Аладдин РД

Строгая аутентификация и квалифицированная электронная подпись для портальных решений и облачный сервисов.

Как получить квалифицированную электронную подпись при работе в недоверенной среде.

Сергей Груздев
Генеральный директор

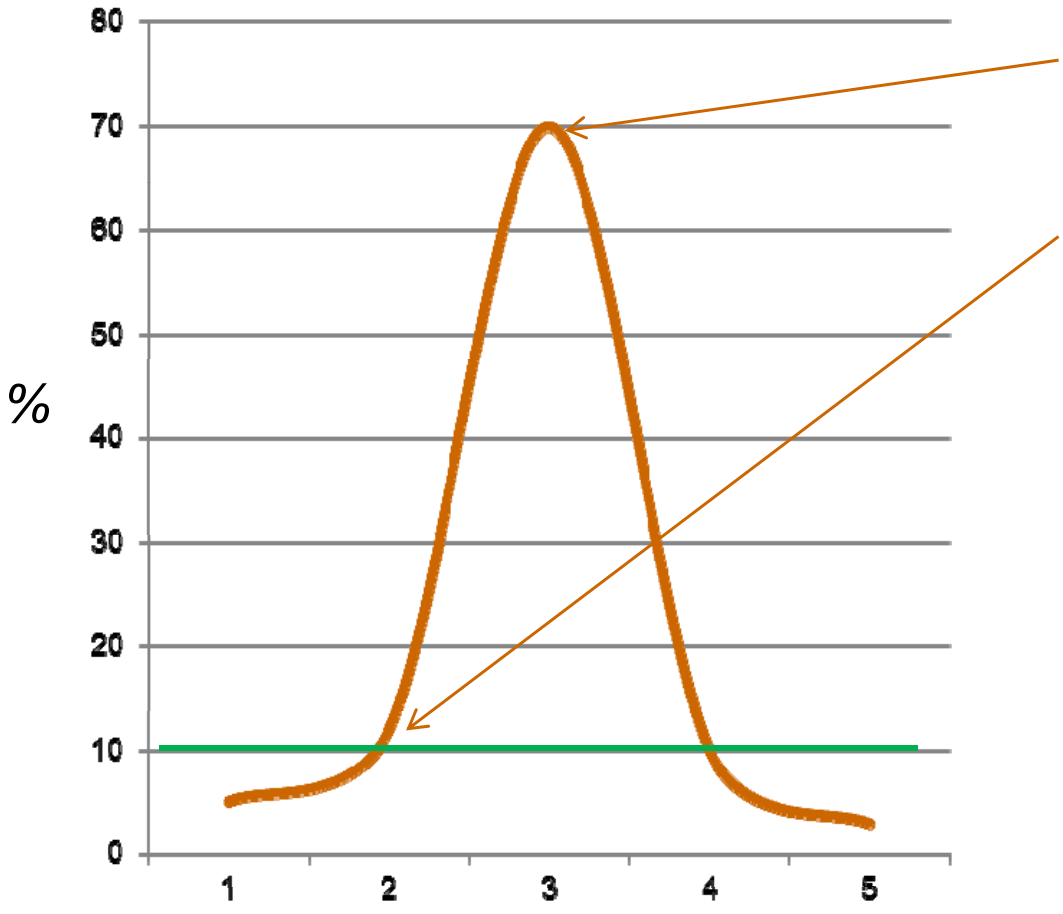
30.03.2012

Облачные сервисы – акселератор развития рынка

- По прогнозам IDC, к концу 2015 года объем российского рынка облачных услуг превысит отметку в $1,2 млрд.
  - Среднегодовой темп роста более 100%
- Примеры действующих Web (облачных) сервисов
  - Единый Портал Госуслуг
  - ДБО
  - Предоставление электронной отчетности и т.д.
- Многие сервисы требуют юридической значимости
  - Требуется **строгая** аутентификация и **квалифицированная** электронная подпись
  - Аутентификация и ЭЦП теперь всегда идут вместе!
    - Необходимым условием является применение e-signature device (смарт-карты или USB-токена с ЭЦП «на борту» и УЦ

