Мобильная PKI: наше будущее?

Как технологии меняют нашу жизнь

Сергей Груздев

Ген. директор
Аладдин Р.Д.

Вектор развития рынка - мобильность

- Мобильный телефон есть у каждого (у многих - 2-3)
- Он всегда при нас
- Мы привыкли использовать его для кучи разных задач
  - Звонки, почта, навигация, поиск информации, музыкальный/ видео плейер…
    - Так почему бы не использовать телефон для задач PKI?
      - *Надежная идентификация, аутентификация и УКЭП*

В основе PKI лежит несколько принципов, основной из которых гласит:

Закрытый ключ ЭП известен только его владельцу

Как решать проблему?

Криптография в телефоне

Проблемы реализации криптографии в мобильном телефоне

- Программная реализация
  - Недоверенная среда, разные ОС, частое обновление и смена платформ
  - Легитимность
    - *В iOS - проблема распространения приложений с крипто-библиотеками*
    - *Нарушение законов при публикации приложений в AppStore, распространение СКЗИ с американских сайтов*
  - Возможны атаки с подменой подписываемого документа и кражи закрытого ключа ЭП

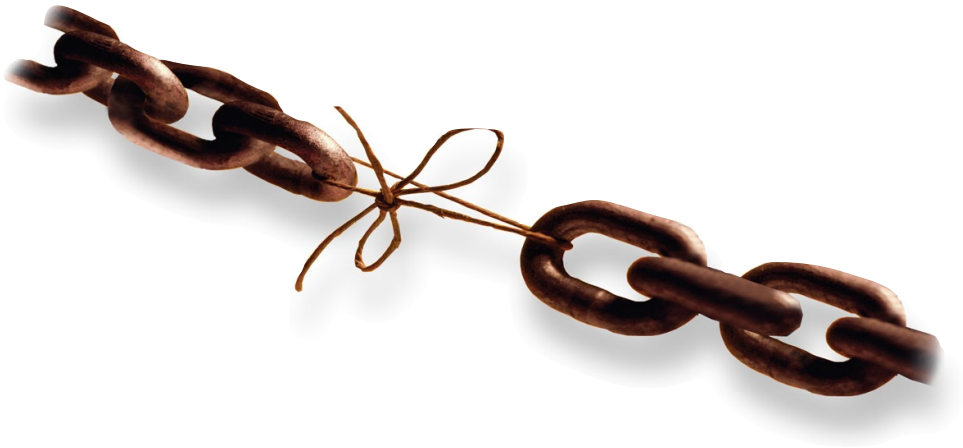
- Подключаемые аппаратные средства
  - Не унифицированы разъёмы и интерфейсы (USB 3.1, NFC, BT - ?)
  - Необходимо всегда носить их с собой и подключать при работе, либо всегда держать его в устройстве (MicroSD - есть не везде)
  - PKI-приложение работает в недоверенной среде - возможны атаки с подменой подписываемого документа (закрытый ключ - неизвлекаемый, на смарт-карте)

Криптография в телефоне

Проблемы реализации криптографии в мобильном телефоне

- На SIM-карте
  - Для реализации ЭП требуется со-процессор (без него ЭП вычисляется 1.5 недели)
  - Со-процессоры на SIM не поддерживают российские параметры ECC
  - Из области приложений напрямую обратиться к SIM-карте нельзя (архитектурное ограничение) - только "по воздуху"
  - Необходимо будет получать новую SIM'ку с поддержкой ЭП
    - Зато
      - *Для использования ЭП на SIM не надо писать приложения для каждой платформы (iOS, Android, Windows, BlackBarry,..)*
      - *Троян (из области приложений) не сможет атаковать процесс визуализации и подписания документа*

