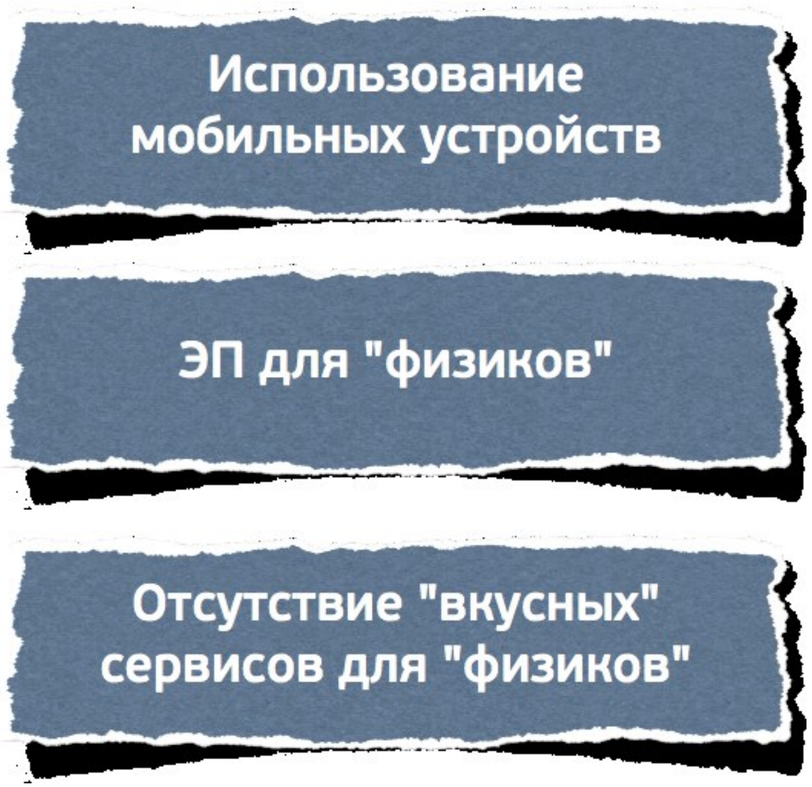
ЭП на SIM-карте

Как работает и почему это безопасно

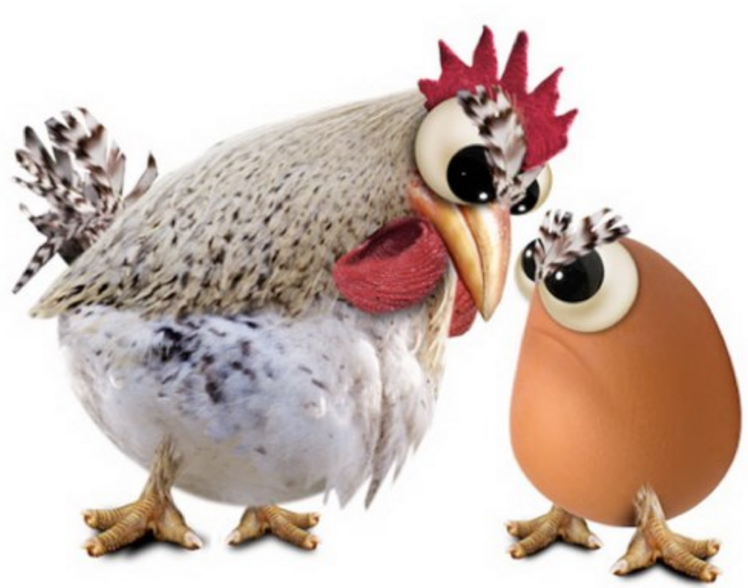
Сергей Груздев
Ген. директор
Аладдин Р.Д.

Проблемы с ЭП для массового рынка



- Программная ЭП
  - **Быстрая смена версий и поколений** - требуется пересертификация
  - **Небезопасно** - криптография работает в среде ОС и приложений, где м.б. трояны
  - **Нелегетимно** (iOS - публикация в AppStore, доставка "по воздуху")
- Аппаратная ЭП
  - **Конструктивно сложно** - разные разъёмы, разные технологии (iOS, Android)
  - **Не всегда удобно**, устройство ЭП всегда должно быть с собой

ЭП для физиков



Сегодня весь рынок ЭП ориентирован на "юриков"

Основная проблема рынка - курица или яйцо?

