



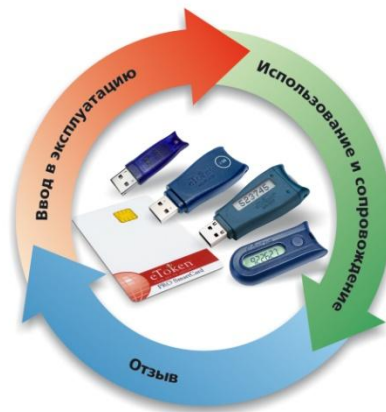
# Средства строгой аутентификации в новой парадигме: от защиты объекта - к защите взаимодействия



Руководитель направления контент-безопасности Владимир Бычек  
v.byчек@aladdin.ru

Киев, 22 апреля 2010 года

# Средство аутентификации -> eToken



Система -> ДБО

eToken & Solutions





# Ключи eToken Java

- Содержат Java карту, полностью соответствующую спецификациям Java Card (SUN) и Global Platform
  - Java Card Platform Specification 2.2.1 (<http://java.sun.com/products/javacard/>)
  - Global Platform (<http://www.globalplatform.org>)
- В карту могут быть загружены разнообразные апплеты, реализующие:
  - Западные криптографические алгоритмы (eToken PRO)
  - Российские криптографические алгоритмы (eToken ГОСТ)
  - Другие национальные криптографические алгоритмы
  - Дополнительные апплеты независимых разработчиков
- Модельный ряд ключей eToken
  - eToken PASS (Генератор одноразовых паролей)
  - eToken PRO (Java) (USB-ключ/смарт-карта)
  - eToken NG-OTP (Java) (Комбинированный USB-ключ с генератором одноразовых паролей)
  - eToken NG-FLASH (Java) (Комбинированный USB-ключ с дополнительным модулем flash-памяти)
  - eToken Anywhere (USB-ключ нового поколения)





# eToken PASS

## eToken PASS – аппаратный OTP токен

- Решает проблемы
  - Кражи регистрационных данных клиента
  - Перехвата SMS с одноразовым паролем
  - Мобильности (ПК, КПК, телефон ...)
- Плюсы решения
  - + Генерация ключа OTP в токене
  - + Аутентификация на Radius сервере или в приложении
  - + Удобство использования
  - + Простота встраивания (1-2 дня)
  - + Невысокая цена
- Минусы решения
  - Подтверждение только факта транзакции, но не ее содержания





# eToken PRO (Java)

eToken PRO (Java) – защищенное хранилище ключей и сертификатов

- Позволяет
  - Значительно снизить вероятность компрометации ключей ЭЦП
  - Обеспечить усиленную двухфакторную аутентификацию
- Плюсы решения
  - + Высокая защищенность хранимых данных
  - + Соответствие ряду международных стандартов - Common Criteria EAL4+, VISA, USB 2.0
  - + Реализация ряда западных криптографических алгоритмов
  - + Нативная поддержка eToken в популярных информационных системах и приложениях (Windows, Lotus Notes Domino, Oracle etc.)
  - + Поддержка большинства СКЗИ, сертифицированных как в России, так и странах бывшего СНГ (Казахстан, Беларусь)
  - + Невысокая цена
- Минусы решения
  - В процессе подписи электронного документа закрытый ключ покидает токен и может быть дискредитирован