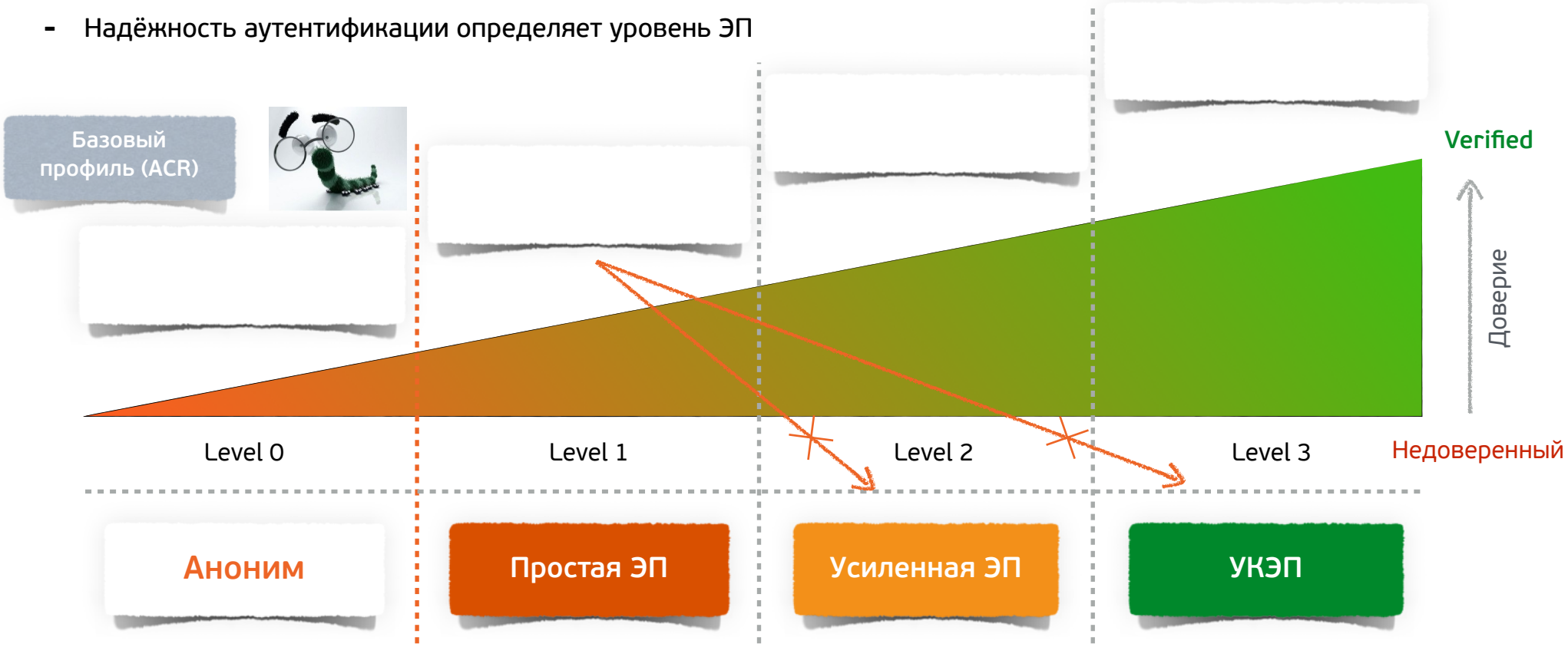
Доверие к идентификации и ЭП



Мобильная идентификация

Mobile ID - уровни доверия к аутентификации и ЭП

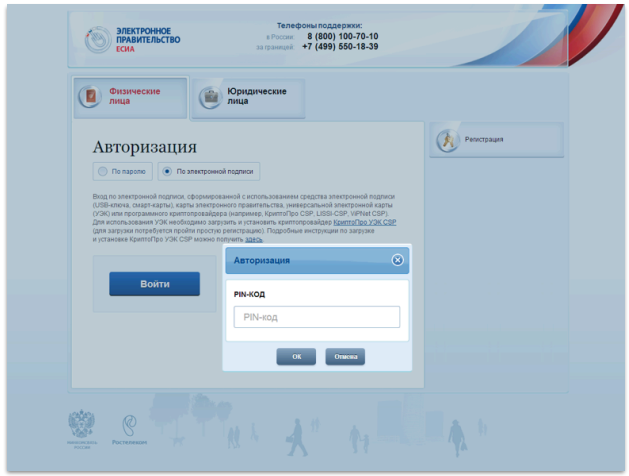
- Аутентификация и ЭП должны рассматриваться вместе
- Надёжность аутентификации определяет уровень ЭП