- Разработчики не пишут э-сервисы для "физиков" т.к. у "физиков" нет ЭП, а выдавать самим - дорого
- "Физики" не покупают ЭП, т.к. для них нет "вкусных" сервисов (стимулирующих приобрести ЭП)
  - > 95% всех работающих сервисов (где нужна юридическая значимость) - для юр. лиц (B2B, G2B)
  - < 5% - для физ. лиц
    - *Госуслуги? Не получилось... Не стимулирует*
    - ЭП в облаке?
    - *Красивая идея, но есть **проблемы с легитимностью** (позиция Минкомсвязи) и **с доверием** - "подписываю не я, а кто-то за меня"*
    - ***Проблемы с безопасностью** - слабое звено: аутентификация (для УКЭП нужна строгая аутентификация, OTP способна дать лишь усиленную)*

ЭП на SIM-карте

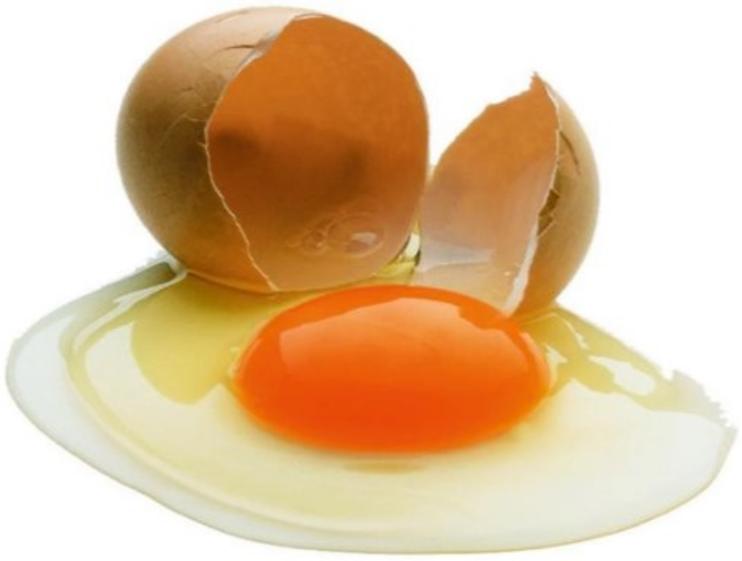
- Начали заниматься этим 3.5 года назад
- Летом 2013 г. - работающее технологическое решение
- Осень 2013 г. - представление проекта на Президентском совете по модернизации экономики и инновационному развитию России
  - Цели:
    - *Запустить проект одновременно у 3-4х операторов*
    - *Не упустить возможность создать **единые стандарты и правила***
    - *Получить поддержку Правительства в рамках нац. проекта*
  - Получили отчаянные попытки провалить проект, слишком много политики...
- Зима 2013 г. - МегаФон приобрёл Платформу "ЭП на SIM" и готовится к широкомасштабному запуску в этом году:
  - Построение **правильной** инфраструктуры выдачи SIM-карт с ЭП
    - *Планируется выдача SIM-карт и через банки (для ДБО, доп. услуг - страхование и пр.)*
  - Схемы монетизации услуг и сервисов (с делением доходов с разработчиками и провайдерами сервисов)
  - Создание и подключение сервисов (ЭДО, ДБО, страхование и пр.)

SIM-карта с ЭП

Совместный проект с компаниями Gemalto, Центр идентификации (Signum) и Мегафон

- Работает на всех моделях планшетов и телефонов (старше 1995 г.)
- Позволяет идентифицировать пользователя, безопасно и полноценно работать с ЭП (по ГОСТ)
  - Генерация ключей
  - Операции с ЭП с неизвлекаемым ключом ЭП
  - Хэш, шифрование, согласование ключей
  - Визуализация данных и безопасный ввод PIN-кода для формирования ЭП
- Все операции выполняются на SIM-карте, все приложения (включая троянские), ОС, процессор доступа к обрабатываемым данным не имеют
- Данные на обработку и подпись передаются на SIM-карту по второму независимому каналу ("по воздуху") с сервера (ДБО)

ЭП на SIM-карте



Не все получается
с первого раза...

Почему до сих пор никто не сделал?

- Это крайне нетривиально (SIM + инфраструктура)
  - Сопроцессор на чипе "не умеет" работать с российскими параметрами эллиптических кривых - требуются доработки
  - Апплеты не могут напрямую работать с криптопроцессором
- Мы потратили 1.5 года на исследования, как из приложения "достучаться" до криптографии на SIM-карте
  - Если нельзя, но очень хочется, то можно?..
    - Не смогли... Значит, не смогут и злоумышленники!
- Архитектура не позволяет напрямую из приложений работать с ЭП на SIM
  - Но можно воспользоваться вторым каналом передачи и "по воздуху" загрузить в SIM-карту данные для подписи
    - Для этого надо ещё построить инфраструктуру (главное!)