Распределение по типам атак *

- Банки, ДБО – лакмусовая бумажка – что нас ждет
- Рынок ДБО - «средняя температура по больнице» выглядит так:



- **Кража закрытого ключа** с диска или незащищённого носителя **#3** – (>70%)
- **Удаленное управление компьютером** (с пробросом USB-порта) **#2** – (~10%)
- Кража СКЗИ, несанкционированное использование **#4** – (<10%)
- Кража ключей из памяти **#1** (<5%)
- **Подмена документа #5** (около 1%)

70% угроз снимается простым использованием токенов (s/c)

** - По данным GroupIB*

Работа с Web-порталами и облачными сервисами

Для облачных сервисов
на первое место ставится
удобство использования

Задача:

- Взаимная двухфакторная аутентификация (по ГОСТ)
- Квалифицированная ЭП Web-форм и документов (по ГОСТ)
- Защита данных в канале (по ГОСТ)
- Возможность **удобной** работы из **любой**, в т.ч. недоверенной среды
  - Windows 9x-7/CE, MacOS, Linux+
  - ПК, терминалка, любой Web-браузер
  - Защита от новейших атак с навязыванием и подменой подписываемого документа
  - Без предварительной установки ПО третьих фирм
  - Без прав администратора

Звучит фантастически?

Работа с Web-порталами и облачными сервисами

Решение:

- **USB-токен или смарт-карта** с реализацией сертифицированной российской криптографии «на борту»
  - Используется как персональное средство взаимной строгой двухфакторной аутентификации пользователя и портала, для формирования ЭЦП с неизвлекаемым закрытым ключом
  - Не требуется установка драйверов в современных ОС (Windows XP, MacOS, Linux), не требуются права локального администратора
  - Сертификат ФСБ (КС2), срок хранения закрытого ключа до 3х лет с возможность самостоятельной перегенерации ключей (*у конкурентов надо принести токен и переформатировать его на АРМе*)

Работа с Web-порталами и облачными сервисами

Решение:

