

Технологии «Смотри, что подписываешь»

в системах ДБО юридических и физических лиц

Денис Калемберг

Генеральный директор

Башкортостан, 2014

О Компании

- Была основана в 2010г.;
- Разработчик и поставщик средств безопасности систем ДБО;
- Первые внедрения устройств с возможностью визуализации подписываемых данных SafeTouch – 2012г.;
- На сегодняшний день клиентами компании являются 43 банка из России и Казахстана, в том числе, входящие в список ТОП-30;
- В 2013г. в продуктовую линейку компании вошли новые решения, как для юридических, так и для физических лиц.

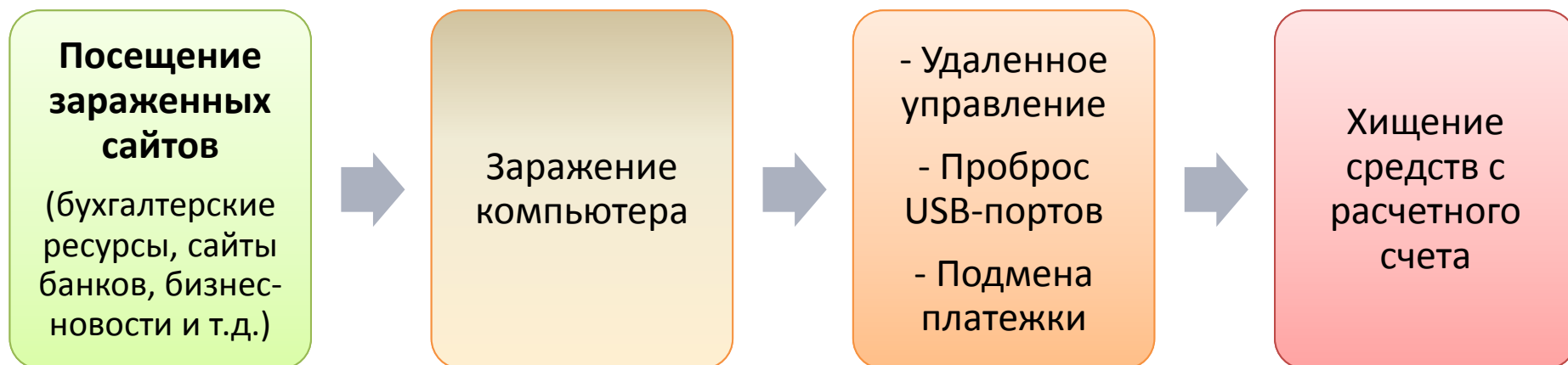
Проблемы безопасности систем ДБО. Текущая ситуация

- За последний год Центробанком было зафиксировано **более 18000** инцидентов хищения у клиентов систем Интернет-банкинга.
- **Клиент** в любой момент **может отказаться** от проведенного им платежа, сославшись на то, что его не проинформировали об операции по счету.*

* С 1 января 2014г. вступил в силу **9-я глава 161-ФЗ** «О национальной платежной системе», согласно которой оператор обязан возместить клиенту сумму операции, о которой он его не проинформировал.

Почему хищения возможны?

- Незащищенность компьютеров от современных вирусов (Антивирусное программное обеспечение не эффективно);
- Массовые заражения крупнейших легальных сайтов компьютерными вирусами;
- Возможность удаленно управлять зараженным компьютером через Интернет;



Как происходит атака:

Вредоносное ПО

74 65 6D 70 6C 61 74 65	20 22 45 78 74 32 2F 45
78 74 33 20 47 72 6F 75	70 20 44 65 73 63 72 69
70 74 6F 72 22 0D 0A 0D	0A 2F 2F 20 43 72 65 61
74 65 64 20 62 79 20 4A	65 6E 73 20 4B 69 72 73
63 68 6E 65 72 20 6F 6E	20 53 65 70 20 32 39 2C
20 32 30 30 34 0D 0A 2F	2F 20 58 2D 57 61 79 73
20 53 6F 66 74 77 61 72	65 20 54 65 63 68 6E 6F
6C 6F 67 79 20 41 47 0D	0A 0D 0A 64 65 73 63 72
69 70 74 69 6F 6E 20 22	4C 6F 63 61 74 65 73 20
74 68 65 20 6D 65 74 61	20 62 6C 6F 63 6B 73 20
66 6F 72 20 61 20 62 6C	6F 63 6B 20 67 72 6F 75
70 22 0D 0A 61 70 70 6C	69 65 73 5F 74 6F 20 64

