Аладдин РД

Электронная подпись для мобильных устройств

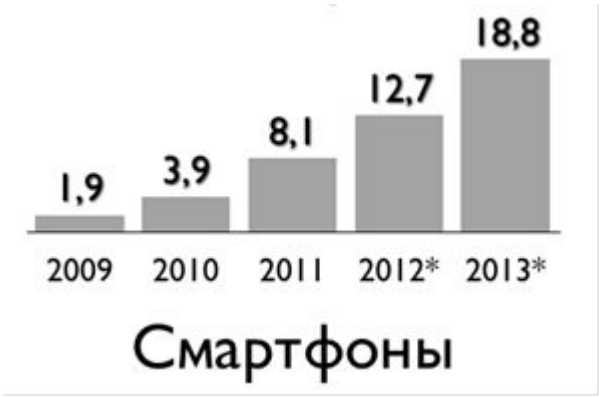
Коллеги из Apple и Samsung назвали наше решение прорывным и революционным

Сергей Груздев
Генеральный директор

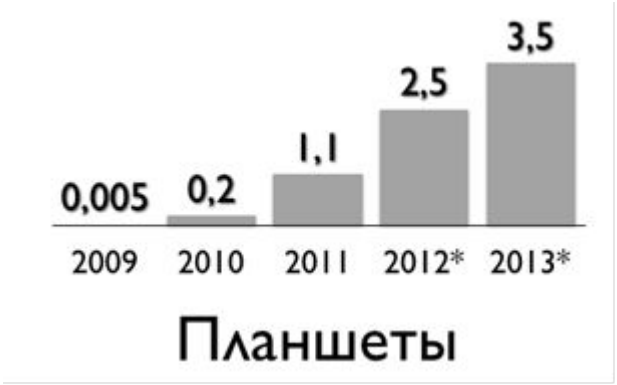
5informatika.net

Мобильные устройства – рынок и тренды

Объемы продаж м/у (млн. шт.)



Canalys (Декабрь 2012)



IDC (Октябрь 2012)

К 2016 г мобильных устройств будет в 3-4 раза больше, чем ПК
(CNews)

К концу 2015 г из 5 создаваемых программных продуктов только 1 будет для ПК
(CNews, Gartner)

75% респондентов (CIO) назвали мобильные решения в качестве одной из приоритетных статей своих ИТ-расходов
(IBM CIO Study)

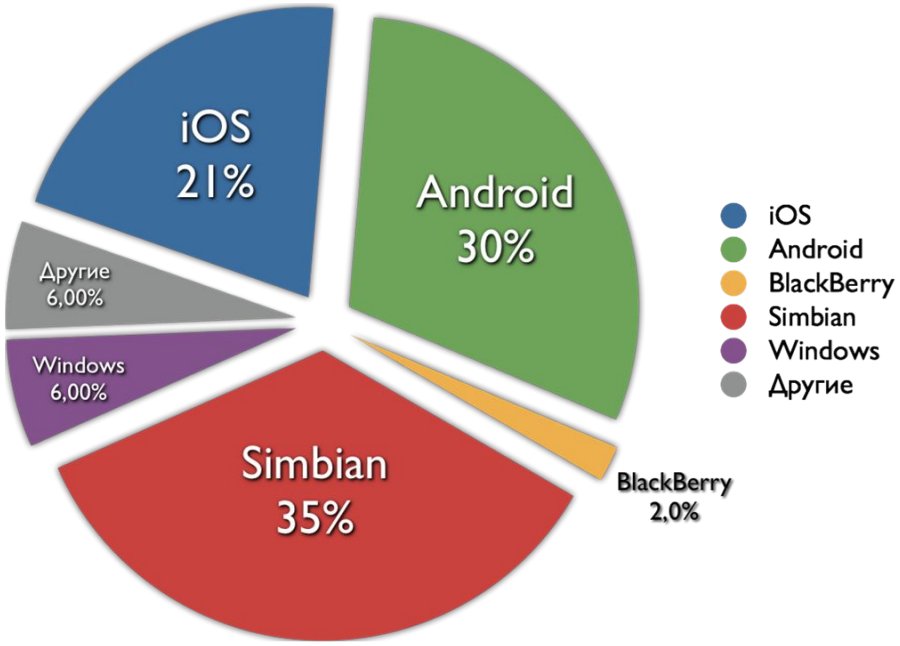
В России проникновение смартфонов в бизнес составляет около 18%, в США – 40%. До конца 2013 г. проникновение смартфонов в B2B-сегмент вырастет до 36%-40%
(Nielsen, CNews, «Билайн»)

За последние 4 года спрос на разработчиков мобильных приложений вырос в 14 раз!
(CNews, HeadHunter)