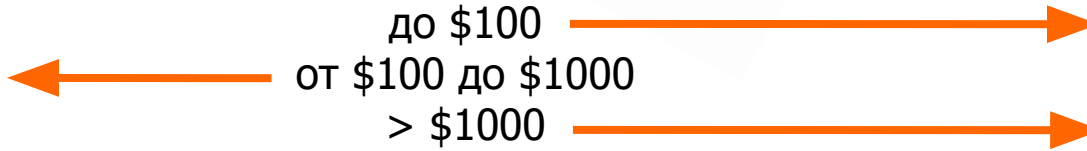


# eToken NG-OTP (Java)

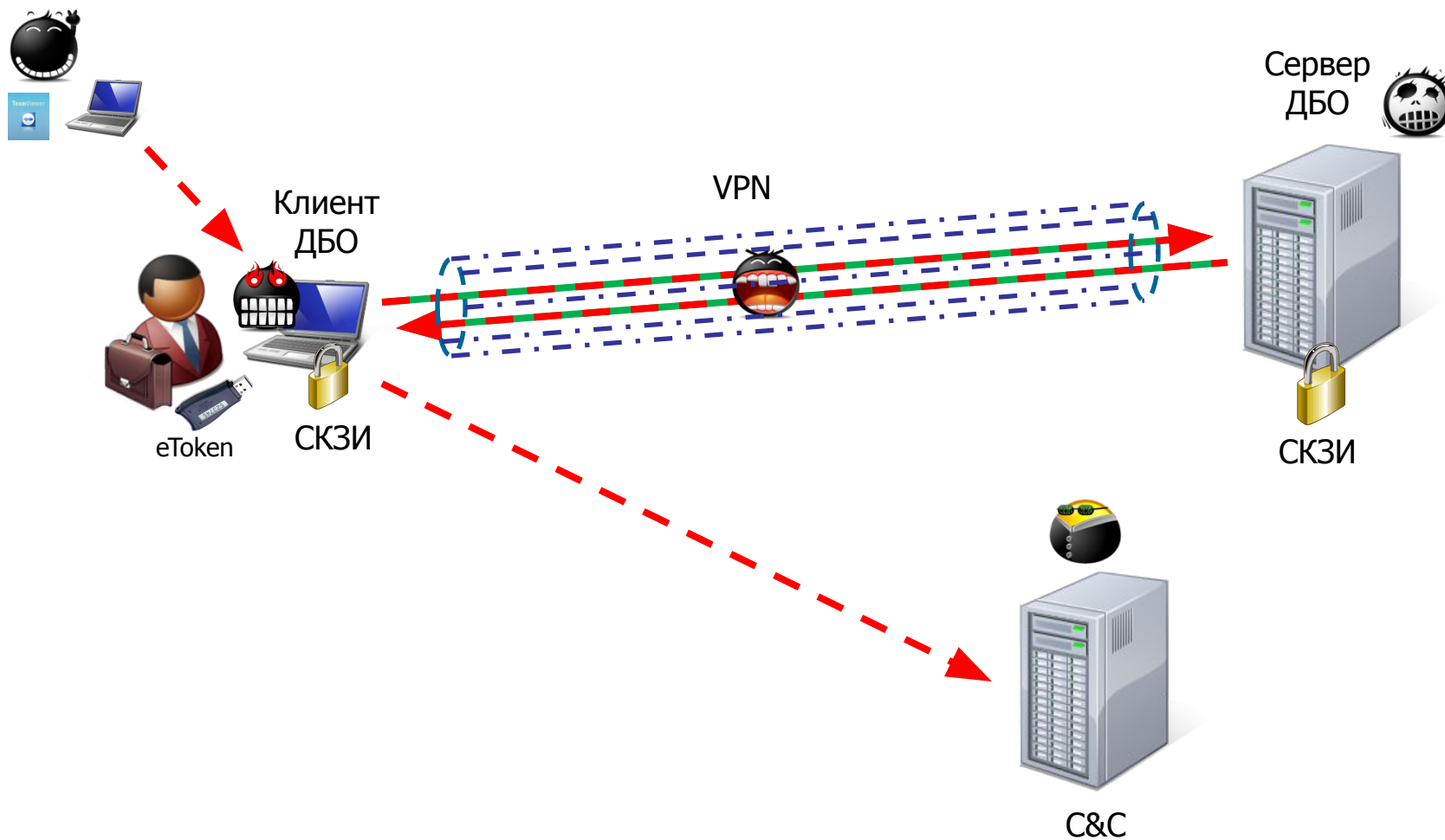
eToken NG-OTP (Java) - Комбинированный USB-ключ с генератором одноразовых паролей



“Вес” транзакц.  
до \$100  
от \$100 до \$1000  
> \$1000



# Типичная система ДБО



# Наглядный пример атаки



PC Week Украина - Поиск... x PC Всего 3 дня до конферен... x О попытках хищений с ис... x

http://dom.bankir.ru/showthread.php?t=99228

Российская VISA: быть или не быть

Доллар и евро снижаются к рублю на ММВБ (2)

Комитет ГД рекомендовал переназначить двух членов совета директоров ЦБ (3)

Судьба ставки решится скоро (1)

Банковский форум > Технологический департамент > Электронный банкинг

О попытках хищений с использованием USB-токенов "iBank 2 Key"

Имя Имя  Заполнить?  
Пароль

Регистрация Дневники  Справка Пользователи Календарь Сообщения за день Поиск

Электронный банкинг: Обзорные проблемы построения и развития систем Internet-banking, Unified Web-banking, Tel-banking, Swift и т.д. Безопасность и юридическая сторона вопроса. Проблемы сферы банковского сотрудничества.