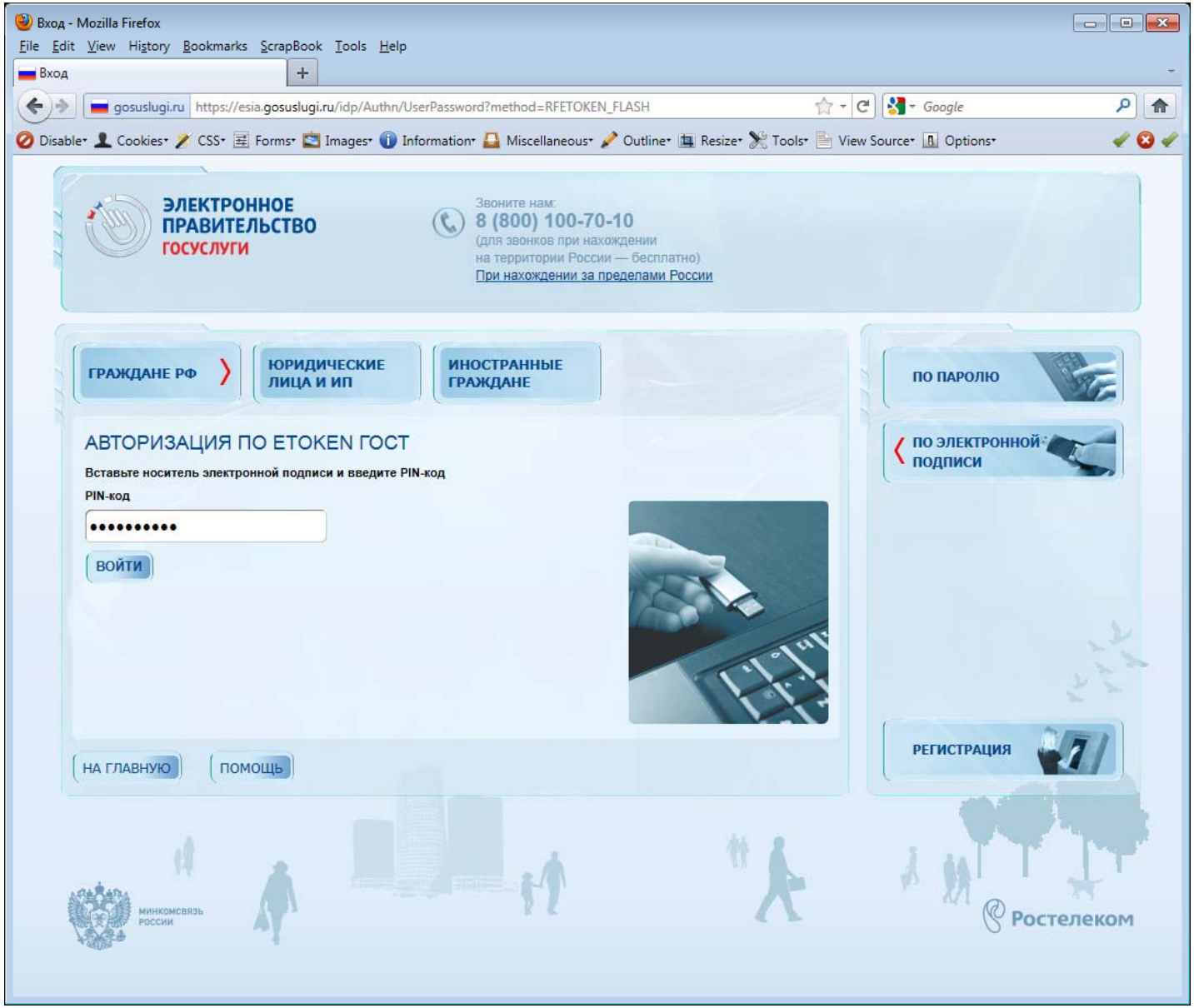
- **Кроссплатформенный мультибраузерный плагин**, обеспечивающий взаимодействие Web-приложения с токеном/картой в контексте браузера
  - **Устанавливается автоматически** при первом посещении Web-портала (как плагин в IE, Firefox, Chrome, Safari, Opera), *права локального администратора не нужны*
  - **Аутентификация** – с использованием ЭЦП (на прикладном уровне)
  - **Защита данных** – устанавливается SSL-соединение, поверх него – шифрование передаваемых данных по ГОСТ 28147-89 (на прикладном уровне)

  - **ЭЦП** Web-форм / файлов (аппаратно – токеном или картой)

Работа с Web-порталами и облачными сервисами

Пример:

www.gosuslugi.ru



Платежная карта с ЭЦП на борту

- В рамках проекта «Электронное правительство» отработана технология выпуска и применения платежных карт с сертифицированной ЭЦП «на борту»
  - Обеспечена 100% совместимость карт в платежной инфраструктуре, в PKI, с Web / облачными сервисами
  - В 2011 несколько крупных банков вместе с Ростелекомом запустили первые ко-брендинговые проекты
    - Зарплатные проекты
    - Доступ к порталу госуслуг
- ЭЦП на карте может использоваться в других системах
  - ДБО
  - е-отчетность, е-торги, е-декларирование, е-коммерция (счета-фактуры), облачные сервисы (1С, MS Office 365 и др.)

Платежная карта с ЭЦП на борту (пример)

ЭЦП с неизвлекаемым закрытым ключом, *3 года с возможностью самостоятельной перегенерации*

Можем использовать третий фактор – биометрию

Можем работать:

- MasterCard
- Visa
- *Про100**

Ридеры для смарт-карт

С биометрией

Аладдин наладил выпуск компактных и надежных ридеров по японской технологии.