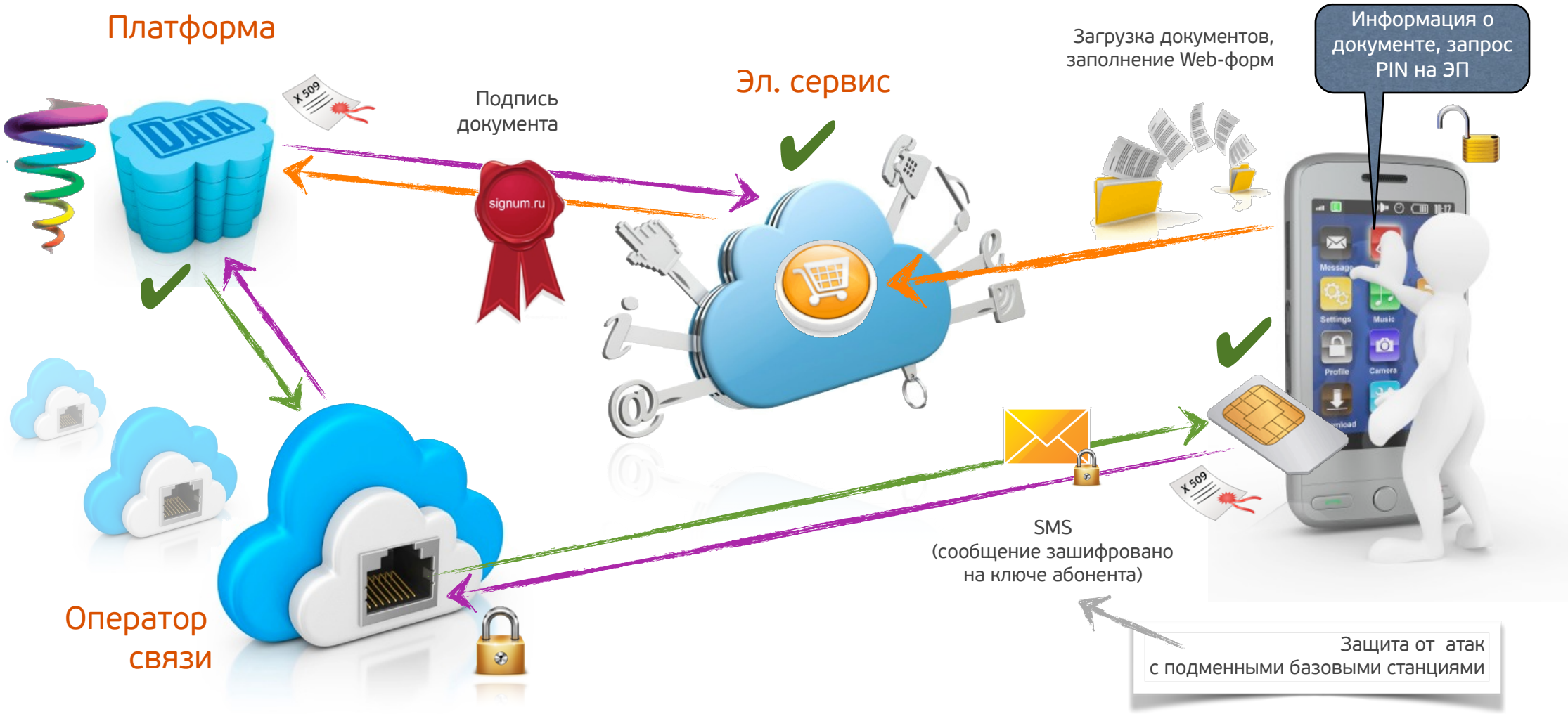
ЭП на SIM

On-line

Off-line



ЭП на SIM через SMS



Контроль и подпись

Платёжное поручение

Сверьте выделенные ниже поля платёжного поручения со значениями, выведенными на экран Антифрод-терминала. В случае совпадения всех полей подтвердите операцию на клавиатуре терминала **OK**. Иначе - отклоните **C**.