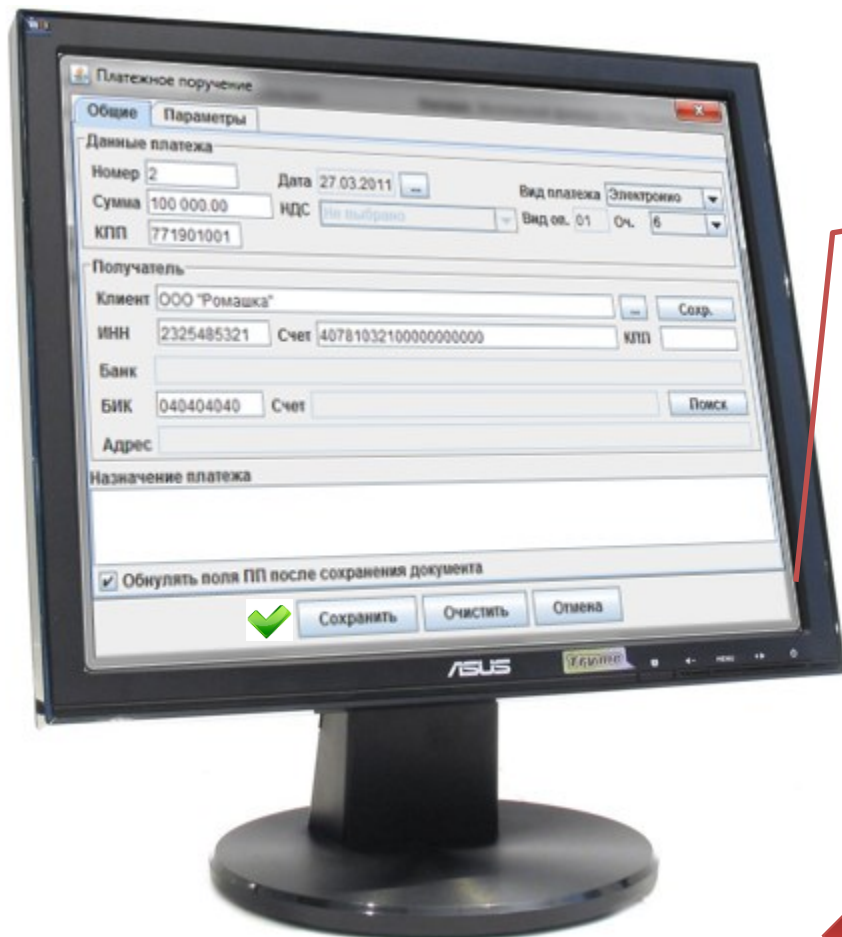
Данные

74 65 6D 70 6C 61 74 65
78 74 33 20 47 72 6F 75
70 74 6F 72 22 0D 0A 0D
74 65 64 20 62 79 20 4A
63 68 6E 65 72 20 6F 6E
20 32 30 30 34 0D 0A 2F
20 53 6F 66 74 77 61 72
6C 6F 67 79 20 41 47 0D
69 70 74 69 6F 6E 20 22
74 68 65 20 6D 65 74 61
66 6F 72 20 61 20 62 6C
70 22 0D 0A 61 70 70 6C

Подпись

6F 63 6B 20 67 72 6F 75
69 65 73 5F 74 6F 20 64

Подпись подмененного документа



SafeTouch. Средство визуализации подписываемых данных.



Защита от **всех** известных на сегодняшний день удаленных атак:

- Визуальный контроль данных, передаваемых на подпись;
- Блокирование операции подписи до момента **физического нажатия** кнопки подтверждения.

Поддержка **всех** российских аппаратных СКЗИ (средств подписи):

- eToken ГОСТ, JaCarta ГОСТ, eToken PRO;
- Рутокен ЭЦП;
- MS-Key;
- КриптоПро Рутокен CSP, КриптоПро eToken CSP, КриптоПро Магистра CSP.

