждения платежных операций.

eToken NG-OTP (Java)

- **Рекомендуется:**
- сотрудникам организаций, которым требуется постоянный удаленный доступ к информационным ресурсам вне зависимости от типа используемого для выхода в Интернет устройства;
- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- разработчикам систем ДБО – для создания конкурентоспособных систем ДБО, позволяющих банкам, использующим эти системы, повышать уровень доступности предоставляемых услуг.

eToken PASS

- eToken PASS – автономный генератор одноразовых паролей, не требующий подключения к компьютеру. Является более дешевой альтернативой eToken NG-OTP (Java), без возможности использования в PKI-системах.

eToken PASS

Рекомендуется:

- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- разработчикам систем ДБО – для создания конкурентоспособных систем ДБО, позволяющих банкам, использующим эти системы, повышать уровень доступности предоставляемых услуг;
- поставщикам on-line услуг – для аутентификации доступа подписчиков и максимального расширения аудитории;
- пользователям мобильных устройств (телефонов, смартфонов, коммуникаторов).

eToken ГОСТ

eToken ГОСТ – персональное средство криптографической защиты информации для формирования электронной подписи по ГОСТ Р 34.10-2001 с неизвлекаемым закрытым ключом, выполненное в виде USB-ключа или смарт-карты.

eToken ГОСТ

Использование eToken ГОСТ в составе существующих и разрабатываемых информационных систем повышает их защищенность и обеспечивает соответствие требованиям российского законодательства в части защиты информации.

eToken ГОСТ

Аппаратная реализация российских криптографических алгоритмов и протоколов:

- ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка электронной цифровой подписи);
- ГОСТ Р 34.11-94 (вычисление значения хэш-функции);
- ГОСТ 28147-89 (зашифрование/расшифрование блоков данных, вычисление имитовставки);
- генерация последовательности случайных чисел;
- выработка ключа парной связи по алгоритму Диффи-Хеллмана согласно RFC 4357.

eToken ГОСТ

Рекомендуется:

- разработчикам систем ДБО, электронных торговых площадок, систем сдачи налоговой отчетности – для обеспечения безопасности закрытых ключей электронной подписи пользователей этих систем;
- разработчикам СКЗИ – для использования в своих СКЗИ аппаратно реализованных российских криптографических алгоритмов, генератора ПСЧ, а также обеспечения неизвлекаемого хранения закрытых ключей;
- разработчикам СЗИ – для встраивания СКЗИ eToken ГОСТ в создаваемые ими продукты.

eToken ГОСТ

- eToken ГОСТ имеет сертификат ФСБ России по классам защиты КС1 и КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

КриптоПро eToken CSP

- КриптоПро eToken CSP – аппаратно-программное средство формирования квалифицированной электронной подписи с неизвлекаемым закрытым ключом.

КриптоПро eToken CSP

- Данное решение обеспечивает полный набор криптографических операций, реализованных в СКЗИ КриптоПро CSP 3.6 и полную интеграцию с инфраструктурой PKI на базе КриптоПро УЦ. При этом все операции с закрытыми ключами электронной подписи выполняются аппаратно, а сами закрытые ключи никогда не покидают устройство и не могут быть перехвачены.

КриптоПро eToken CSP

СКЗИ КриптоПро eToken CSP рекомендуется для использования в:

- автоматизированных системах органов государственной власти и местного самоуправления;
- системах защищенного юридически значимого электронного документооборота – для аутентификации
- пользователей и формирования электронной подписи;
- системах клиент-банк, электронных торгов – для подтверждения платежных операций;
- проектах с социальной / идентификационной картой;
- системах мобильных платежей.

Приложения eToken

- Check Point VPN-1 SecuRemote
- eToken Network Logon
- eToken SafeData и «Крипто БД»
- eToken Single Sign-On
- Аутентификация (Oracle, SAP, Lotus Notes, Windows и т.д)
- Token Management System

Недостатки eToken

- с помощью троянской программы злоумышленник может перехватить PIN-код и произвести неоднократное несанкционированное подписывание или шифрование любой информации от имени владельца устройства (необходима встроенная клавиатура или доверенный терминал)

JaCarta

- JaCarta – новое поколение смарт-карт, USB-, MicroUSB- и Secure MicroSD-токенов для строгой аутентификации, электронной подписи и безопасного хранения ключей, цифровых сертификатов (смена eToken)

JaCarta. Аутентификация

- Строгая двух- и трёхфакторная аутентификация
- Биометрическая идентификация
- Неотчуждаемость токена от его владельца
- Строгая аутентификация для Web-порталов и облачных сервисов
- Электронное удостоверение сотрудника (интеграция со СКУД, визуальная идентификация владельца)
- Штатная работа в существующей PKI-инфраструктуре (если на предприятии не развёрнута PKI-инфраструктура и нет собственного центра сертификации, для работы токенов и смарт-карт используйте JaCarta SecurLogon)