У вас осталось 30 сек. для подтверждения операции.

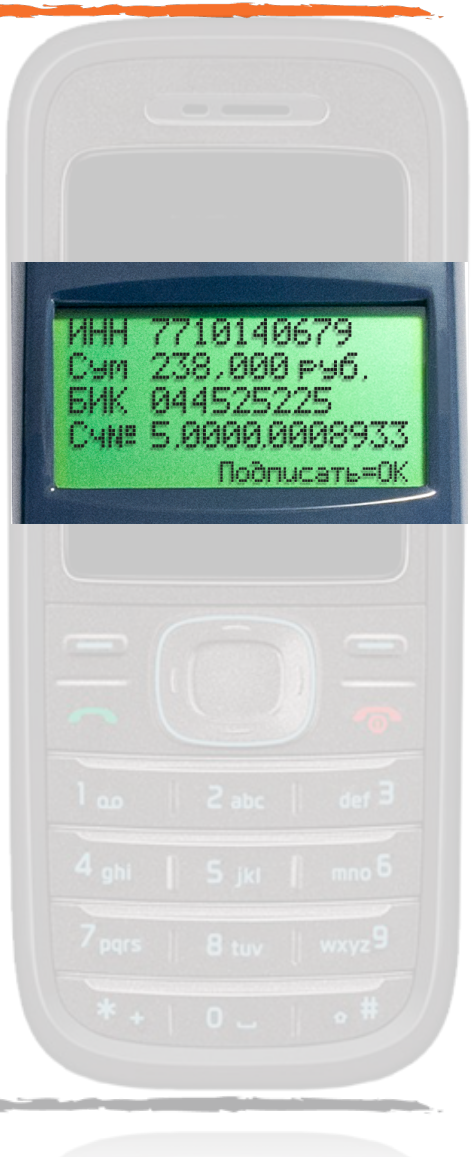
ПЛАТЁЖНОЕ ПОРУЧЕНИЕ №2077 — 22.01.2014 (Дата) — Электронный (Вид платежа)

ИНН 7719165935	КПП 771601001	Сумма	238,000.00			
ЗАО "Аладдин Р.Д." Плательщик		Сч. №	407.02.810.4.0002.1087822			
ОАО "Уралсиб" Банк плательщика		БИК	044525787			
		Сч. №	301.01.810.1.0000.0000787			
ОАО БАНК "ВОЗРОЖДЕНИЕ" Банк получателя		БИК	044525225			
		Сч. №	301.01.810.5.0000.0008933			
ИНН 7710140679	КПП 775000856	Сч. №	407.02.810.5.0000.0008933			
ООО "Мажторг" Получатель		Вид оп.	01	Срок плат.		
		Наз оп.		Очер. плат.	3	
		Код		Рез. поле		
За оборудование Назначение платежа						

Проверка данных на экране телефона и подпись

Значимые (выделенные) поля документа

Документ на Web-портале с выделенными полями для контроля



PKI на SIM через NFC

SECURE
PC LOG-ON

- Аутентификация в ПК, в сети, на Web-порталах, в публичных сетях WiFi
- ЭП для документов
  - *Ввод PIN-кода - в телефоне (безопасно), а не в ПК*

Эл. сделки
могут совершаться так:

Mobile PKI в мире

- Финляндия
- Турция
- Швеция
- Норвегия
- Швейцария
- Испания
- Латвия
- Литва
- Нидерланды
- Дания
- Словакия
- Словения
- Египет
- Оман
- Индия
- Корея
- Малайзия
- ...

Mobile PKI в мире

- **Финляндия**
- **Турция**
- Швеция
- Норвегия
- Швейцария
- Испания
- Латвия
- Литва
- Нидерланды
- Дания
- Словакия
- Словения
- Египет
- Оман
- Индия
- Корея
- Малайзия
- ...