Как работает ЭП на SIM-карте

- Для подготовки документов и их публикации может использоваться любой компьютер, планшет, мобильный телефон
- Предполагается, что **мы не доверяем** ни компьютеру, ни каналу, и особо не заботимся об их защите
  - Защитить их у массового пользователя дорого и практически невозможно
- На подпись отправляется документ, загруженный пользователем на сервер в систему ДБО, ЭДО и пр. по сети, по каналу WiFi, GPRS, 3G...
- Для передачи на SIM-карту с ЭП используется **второй независимый канал** (цепочка SMS)

Как работает ЭП на SIM-карте

- Передается либо весь документ, либо его значимая часть + хэш документа (посчитанный на сервере в доверенной среде)
  - Содержимое SMS зашифровано на ключе пользователя
    - Защита передаваемых данных: банковская тайна
    - Защита от атак с подменой базовой станции
- SIM-карта
  - Принимает цепочку SMS
  - Отображает данные на экране (без участия ОС)
  - Запрашивает PIN на ЭП
  - Считает хэш от визуализированных данных
  - Подписывает хеш от документа
  - Отправляет зашифрованные данные через Оператора обратно на сервер (ДБО, ЭДО…)
- Сервер проверяет хэш от визуализированных данных, ЭП

Как работает ЭП на SIM

Платформа

Подпись документа

Эл. сервис

Загрузка документов, заполнение Web-форм

Информация о

SMS

(сообщение зашифровано на ключе абонента)