Мобильные устройства – рынок и тренды

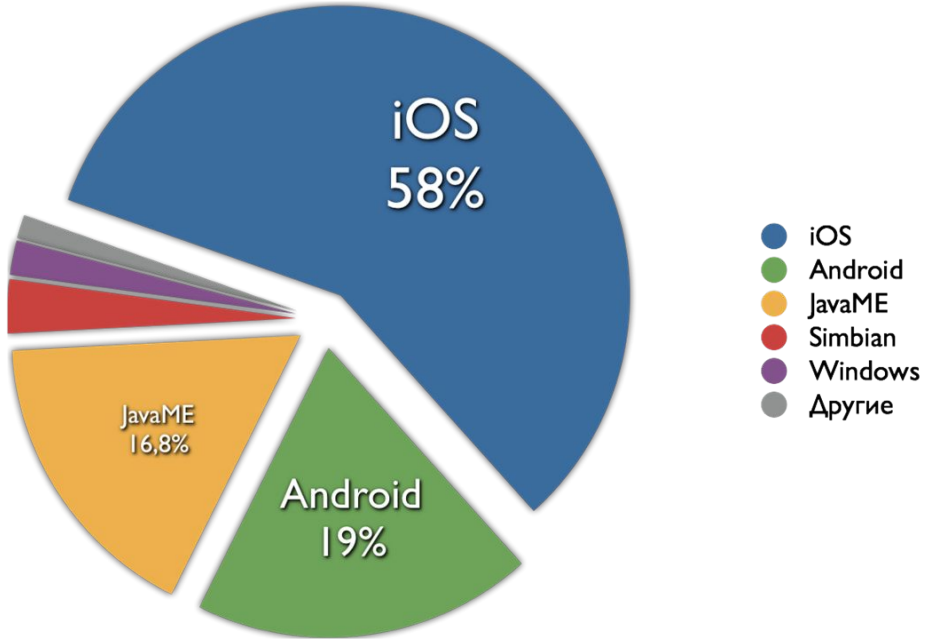
Распространенность мобильных платформ

В мире:



IDC, Сентябрь 2012

В России:



NET Applications, Октябрь 2012

Развитие корпоративной мобильности

BYOD (Bring Your Own Device) —

Принеси свое собственное устройство

Gartner:

К 2014 году 90% компаний будут поддерживать корпоративные приложения на устройствах, которые находятся в собственности работников

http://www.gartner.com/resId=2004115

Gartner:

«Внедрение пользовательских устройств (смартфонов и планшетов) в корпоративные ИТ-системы будет самым значительным трендом, влияющим на ИТ в ближайшие 10 лет».

Основные отрасли — финансы и страхование, так как в них работает наибольшее количество мобильных сотрудников»

Проблемы ЭП для Apple iOS

- Закрытая платформа (и меньшая уязвимость)
  - Жесткая политика Apple – не дает рос. разработчикам SDK нижнего уровня (уровня ОС, для работы с “железом”, коммуникациями – порт, SIM)
  - Нет USB, MicroSD, только “закрытый” разъем Apple Dock
  - Jailbreak? Только усугубит проблему безопасности
- Архитектурные ограничения iOS, политика Apple и законодательные ограничения
  - Монолитный код приложений, нет подгружаемых модулей
  - Приложение компилируется вместе с СКЗИ (и содержит СКЗИ…)
  - При распространении приложений через AppStore
    - Приложение не должно содержать криптографию (политика Apple)
    - Получаем распространение нашей криптографии с американского сайта (законодательные ограничения - экспорт криптографии)
  - Единственный путь – “In-House Distribution”
    - Приемлем не всегда и не для всех …

Apple iOS - вариант решения

- Использование смарт-карт с сертифицированной российской криптографией и специального карт-ридера

Смарт-карты для Apple iOS - что это дает?

- Соответствие требованиям законодательства
  - ЭП ставится пользователем под документом на его устройстве, с помощью его персонального средства формирования ЭП
- Сокращение сроков выпуска продуктов на рынок
  - Используется уже сертифицированное СКЗИ (средство ЭП)
  - Быстрое встраивание в приложения ЭДО, ДБО и пр. – предоставляем SDK с высокоуровневыми интерфейсами (PKCS#11, PKI-расширение), средства отладки, примеры
    - Поддержка хранения контейнеров КриптоПро CSP (кто пользуется)
- Упрощается режим эксплуатации
  - Ключи не в устройстве, а на внешнем защищенном носителе – в карте (неизвлекаемые, срок хранения закрытого ключа – 3 года)
- Удобство
  - Одна карта, один ридер – для всех используемых устройств, для всех платформ (ПК, iPad, iPhone)
- Преемственность
  - Карта для входа в домен с ПК, VPN, ЭП и пр.

