Жизнь в эпоху перемен…

Сергей Груздев

Ген. директор
Аладдин Р.Д.

Магнитогорск, февраль 2015 г.

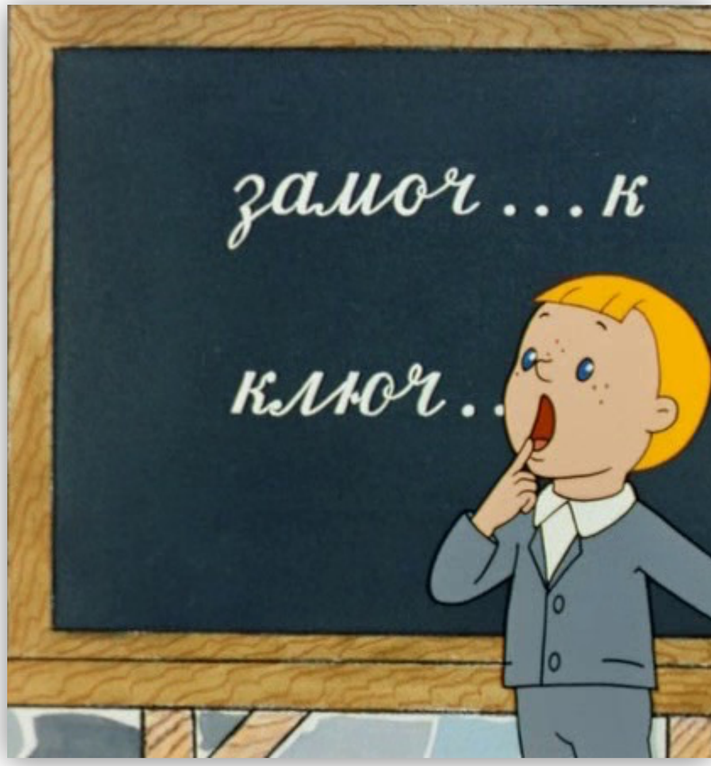
Влияние кризиса

- Главная проблема во время любого кризиса - урезание бюджетов и "кризис в головах"
  - Во время экономических проблем и кризисов на рынке всегда обостряются проблемы с ИБ
    - И внешние (хакеры, конкуренты), и внутренние (с персоналом)
  - Что мы видим
    - Рост количества инцидентов и качества атак (аргумент "а нас не ломают" скоро работать перестанет)
    - Первым делом режут "неоправданно высокие" (неочевидные) затраты на ИБ
    - ▸ Возникает опасная положительная обратная связь
  - К чему это приведёт
    - К накоплению нерешённых проблем с ИБ ("снежный ком")
    - После громких инцидентов - будут готовы на всё, лишь бы закрыть проблему (так было после предыдущих кризисов)
    - Уход профессионалов, снижение уровня компетенции, принятие некомпетентных решений
    - ▸ Выиграют те, кто не стал экономить на ИБ

В стране невыученных уроков

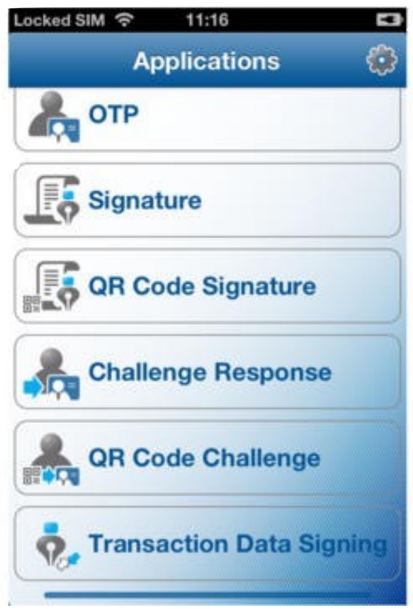
Типовые ошибки архитекторов и разработчиков

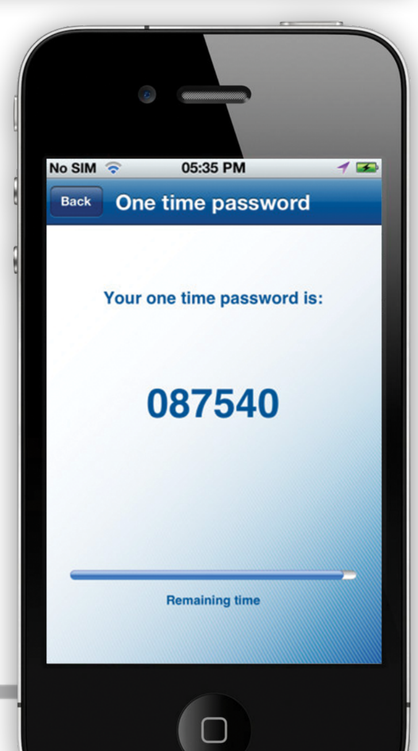
- В эл. сервисах аутентификация и ЭП всегда должны рассматриваться вместе
- Надёжность системы определяется по её самому слабому звену
  - Надёжность идентификации и аутентификации пользователя напрямую определяет **тип ЭП**, которую можем получить
  - Типы аутентификации (по аналогии с типами ЭП)
    - Простая
    - Усиленная
    - Строгая (с использованием криптографии)
      - Усиленная не значит двухфакторная (как в новом профиле)