Добро пожал

Если это ваш

ответить

Перейти к но

09.04.2010, 12:

Дмитрий Банзир

Регистрация: 07  
Адрес: Москва,  
Сообщений: 1,1

Во всех выявленных случаях злоумышленники пользовались халатностью клиентов, оставляющих USB-токены "iBank 2 Key" **постоянно (круглосуточно) подключенными к компьютеру.**

Поскольку использование USB-токенов "iBank 2 Key" исключает хищение секретных ключей ЭЦП клиентов, все выявленные попытки хищений средств осуществлялись только в моменты, когда USB-токен был подключен к клиентскому компьютеру.

Для этого злоумышленники использовали следующие механизмы:

- Программы для дистанционного управления компьютером клиента (Microsoft Remote Assistant, TeamViewer, RAdmin и др.). Злоумышленник с помощью трояна запускал на компьютере клиента программу для дистанционного управления, подключался к данному компьютеру, загружал и запускал на нем Java-апплет Интернет-Банкинга, от имени клиента создавал и подписывал платежные документы с использованием постоянно подключенного к компьютеру USB-токена.
- Новая разновидность трояна, который предоставляет удаленный доступ к USB-портам компьютера, а также осуществляет туннелирование TCP-трафика с компьютера злоумышленника через компьютер клиента до банковского Сервера Приложения "iBank 2". При этом Java-апплет Интернет-Банкинга загружается и исполняется на компьютере злоумышленника, а для входа в систему "iBank 2" и формирования ЭЦП клиента под платежными документами используется удаленный доступ к USB-портам компьютера клиента с постоянно подключенным USB-током.

злоумышленника, а для входа в систему "iBank 2" и формирования ЭЦП клиента под платежными документами используется удаленный доступ к USB-портам компьютера клиента с постоянно подключенным USB-током.

**Выводы:**

1. Ни в одном из случаев секретный ключ ЭЦП корпоративного клиента не был похищен из USB-токена "iBank 2 Key". Во всех случаях злоумышленники подписывали документы, используя удаленный доступ к компьютеру корпоративного клиента или к "расшаренным" USB-портам компьютера клиента.

ПУСК

Microsoft Office O... Подготовку к семин... О попытках хищени... 2 Microsoft Office P... RU 16:16





# Особенности “толстого” клиента

Что получает клиент после заключения договора:

- Клиентское ПО
- Аппаратный ключ ( в хорошем случае)
- ПО СКЗИ (драйверы etc.)
- Руководство пользователя



- Не доверенная среда
- Не контролируемая среда

Почему не контролируемая среда?

- Мы изначально не знаем конфигурации ПК клиента
- Мы не знаем какие программы клиент устанавливает на свой ПК и тем более не знаем какие программы устанавливаются без его ведома

Почему не доверенная среда?

- Мы не знаем насколько аккуратно клиент будет выполнять рекомендации, данные ему вместе с ПО и аппаратным ключом
- Мы не знаем на какой ПК и с какого носителя будет устанавливаться ПО
- Мы только ограниченно можем влиять на процесс установки необходимых дополнений компонентов системы (ДБО, СКЗИ, ОС)



# eToken NG-FLASH (Java) - Сценарии

eToken NG-FLASH (Java) – комбинированный USB-ключ

eToken PRO (Java) + 1, 2, 4, 8\*, 16\* Гб флэш памяти (две области – только чтение и чтение/запись) на борту

