конференция РусКрипто

# Практика внедрения и использования Трастскринов для радикального снижения рисков в ДБО

АО «БИФИТ»

# О чем мы говорили год назад

- ✓ Число инцидентов растет и будет расти
- ✓ Среда клиента стала тотально враждебной
- ✓ Правильный путь – перенос выполнения криптографических функций на доверенные аппаратные платформы с визуализацией подписываемых данных

Все наши прогнозы сбылись

# Хищения в ДБО: текущие тенденции

- ✓ Количество группировок увеличилось с 6 до 8
- ✓ Появление нового вектора атаки (на банки) не привело к снижению частоты атак на клиентов
- ✓ Атаки усложнились – в частности, отмечаем реальные инциденты с одновременными атаками на компьютер и смартфон клиента (для обхода SMS-подтверждения)

# Новое поколение ПАК – Трастскрин

## Поддержка в системе «iBank 2»


Трастскрин 1.0


РУТОКЕН PinPAD

## Практика использования

56 банков приобрели Трастскрины

5 банков осуществляют полный перевод на них корпоративных клиентов ДБО

## Перевод клиентов на Трастскрины: опыт банков

Новые клиенты подключаются с обязательным использованием Трастскрина

Перевод существующих клиентов производится при плановой смене ключей ЭП

## Выводы из эксплуатации

### Преимущества решения:

+ простота и удобство работы клиента
+ простота дистрибуции и администрирования
+ максимальная защищенность
+ экономическая выгода
+ визуализация только критичных полей

## Выводы из эксплуатации

### Недостатки решения:

- подпись каждого документа с визуализацией неудобна и создает потенциальные риски
- невозможность использования с мобильных платформ

## Адаптивная подпись с визуализацией

Решение принимается отдельно стоящей в банке системой Fraud-мониторинга на основании оценки риска по платежу.

Количество подписей с визуализацией - до 2%

Снижается риск атак методами социальной инженерии

# Трастскрины для мобильных платформ

## Трастскрин 2.0

Ключевые особенности:

- ✓ уменьшение размеров
- ✓ OLED-дисплей и аккумулятор
- ✓ Возможность работы по BlueTooth LE 4+

  (с сохранением подключения по USB)

**Пилот – май 2016 года**

## Трастскрин 2.0 – опыт разработки

### Особенности работы с мобильными платформами:

- скорость BlueTooth LE – 10-50 kBit/sec
- время на подпись документов – до 5 минут
- ограничения на встраивание СКЗИ в мобильные платформы

## Трастскрин 2.0 – опыт разработки

### Пути решения:

- расчет hash-функции на стороне сервера
- подготовка CMS-контейнера (hash + параметры + визуализируемые данные) на стороне сервера
- подписание Трастскрином CMS-контейнера
- проверка корректности подписи и визуализации на стороне сервера

# Трастскрины: опыт эксплуатации и внедрения

## Выводы

1. Опыт практического использования Трастскринов исключительно позитивный
2. Необходимо насыщение рынка сертифицированными решениями
3. Решения должны учитывать практические требования (поддержка мобильных платформ, работа с большим документооборотом)

# Трастскрины: опыт эксплуатации и внедрения

## Стратегические цели

1. Не дать простой ЭП стать главным механизмом в ДБО
2. Вернуть усиленной ЭП роль реального средства защиты, а не формальности

Альтернатива – смерть рынка СКЗИ для ДБО

# Спасибо

за внимание

shilov@bifit.com