Смарт-карты с ЭП «на борту»

PKI-карты для корпоративных пользователей

- Для надежной двухфакторной аутентификации
- Для хранения цифровых сертификатов, ключевых контейнеров при работе с PKI
- Для ЭДО в качестве средства формирования усиленной / квалифицированной ЭП (с неизвлекаемым закрытым ключом).
- Поддержка биометрии (Match-On-Card)

ID-карты (электронное удостоверение сотрудника)

- Карта-бейдж для визуальной идентификации владельца
- Электронный пропуск в помещения, на парковку, для льготного или бесплатного проезда на транспорте
- Персональное средство надежной двухфакторной аутентификации в корпоративной сети и безопасного доступа к ИС
- Для формирования усиленной квалифицированной

Смарт-карты с ЭП «на борту»

Платежная карта с российской криптографией

- Полнофункциональная чиповая международная платежная карта MasterCard или VISA с сертифицированной российской криптографией "на борту" (например, зарплатная)
- Карта - персональное средство формирования квалифицированной электронной подписи
  - Для Интернет-банкинга, систем электронной отчетности, счетов-фактур и других электронных и "облачных" сервисов, требующих обеспечения юридической значимости
  - Для портала гос. услуг (www.gosuslugi.ru)

Для социальных проектов

К платежной карте с ЭП добавляется RFID (бесконтактный чип) для льготного проезда в транспорте, доступа на соц. объекты и пр.

Смарт-карт ридер для iOS

Поставляем как часть решения под брендом Аладдин (OEM)

- Универсальный
  - **iOS**, Mac OS, Windows, Linux, Android* – через кабель-переходник
  - CCID-совместимый – не требует установки драйверов
- Быстрый – сразу готов к работе, выбирает максимально возможную скорость обмена
- Совместимый
  - EMV Level 1 (Pay&Sign)
  - Эмбоссированные карты
  - Проект «Электронное правительство», ДБО, ЭДО
  - УЦ
- Специальная прошивка

Подключение к устройствам Apple

В SDK входит модуль-переходник для отладки

Для нового разъема (iPad Mini) используется стандартный переходник

Подключение к устройствам на базе Android

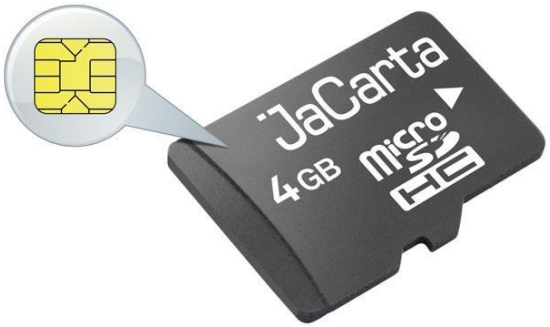
Ожидание SDK – Q2/2013

Подключение к устройствам на базе Android

Мобильные устройства с Android

- Открытая платформа (и потенциально бОльшая уязвимость)
  - Довольно большой “зоопарк”, возможны проблемы совместимости
  - Можно работать с уровнем ОС, с “железом”, с портами
  - Как правило есть USB (но не везде Host), MicroSD
- Средства ЭП – возможные варианты
  1. Карточка Secure MicroSD с интегрированным в нее чипом смарт-карты с российской криптографией “на борту”
  2. Смарт-карта с криптографией (+ тот же ридер – один для всех других ПК, планшета, смартфона)
- Нет единого решения
  - Проблемы “зоопарка”
  - Для карты (ридера) и токена нужен USB-host (есть далеко не везде!)
    - Рекомендуем – **JaCarta Secure MicroSD**

Secure MicroSD с ЭП “на борту”

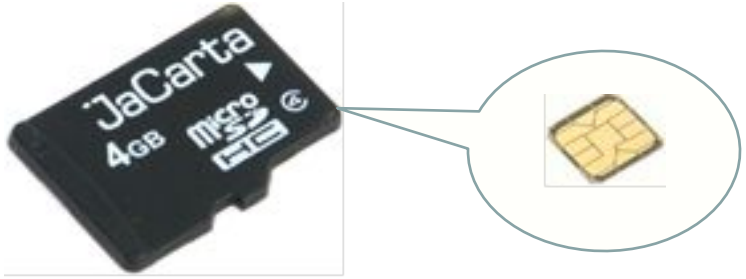


– Даст возможность работать с ЭП на телефоне / планшете на базе Android / Windows,

… и на любом компьютере!

Secure MicroSD с российской криптографией

Одна карточка JaCarta Secure MicroSD для всех устройств



SDK для Android – Q1/2013 – будет доступен для партнеров

Планшет
Телефон

SD-переходник
для ноутбука

USB-переходник
для ноутбука, ПК

Модем с разъемом для
MicroSD – “офис в кармане”

JaCarta Secure MicroSD

Secure MicroSD для мобильных платформ и M2M

- Интегрирован чип смарт-карты с ЭП с неизвлекаемым закрытым ключом
- Функционал как у токенов и смарт-карт с ЭП на борту + Flash (4-8 Гб)
- Телефон/планшет может использоваться как средство визуализации подписываемого документа и как второй канал для подтверждения транзакций
- Может использоваться модем
  - “Офис в кармане” – на Flash находится ОС, все необходимые приложения – мы не пользуемся ресурсами ПК
- Отчуждаемый модуль безопасности для M2M-устройств (доверенная среда, защита и ЭП для передаваемых данных)

Аладдин РД

Спасибо за внимание!

Инновации
Лидерство
Партнерство