JaCarta. Электронная подпись

- Персональное средство ЭП с неизвлекаемым ключом и аппаратной поддержкой национальной криптографии
- Электронная подпись для мобильных устройств
- Электронная подпись в недоверенной среде
- Электронная подпись для Web-порталов и "облачных" сервисов
- Электронное удостоверение сотрудника на "зарплатной" карте (Visa / MasterCard)

JaCarta. Безопасное хранение ключевой информации

- Хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP, VipNet CSP и др.)
- Хранение лицензий, цифровых сертификатов в защищённой области памяти токена
- Возможность использования JaCarta с более чем 100 продуктами технологических партнёров и компаний-разработчиков ПО

JaCarta. Поддержка биометрии

Реализованная в продукте технология идентификации человека по отпечаткам пальца (Biometric Match-On-Card) может использоваться для:

- повышения удобства работы – вместо ввода PIN-кода при аутентификации и работы с электронной подписью (КриптоПро CSP);
- повышения надёжности аутентификации (как третий фактор);
- предотвращения использования карты/токена другим лицами

JaCarta. Поддержка биометрии

JaCarta-2 ГОСТ

- Новое поколение USB-токенов, смарт-карт и модулей безопасности с аппаратной поддержкой ГОСТ Р 34.10-2012и ГОСТ Р 34.11-2012
- Дополнительный PIN-код на операцию формирования ЭП (снижает вероятность ошибочных действий)

JaCarta-2 ГОСТ

- Новые механизмы защиты от атак и блокирования
- В новом устройстве JaCarta-2 ГОСТ реализованы защита от атак на PIN-код и от блокирования устройства, а PIN-код Администратора заменён ключом администратора безопасности.
- Ранее нельзя было использовать заблокированный токен, теперь можно (с очисткой)

ETOKEN API

eToken API

Для использования eToken в разрабатываемом ПО существует 3 вида API:

- PKCS#11
- CAPI
- SAPI

PKCS#11

- PKCS#11 (Public-Key Cryptography Standard - Стандарт криптографии с открытым ключом)
- Разработан RSA Laboratories
- Включает в себя как зависимые от алгоритма, так и не зависимые стандарты разработки.
- Промышленный стандарт, который задает интерфейс для криптографических устройств, таких как смарт-карты и карты PCMCIA.

PKCS#11

- Определяет API (application programming interface - интерфейс программирования приложений), называемый Cryptoki (Cryptographic Token Interface), для устройств, физических или виртуальных, содержащих криптографическую информацию (ключи или данные) и выполняющих криптографические функции.

PKCS#11

- Этот API используется на многих платформах и обладает достаточными возможностями для большинства приложений, связанных с безопасностью.
- Компания Аладдин рекомендует использовать PKCS#11 в качестве основного API для программирования eToken.

CAPI (CryptoAPI)

- Разработан компанией Microsoft в качестве части операционных систем Microsoft Windows.
- Позволяет одновременно использовать несколько криптопровайдеров (cryptographic service providers, CSP) на одном компьютере или в одном приложении.

CAPI (CryptoAPI)

- Позволяет ассоциировать конкретный криптопровайдер с конкретной смарт-картой, так чтобы приложения вызывали корректный криптопровайдер при работе с криптографией.
- Windows содержит много вспомогательных функций, позволяющих упростить код при работе с криптографией или сложными структурами данных (например сертификатами).

SAPI

- SAPI (Supplementary API – дополнительный API) был реализован в версии eToken RTE 3.60 для того, чтобы убрать необходимость в использовании низкоуровневых функций при работе с eToken.
- Он давал доступ к специфичным для eToken возможностям, не рассматриваемым в стандарте PKCS#11. В настоящий момент, этот функционал теперь доступен в PKCS#11 API.

Выбор API

- PKCS#11 позволяет управлять несколькими eToken одновременно. В CAPI нет понятия физического токена (необходимо использовать специальные техники).
- PKCS#11 позволяет ожидать уведомлений о подключении/удалении eToken. CAPI не обладает такой возможностью (возможность есть через Win32 API).

Выбор API

- PKCS#11 позволяет хранить ключи RSA, сертификаты и данные на eToken. CAPI позволяет хранить только ключи RSA и соответствующие им сертификаты.
- В PKCS#11 нет вспомогательных функций для работы с сертификатами. Обработка и проверка сертификатов X.509 может быть довольно сложной задачей. Однако, работая в ОС Windows, имеется возможность использовать функции Win32 даже работая с PKCS#11.