Mobile PKI в России

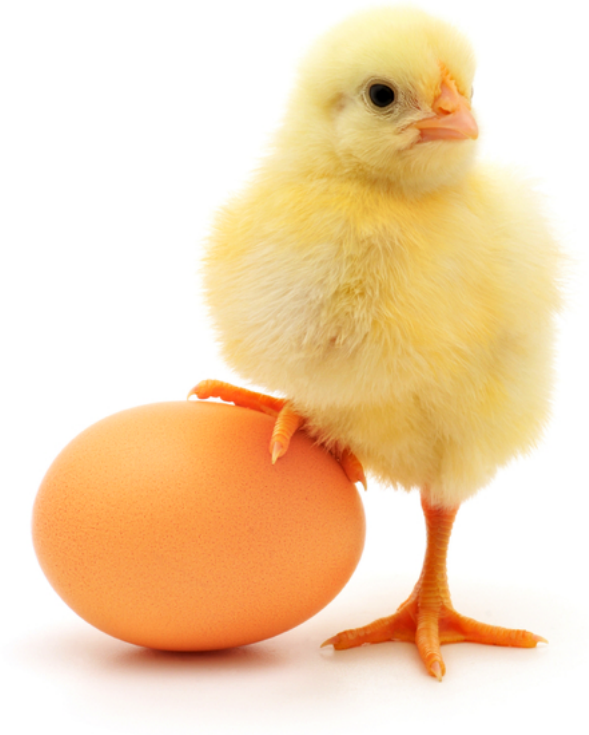
- Август 2013 - доклад о готовности технологии на Совете по инновациям
  - Поручение Правительства
- Готовность операторов
  - "Большая тройка" договорилась использовать одну технологию, единые стандарты и правила
  - РТК / Tele2 - пошли своим путем?
  - Стартовали пилоты
- Сертификация
  - Подписано ТЗ на "Персональное средство ЭП на SIM-карте", идет работа
    - *Криптоаппплет - такой же как в смарт-картах и USB-токенах JaCarta и eToken*
- Виды SIM-карт
  - С SMS-каналом
  - С SMS и NFC-каналами
- Партнёр по проекту - Gemalto

Что даст новая технология рынку

- Возможность использовать мобильный телефон в качестве токена
  - с аппаратно реализованной персональной ЭП
  - с визуализацией подписываемых документов
  - с безопасным вводом PIN-кода
    - В On-line (SMS)
    - В Off-lime (NFC)
- При удалённой работе
  - Web-портал организации, банка, гос. услуг, ДБО, СЭД и др. эл. сервисы - **необходимо**:
    - Надёжно идентифицировать пользователя
    - Убедиться, что он - именно тот, за кого себя выдает (со 100% вероятностью)
    - Обеспечить юридическую значимость документов, оформляемых дистанционно
- Для ускорения обслуживания в точках ритейла, снижения затрат, и удобства
  - Средняя стоимость одного очного контакта (5 мин. обслуживания)
    - По Москве ~850 руб., по стране ~730 руб.
  - Для перехода на безбумажный документооборот
    - Крупный банк, крупный клиент в месяц тратят 6-8 "Газелей" бумаги

Без бумаги к 2020 году

Что даст новая технология рынку



- Решение проблемы "курица или яйцо"
  - Доступность средств ЭП будет стимулировать разработку электронных сервисов
- Появление множества э-сервисов и для граждан ("физиков"), и для юр. лиц (организаций)
  - Появляется большая база пользователей (миллионы), уже имеющих средство ЭП
  - Новый заработок для разработчиков э-сервисов
    - За подключение нового пользователя к э-услуге
    - С транзакций (аутентификация, ЭП как услуга)
    - За подписку (месяц, год)
    - % от стоимости подписываемой услуги
- Откроет новые рынки
  - Массовый рынок "физиков"
  - Мобильный PKI (для юр. лиц)

Мобильная PKI

Будь собой в электронном мире!

Контакты:

Сергей Груздев

www.aladdin-rd.ru
+7 (985) 762-2855
s.gruzdev@aladdin-rd.ru