Не всё то золото, что блестит

- Понятно стремление разработчиков предложить простое и красивое программное решение с использованием мобильного телефона
- Но изобрести вечный двигатель ещё никому не удалось
- Большинство предлагаемых решений имеет серьёзные проблемы с безопасностью
  - Приложение (генератор OTP, чтение данных из QR-кода и отображение их на экране, SMS) работает в недоверенной области ОС смартфона
  - Разработчики часто полагаются на аутентификацию телефона (SIM-карты) в сети сотового оператора
    - Это аутентификация телефона в сети, а не абонента
      - С точки зрения надёжности аутентификации - это **Аноним**
      - Надеяться получить УКЭП для анонима - нонсенс





Не всё то золото, что блестит

- OTP-генератор в телефоне
  - Троян может легко перехватить значение OTP с экрана и переслать его злоумышленнику
  - Современный смартфон - это такой же компьютер, который иногда ещё и живёт своей жизнью

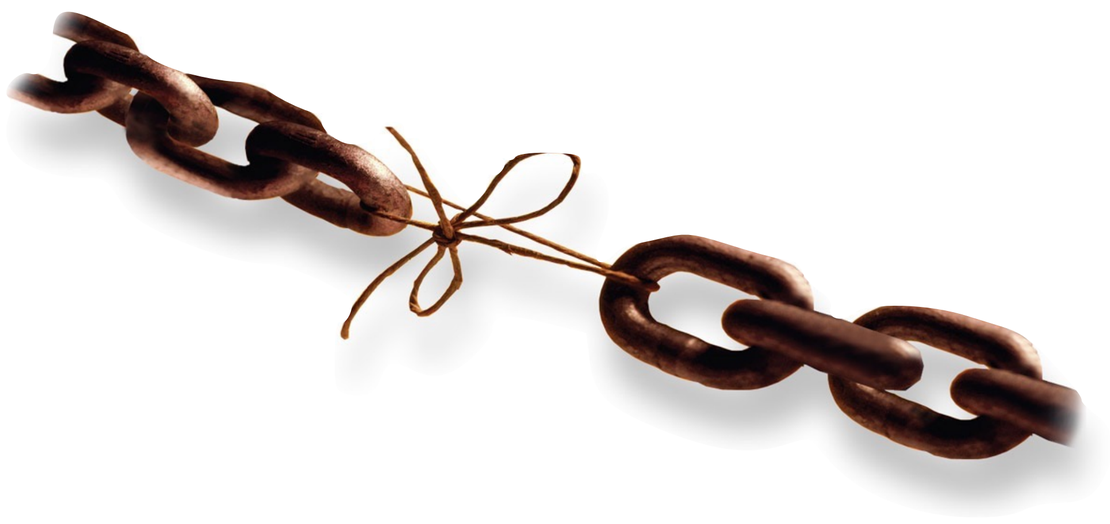
Не всё то золото, что блестит

- OTP-генератор в телефоне
- Мобильный программный (виртуальный) токен
  - Приложение для смартфона имитирует работу пластиковой смарт-карты
  - Двухфакторная аутентификация, электронная подпись, шифрование документов
    - В приложении криптография реализована программно
    - Для iOS приложение и криптобиблиотеки линкуются в единый код, и приложение становится СКЗИ
    - Закрытый (извлекаемый) ключ ЭП или секретный ключ OTP хранится в самом приложении (*Как гарантировать, что мой ключ ни к кому не попал? сколько BackUp'ов и где они?*)
    - Распространять через Apple Store нельзя - только inHouse
    - Загрузка приложения (СКЗИ) по воздуху…

Не всё то золото, что блестит

- OTP-генератор в телефоне
- Мобильный программный (виртуальный) токен
- Считыватель QR-кода (штрих-, динамического и пр.) с платёжной информацией с экрана
- SMS с одноразовым паролем
  - Приложение (генератор OTP, чтение данных из QR-кода и отображение их на экране, SMS) работает в недоверенной области ОС смартфона
  - Всё, что выводится на экран, может быть и будет украдено