SafeTouch. Попытка подмены документа

Вредоносное ПО



74 65 6D 70 6C 61 74 65	20 22 45 78 74 32 2F 45
78 74 33 20 47 72 6F 75	70 20 44 65 73 63 72 69
70 74 6F 72 22 0D 0A 0D	0A 2F 2F 20 43 72 65 61
74 65 64 20 62 79 20 4A	65 6E 73 20 4B 69 72 73
63 68 6E 65 72 20 6F 6E	20 53 65 70 20 32 39 2C
20 32 30 30 34 0D 0A 2F	2F 20 58 2D 57 61 79 73
20 53 6F 66 74 77 61 72	65 20 54 65 63 68 6E 6F
6C 6F 67 79 20 41 47 0D	0A 0D 0A 64 65 73 63 72
69 70 74 69 6F 6E 20 22	4C 6F 63 61 74 65 73 20
74 68 65 20 6D 65 74 61	20 62 6C 6F 63 6B 73 20
66 6F 72 20 61 20 62 6C	6F 63 6B 20 67 72 6F 75
70 22 0D 0A 61 70 70 6C	69 65 73 5F 74 6F 20 64



Успешные проекты

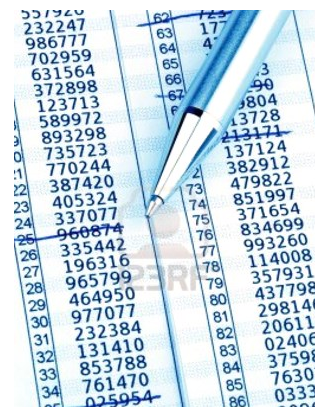
- Банк «Возрождение»;
- Банк «Нейва»;
- Банк «Русь»;
- Банк «Кольцо Урала»;
- Экономбанк;
- Межтопэнергобанк;
- Независимый строительный банк;
- Военно-промышленный банк;
- Башкомснаббанк;
- Собинбанк;
- Чувашкредитпромбанк;
- Волжский социальный банк;
- Кредитимпэксбанк;
- банк «Снежинский»;
- Вита банк;
- Мосстройэкономбанк;
- Московский Индустриальный Банк
- Крайинвестбанк
- Банк «Балтика»;
- Гута банк;
- БайкалИнвестБанк;
- Первый ДорТрансБанк;
- Банк «Кредит-Москва»;
- Банк «БТА-Казань»;
- Банк «Аверс»;
- Констансбанк;
- Банк «Развитие»;
- Банк «Таврический»;
- ПриоВнешторгбанк
- Банк «Кузнецкий»;
- и многие другие...

Средства подтверждения в системах ДБО для физлиц

Одноразовые пароли

- SMS
 - негарантированная доставка
 - задержки в доставке
 - возможность перехвата на уровне канала связи или ввода в систему
 - возможность перехвата на уровне оператора мобильной связи
 - возможность переоформления сим-карты клиента на мошенника по поддельной доверенности (и перехвата SMS)
 - возможность направления клиенту SMS-сообщений с подменного номера
 - цена
- Скретч-карты
 - требуют регулярных визитов клиента в банк
 - в век мобильных технологий выглядят архаично
- Аппаратные генераторы одноразовых паролей
 - цена около 600 рублей
 - необходимость иметь его под рукой

Podtverdite oplatu
interneta na summu
800.00 RUR na schet
916296. Parol: 709461.



Нет привязки
к реквизитам



Нет защиты от
фишинга

«Продвинутые» средства подтверждения

Коды подтверждения транзакций (MAC)

- Аппаратные MAC-токены (криптокалькуляторы)
 - требуется вручную вводить реквизиты платежа
 - стоимость от 700 рублей
- Оптические MAC-токены
 - автоматически считывают с экрана реквизиты платежа
 - стоимость 1500 руб. (целевая аудитория – VIP-клиенты)



Что делать с обычными клиентами?