## Сценарий 1

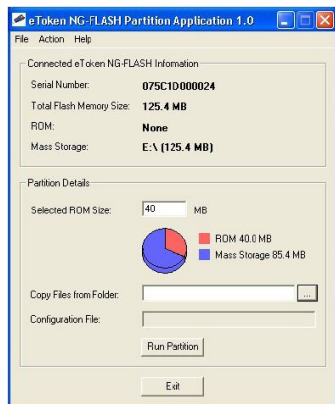
Автоматическая загрузка и установка необходимых драйверов и ПО из защищенной области eToken на любом ПК с ОС Windows (XP, Vista, 7)

### Достоинства

- Корректная установка драйверов и ПО на любой ПК (netbook, например)

### Недостатки

- Практически никакие проблемы безопасности не решены



### USB CD-ROM:

- Дистрибутив системы ДБО
- Криптопровайдер
- Драйверы eToken

### Flash-часть:

- Любая необходимая информация





# eToken NG-FLASH (Java) - Сценарии

## Сценарий 2

Загрузка специализированной операционной системы клиентского ПК из защищенной области eToken NG-Flash

### Достоинства

- Предустановленные системы ДБО и СКЗИ в среде специализированной операционной системы
- Существенно более низкая вероятность заражения вредоносным кодом
- Гарантированная корректная работа СКЗИ и ДБО в среде специализированной ОС

### Недостатки

- Серьезные ограничения на выполняемые в среде специализированной ОС программы – необходимость специализированной версии клиента ДБО
- Возможность для пользователя взаимодействовать с ресурсами ПК
- Сложная процедура выполнения обновлений программ, выполняемых в среде специализированной ОС
- Более высокая цена решения за счет стоимости лицензии (в случае установки ОС Microsoft)





# eToken NG-FLASH (Java) - Сценарии

## Сценарий 3

Загрузка ОС Linux с eToken NG-Flash

Запуск VMware Player в среде Linux

Запуск ОС Windows (XP, Vista, 7) в среде VMware ACE

## Достоинства

- Предустановленные системы ДБО и СКЗИ в привычной среде ОС Windows
- Отсутствие ограничений на устанавливаемые программы
- Возможность надежного изолирования пользователя от всех внутренних (ПК) и внешних (Интернет) ресурсов, кроме сервера ДБО = **обеспечению доверенной среды в любом не доверенном окружении**
- Удобство использования

## Недостатки

- Высокая цена решения (сравнимая со средним netbook), вызванная необходимостью лицензирования VMware ACE и Microsoft Windows

Несмотря на высокую цену, в одном из крупнейших банков России идет работа по разработке соответствующего решения на базе eToken NG-Flash. Подобное решение разработано компаниями Aladdin и Almittech еще в 2008 году.



# “Тонкий” клиент и eToken Anywhere

## Особенности ДБО, использующих “тонких” клиентов

- Клиентом ДБО является браузер
- Для взаимодействия СКЗИ с аппаратным ключом используются ActiveX или Java компоненты, предустановленные либо загружаемые в начале сеанса работы

## eToken Anywhere – новый уровень мобильности и безопасности

- Полный Plug & Play
- Минимизация возможности фишинга (URL, к которым обращается устройство, содержатся в памяти ключа)
- Строгая аутентификация клиента и сервера
- Повышенная защищенность от вредоносного кода
- Устранение всех следов с ПК, на котором производилась работа с системой ДБО





# eToken Anywhere – как это работает


## Алгоритм работы eToken Anywhere

- После включения eToken Anywhere в порт он распознается системой как CD ROM, с которого выполняется загрузка предустановленного приложения
- Выполняется проверка наличия на ПК установленного приложения PKI Client
- Если приложение установлено, eToken переводится в режим PRO и далее работает в этом режиме
- Если приложение не установлено, с жестко прописанного в ключе URL выполняется загрузка mini PKI Client, целостность которого удостоверяется путем проверки ЭЦП
- eToken Anywhere переводится в HID режим
- Mini PKI Client регистрируется в браузере по умолчанию (IE или Firefox)
- Выполняется сеанс ДБО
- При корректном завершении сеанса (извлечение ключа или выход из программы через пиктограмму в трее) mini PKI Client выгружается из системы
- При повторном включении алгоритм в точности повторяется



Вопросы?





# Благодарю за внимание!

Руководитель направления контент-  
безопасности Владимир Бычек  
[v.byчек@aladdin.ru](mailto:v.byчек@aladdin.ru)