Доверие к идентификации, аутентификации абонента и ЭП при использовании мобильных устройств



ЭП с помощью мобильного устройства

Риск
на основе известных атак и уязвимостей

	Большой	Средний	Малый
Высокая			
Средняя	SMS с кодом подтверждения (Login-Password)	SMS с OTP + PIN Приложения в области ОС смартфона (QR-код, генератор OTP и пр.)	ЭП/OTP на SIM-карте (без передачи данных в ОС)
Низкая			

Надёжность аутентификации

Тип аутентификации:	Простая	Усиленная	Строгая
Тип ЭП:	Простая	Усиленная	Квалифицированная

Накипело!

Или если мы хотим что-то сделать в этой стране...

К диалогу с регуляторами

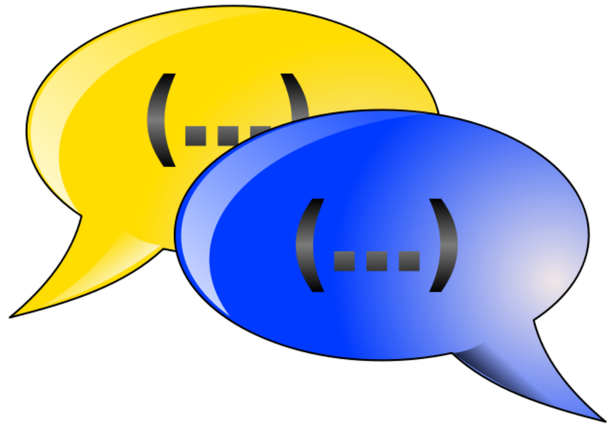
Давно назрело

- Разрешить распространять персональные средства ЭП без оформления лицензии ФСБ России на распространение СКЗИ (хотя бы банкам)
  - Добавить в исключения Постановление Правительства № 313
- Вопрос со сроками согласования ТЗ (~9 мес.) и сертификации СКЗИ (1.5-2 года)
  - Срок жизни современного процессора для мобильных платформ - 3-3.5 года, дальше выпускается новый
- Ориентироваться на Европейские требования к ЭП
  - Изменения к 63-ФЗ - "буря в стакане" - не сделано главное, не обеспечено доверие к средству формирования ЭП:
    - УКЭП должна формироваться только с использованием безопасного аппаратного устройства (Qualified Signature Creation Device)
    - Должна быть подтверждена **безопасность** и **неклонируемость** такого устройства (Secure by design)
  - За основу стоит взять сертификацию для платёжных систем (EMVCo) - тестируют изделие в комплексе на предмет устойчивости его ко всем известным на сегодня видам атак
    - Иначе, будет как у А. Райкина: "К пуговицам есть претензии?"

К диалогу с регуляторами

Аутентификация

- Надо классифицировать не как однофакторную и двухфакторную, а по аналогии с ЭП (Простая, Усиленная и Строгая)
- Сделать надёжную аутентификацию без криптографии нельзя
- Если упоминаем (используем) криптографию, то попадаем на лицензионные требования к СКЗИ со всеми вытекающими…
- Реализация текущих "бумажных" требований, к сожалению, не сильно повышает реальную безопасность
  - **Надо серьёзно заниматься нормативной базой в части аутентификации**



Конкуренция - кризис всё спишет?

- Рынок ИБ небольшой, достаточно цивилизованный, лет 10 удавалось оставаться в этических рамках
- Последние год-два - опасные "звоночки"
  - Наши друзья-конкуренты стали делать в своём ПО **закладки** (преднамеренные ошибки) против других токенов
    - Если на ПК был установлен такой токен, он вместо двух-трёх захватывает (и не освобождает при удалении) 8 слотов для USB-устройств, а в Windows их всего 10...
    - При установке других токенов и смарт-карт на такой компьютер - они не работают
  - Так коллеги метят свою территорию и не пускают конкурентов - страдают клиенты и разработчики других систем и сервисов

Спасибо

Будь собой в электронном мире!

Контакты:

Сергей Груздев

www.aladdin-rd.ru
+7 (495) 223-0001

Будь собой в электронном мире!

- Лицензии ФСТЭК России № 0037, № 0054, № 2874
- Лицензии ФСБ России № 12632Н, № 24530
- Сертификат соответствия системы управления качеством СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00079 от 29.07.14

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

*Приведённая информация актуальна по состоянию на **15 февраля 2015 г.***