Встроенный

Проблемы недоверенной среды

Как получить квалифицированную электронную подпись при работе в недоверенной среде?

Проблемы недоверенной среды

…идут от недоверенного «железа»

Проблемы недоверенной среды

- Доверия невозможно добиться без доверенного “железа”
  - Закрытый модуль BMC, зашитый в BIOS код Management Agent (5 Мб бинарного кода!), выкусить его нельзя – в нем Clock-генератор
  - Использование сертифицированных ОС и др. средств ИБ, проверок BIOS на недоверенном “железе”, с новыми функциями удаленного управления **не решает проблем**
  - BIOS-гипервизор, закладки по технологии аппаратной виртуализации «не ловятся»

Проект “Защищенный компьютер”

- **Что сделано** (попытка решения проблемы доверенного железа)
  - Собственный дизайн архитектуры и материнской платы (зачем нужна каждая компонента, какая прошивка) - Kraftway
    - Выбрана embedded-серия процессоров – доступна 5 лет
  - BIOS – в исходниках, удалены “проблемные” зоны, функции, относящиеся к безопасности, собраны с одном месте – TSM
  - Модуль безопасности (embedded Trusted Security Module)
    - Защищенный SPI-Flash (в режиме Пользователь исчезает из адресного пространства и не может быть атакован)
    - Получает управление сразу после включения питания и POST-инициализации BIOS, инициализацию контроллеров делаем сами
    - Умеет отслеживать появление/активность BIOS-гипервизоров (аппаратной виртуализации), “севших” до TSM
  - Собственное сертифицированное производство (завод в Обнинске)
  - Компьютеры под брендами Kraftway (РФ) и Fujitsu* (Япония)

Проект “Защищенный компьютер”

Терминалка с пассивным охлаждением, развязкой сетей

Проект “Защищенный компьютер”

- **Embedded TSM – доверенная загрузка и контроль среды**
  - Двухфакторная аутентификация пользователя ДО загрузки BIOS
  - Ролевое разделение прав (Админ / Пользователь)
  - Контроль целостности BIOS и его настроек (аппаратуры), ОС, важных приложений
    - Поддержка Windows 9x-7, CE, Linux (утилиты администрирования)
    - Поддержка файловых систем FAT16/32, NTFS, Ext2/3
  - Журналирование всех событий (в защищенную SPI-Flash)
  - Администрирование – из консоли Windows, Linux
  - Возможность дистанционного мониторинга внешними системами
  - Решены узкие места, присущие АПМДЗ
  - Сертификат ФСТЭК по 1Г (сделан по 1Б), НДВ 3 (!!!), ИСПДн 1
  - *Важное свойство – использование в неконтролируемых помещениях*
- Защищенная терминалка может использоваться для работы с облачными сервисами
  - С прошитым VPN (Инфотекс)

Работа с Web-порталами и облачными сервисами

- Защита от атак с подменой подписываемого документа на “зараженном” компьютере, с перехватом управления или с пробросом USB-порта на удаленный компьютер злоумышленника
  - Смарт-карт ридер с визуализацией подписываемого документа (значимые поля – по тегам)
  - Встроенная поддержка в плагин для браузеров

Что дальше? ЭЦП для мобильных платформ

Secure MicroSD для планшетов и телефонов

- Интегрирован чип смарт-карты с сертифицированной российской криптографией (ЭЦП с неизвлекаемым закрытым ключом)
- Функционал как у токенов и смарт-карт с ЭЦП на борту + Flash (2-8 Гб)
- Телефон может использоваться как средство визуализации подписываемого документа и как второй канал для подтверждения транзакций
  - В новой версии скорость аппаратного вычисления хэш и шифрование по ГОСТ 28147-89 – до 40 Кб/с

SIM-карта с ЭЦП на «борту»

- Технология аутентификации и ЭЦП документов через операторов мобильной связи

Аладдин РД

Спасибо за Ваше внимание!

Просто
Надежно
Удобно