Выбор API

- PKCS#11 - это API, а не архитектура. Если приложению требуется работать с несколькими провайдерами, оно само должно определить как взаимодействовать с ними. CAPI является частью ОС Windows и поэтому, как только новый провайдер установлен в систему, он автоматически становится доступен для всех приложений.

Выбор API

- В CAPI имеется множество вспомогательных функций. Они могут помочь программисту сконцентрироваться на логике работы приложения, не сталкиваясь с низкоуровневыми проблемами.

Слоты eToken

- Чтобы получить информацию о подключенном eToken, необходимо знать идентификатор виртуального слота, к которому подключен eToken.
- USB порт является слотом в данном API.
- Состояние слота показывает, подключен ли к нему eToken.

Слоты eToken

- Позволяют получить информацию о eToken

```
Slot#1 - AKS ifdh 1                          : Token was removed


Slot#1 - AKS ifdh 1                          :
      <Common Token Information>
            Label: SSV
            Manufacturer: Aladdin Knowledge Systems Ltd.
            Model: eToken
            Serial number: 4059ae0c
            Version hardware/firmware: 1.2, 0.4
            Current session count: 0
            Maximum session count: 0
            Maximum RW session count: 0
            PIN length: [12..255]
            Public memory: 4303/16384 bytes
            Private memory: 4303/16384 bytes
            Random number generator: Yes
            Is write protected: No
            Login required: Yes
            User's PIN is set: Yes
            Restore key is not needed: No
            Clock on token: No
            Has protected authentication path: No
            Dual crypto operations: Yes
```

Функции eToken API

Функции по работе с объектами

- Создание объектов на eToken;
- Получение значений атрибута объекта;
- Изменение значения атрибута объекта;
- Поиск объектов на eToken;
- Удаление объекта;
- Копирование объекта.

Криптографические функции…

Объекты eToken

- **CKO_DATA**. Объект типа данные, может содержать любую информацию, которая может использоваться сторонними приложениями. В случае наличия атрибута CKA_PRIVATE, объект будет скрыт до момента ввода ПИН-кода пользователя.
- **CKO_CERTIFICATE**. Объект – сертификат открытого ключа (поддерживаются только сертификаты X.509). Бывают двух категорий, обычный сертификат (CKA_CERTIFICATE_CATEGORY=0) и сертификат Центра Сертификации (CKA_CERTIFICATE_CATEGORY=2).

Объекты eToken

- **CKO_PRIVATE_KEY, CKO_PUBLIC_KEY**. Объекты – закрытый и открытый ключи шифрования. eToken PRO поддерживает только алгоритм и ключи RSA. Экспорт закрытого ключа с токена в целях обеспечения безопасности не поддерживается.
- **CKO_SECRET_KEY**. Объект – секретный ключ симметричного алгоритма шифрования. Поддерживаются алгоритмы DES, DES2, DES3, HOTP, AES, RC4. Можно задать в атрибутах тип алгоритма CKK_GENERIC_SECRET, в случае наличия требований дополнительной защиты для ключа шифрования, реализация которого не поддерживается токеном.

Шаблоны объектов eToken

- Для работы с объектами используются шаблоны – объекты типа CK_ATTRIBUTE, содержащие набор атрибутов, свойственных либо конкретному типу объектов, либо общие для всех объектов.

Шаблоны объектов eToken

- Для различных видов объектов характерны различные шаблоны.
- Для всех типов объектов могут быть заданы атрибуты:
  - CKA_CLASS – класс объекта;
  - CKA_TOKEN – объект находится на токене, если истина (всегда истина для аппаратных токенов);
  - CKA_VALUE – значение, содержит хранимую объектом информацию (необязательный атрибут);
  - CKA_LABEL – метка объекта (название);
  - CKA_APPLICATION – идентификатор приложения, которое работает с объектом;
  - CKA_PRIVATE – объект приватный, если истина, он не виден до момента аутентификации пользователя.

Шаблон сертификата

```
CK_ATTRIBUTE templateArray [] =
        {
                {CKA_CLASS, &classAttr, sizeof(classAttr)},
                {CKA_CERTIFICATE_TYPE, &certType,
sizeof(certType)},
                {CKA_TOKEN, &trueVal, sizeof(trueVal)},
                {CKA_SUBJECT, subject, subjSize },
                {CKA_VALUE, (void *)cert, certSize },
                {CKA_CERTIFICATE_CATEGORY, (void
*)&certCategory, sizeof (certCategory) },
        };
```

Рассмотренные вопросы

- Персональное средство аутентификации eToken
- eToken API