



Использование токенов с аппаратной реализацией ЭЦП для обеспечения безопасности Web- сервисов

*С.А. Белов, руководитель
стратегических проектов, Aladdin*

Москва, 11 декабря 2008

Введение

- *Чтобы внедрить СЭД, необходим административный ресурс*

Из интервью одного из разработчиков СЭД

- *Удобство и простота использования имеют особое значение.*

Если пользователям неудобно или сложно работать в СЭД, то внедрение почти наверняка закончится неудачей

ТРЕБОВАНИЯ MoReq2

Общая схема электронного документооборота с использованием WEB-доступа



Существуют две альтернативные технологии для использования специальных программ, загружаемых на рабочую станцию с сервера и выполняющихся в окне Web-браузера : JAVA приложения (апплеты) и ActiveX



Проблемы безопасного использования Web-доступа

- Аутентификация сторон
 - Взаимная
 - Двухфакторная
 - Строгая
- Конфиденциальность и целостность всех данных, передаваемых по сетям общего пользования
 - Построение защищённого канала (SSL, TLS)
- Юридическая значимость, неотказуемость от совершённых действий
 - ЭЦП
- Области использования
 - Электронные платежи («Клиент-Банк», Интернет-банкинг)
 - Электронный документооборот
 - Электронный архив

ЭЦП на удалённой рабочей станции

- Проблемы
 - Неконтролируемая среда
 - Недоверенная среда
- Решение
 - Применение персональных средств (токенов) для аппаратного формирования ЭЦП
- Преимущества токенов
 - Аппаратная реализация ЭЦП по ГОСТ Р 34.10-2001
 - Незвлекаемое хранение закрытого ключа ЭЦП
 - Подключение по USB
 - Поддержка различных платформ: Windows, Linux, MAC OS X



Решение компании Аладдин

Рабочая станция



Сеть общего пользования

Web-сервис



- eToken Java – новое поколение токенов
 - Неизвлекаемое хранение закрытых ключей и аппаратная реализация ЭЦП по ГОСТ Р 34.10-2001
 - Строгая аутентификация пользователя при установлении сеанса связи (SSL, TLS)
 - Формирование ЭЦП передаваемых на сервер транзакций (данных форм)

eToken Java – новое поколение электронных ключей для ЭЦП

- eToken PRO на основе Java-карты
 - Форм-факторы USB-ключа и смарт-карты
- Апплет Криптотокен
 - Генерация и неизвлекаемое хранение ключей ЭЦП
 - Формирование ЭЦП по ГОСТ Р 34.10-2001
- Криптографические функции доступны через:
 - APDU-команды
 - Интерфейс прикладного программирования PKCS#11
- CCID-совместимое устройство
 - Драйвера в составе Windows Vista, Linux, MAC OS X





Преимущества

- Не требуется установка ПО на рабочей станции пользователя
 - Драйвера устройств (входят в состав ОС)
 - СКЗИ (криптографические функции выполняются токеном)
 - Необходим только браузер (входит в состав ОС)
- Любая платформа
 - Windows (2000, XP, Vista, 32 и 64-бит), Linux, MAC OS X
- Незвлекемый закрытый ключ и аппаратная реализация ЭЦП по ГОСТ Р 34.10-2001
- Стоимость на 1 рабочее место – менее 1000 руб.



Планы по сертификации eToken Java

- **Сертификация**
 - Common Criteria EAL4+
 - VISA
 - CAST
 - USB 2.0
- Сертификация во ФСТЭК России - проводится
- Сертификация в ФСБ России - проводится
- Сертификация на Украине – экспертное заключение
- Сертификация в Казахстане - Сертификат



Спасибо за внимание!

Электронная почта: aladdin@aladdin.ru

Web-сайт: www.aladdin.ru