Оператор связи

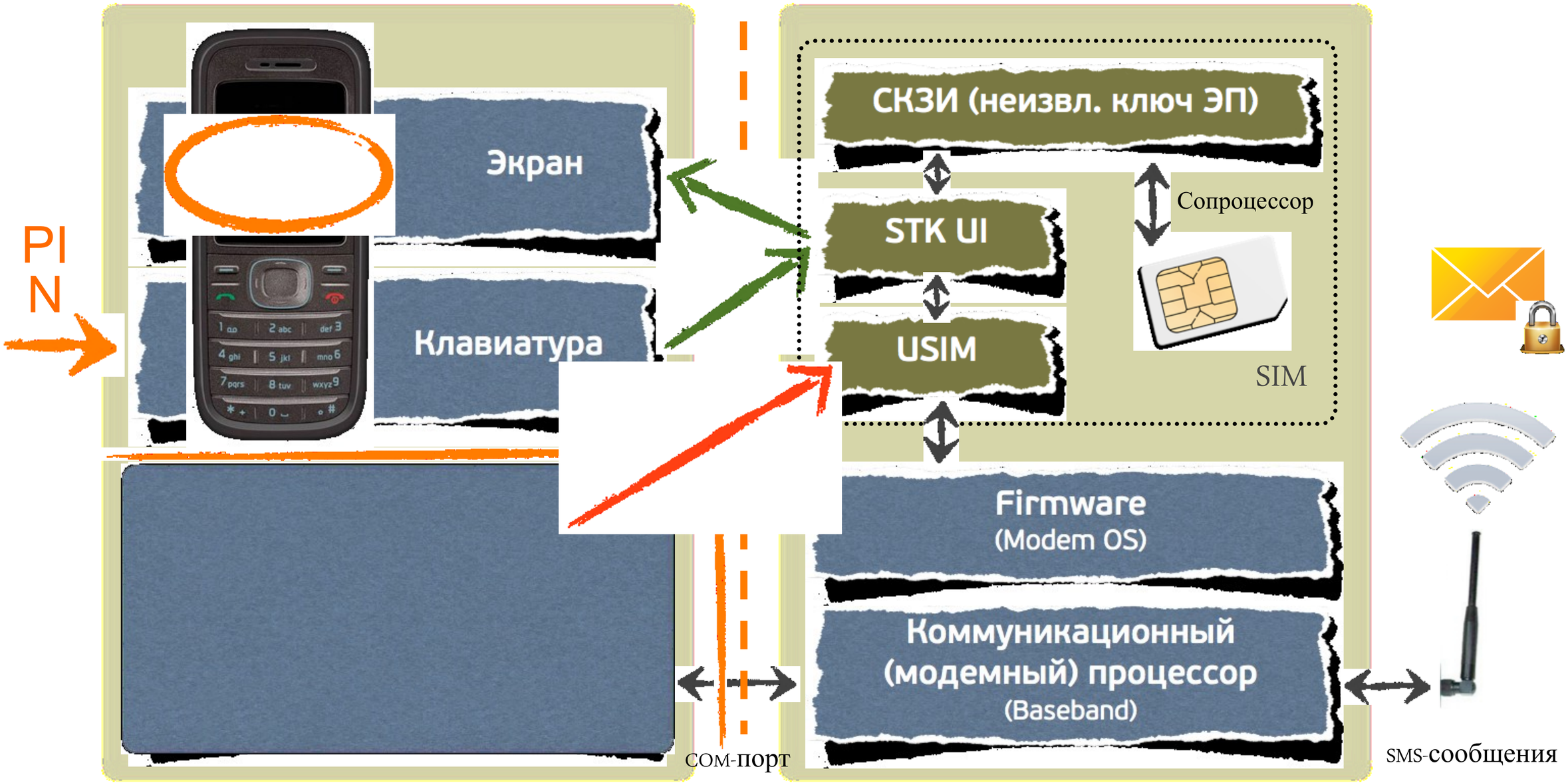
ЭП на SIM-карте

Архитектура SIM

- Чем SIM-карта отличается от смарт-карты?
  - Это та же современная платформа Java Card Global Platform
- За функциональность карты отвечают Java-апплеты
  - Чтобы работать с ЭП на телефоне нам пришлось сделать ещё ТРИ апплета:
    - *Коммуникационный, GUI, криптографический*
  - Все они умеют безопасно общаться друг с другом, "не выходя наружу"
  - ЭП для SIM-карты реализуется таким же криптографическим апплетом, что и в s/c JaCarta ГОСТ
  - Этот апплет умеет работать с сопроцессором SIM-карты
    - *Без сопроцессора ЭП будет формироваться ~ неделю*

Каждый апплет в своем лотке ("песочнице")

Почему это безопасно



Что даст новая технология рынку

- Решение проблемы надёжной **идентификации и строгой двухфакторной аутентификации** пользователей при подключении к э-сервисам
  - Аутентификация пользователя, а не его SIM-карты (как в сети GSM)
  - **Строгая** аутентификация как сервис (услуга для банков, социальных сетей и пр.)
- Усиленная квалифицированная* **персональная** ЭП в любом мобильнике
  - Выполняются все требования 63-ФЗ и 796-го приказа ФСБ (включая визуализацию подписываемых данных)
  - **Безопасность** - неизвлекаемые ключи ЭП, формирование ЭП в SIM-карте, а не в области приложений, получение загруженных в систему данных по второму независимому каналу
  - **Усиленная квалифицированная ЭП как сервис** (услуга для множества сервисов)

Что даст новая технология рынку

- Стимулирует разработчиков э-сервисов
  - Появляется большая база пользователей (миллионы), уже имеющих средство ЭП
  - Новый заработок
    - За подключение нового пользователя к э-услуге
    - С транзакций за ЭП
    - За подписку
    - % от стоимости подписываемой услуги
- Откроет новые рынки
  - Массовый рынок "физиков"
  - Мобильный PKI
  - M2M

ЭП на SIM

Как новая технология способна изменить наш мир?

Так же как и в своё время eToken!

Спасибо

Будь собой в электронном мире!

Контакты:

Сергей Груздев

+7 (495) 762-2855

s.gruzdev@aladdin-rd.ru

www.aladdin-rd.ru

Будь собой в электронном мире!

Лицензии ФСТЭК России №0037, №0054, №2874
Лицензии ФСБ России №12632Н, №18229
Сертификат соответствия системы управления качеством СМК ГОСТ Р ИСО 9001-2008
№ РОСС RU.ИС72.К00069

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru

*Приведённая информация актуальна по состоянию на **1 февраля** 2014 г.*

Используемые сокращения

ДБО Дистанционное банковское обслуживание

ИБ Информационная безопасность

СКЗИ Система криптографической защиты

ОС Операционная система

ЭДО Система электронного документооборота

Троян Вредоносная программа, маскирующаяся под видом обычного приложения

ЭП Электронная подпись

УЭП Усиленная электронная подпись

УКЭП Усиленная квалифицированная подпись

Хэш Значение хэш-функции, свёртки от документа, необходима для вычисления ЭП документа

B2C Бизнес для Потребителя (Business-to-customer)

B2B Бизнес для бизнеса (Business-to-Business)

GUI Пользовательский интерфейс (Graphical user interface)

PKCS Public Key Cryptography Standards (стандарты криптографии с открытым ключом)

PKI Public Key Infrastructure (инфраструктура открытых ключей)