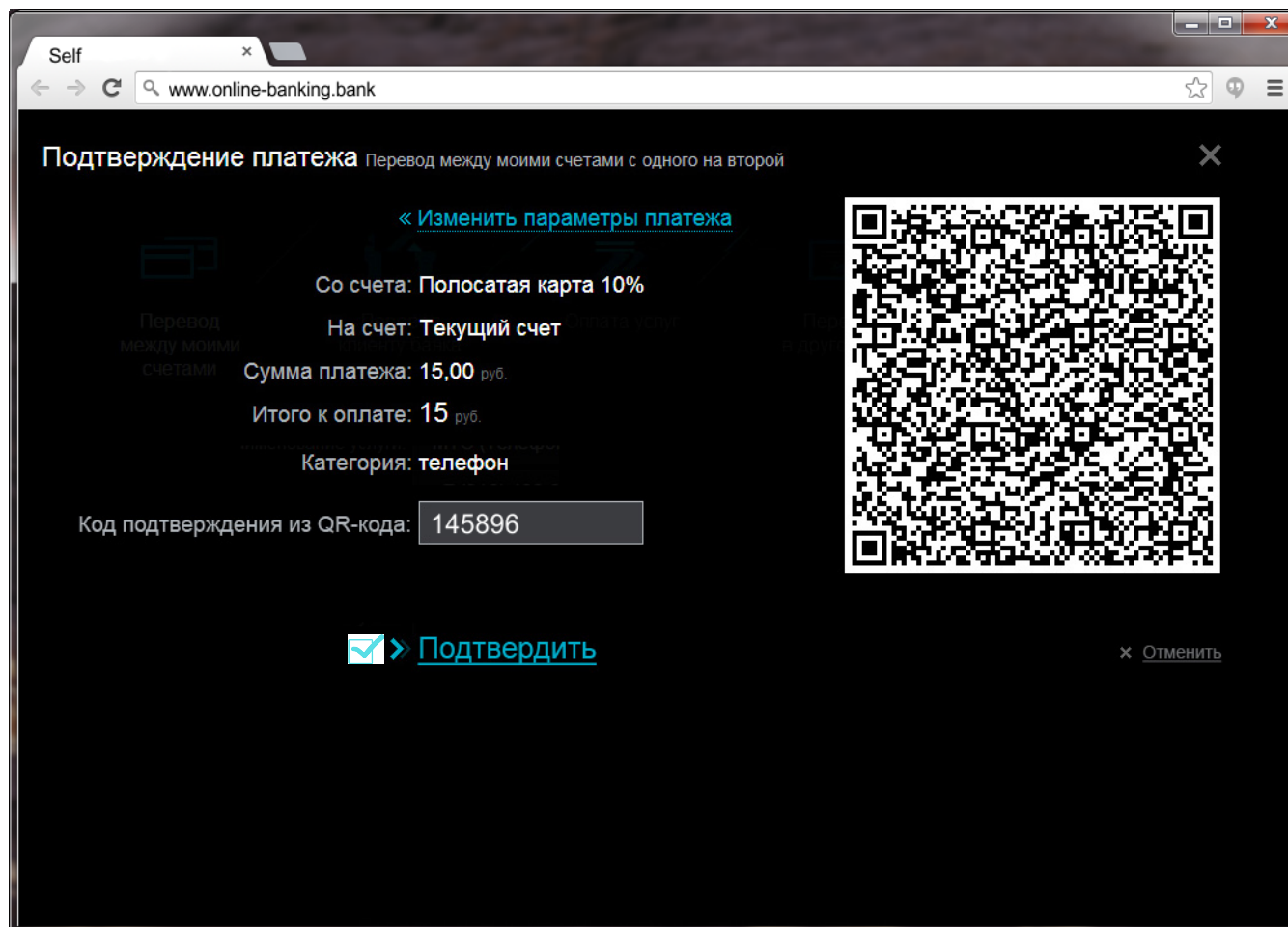
PayControl. «Оптический MAC-токен» в смартфоне

Мобильное приложение для iOS и Android-устройств

- Удобное считывание документа с экрана монитора при помощи **QR-кода**
- **Визуальный контроль** подписываемого документа любого формата на отдельном устройстве (телефоне или планшете)
- Генерация **кода** подтверждения, «**привязанного**» к реквизитам платежа
- Телефон может находиться в «**офлайне**»
- **Гарантированное уведомление клиента** о совершаемой транзакции

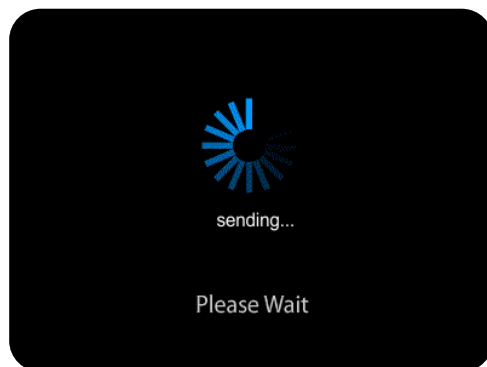


PayControl



PayControl. Преимущества для клиента

Не нужно ждать SMS



Гарантированная работа в роуминге



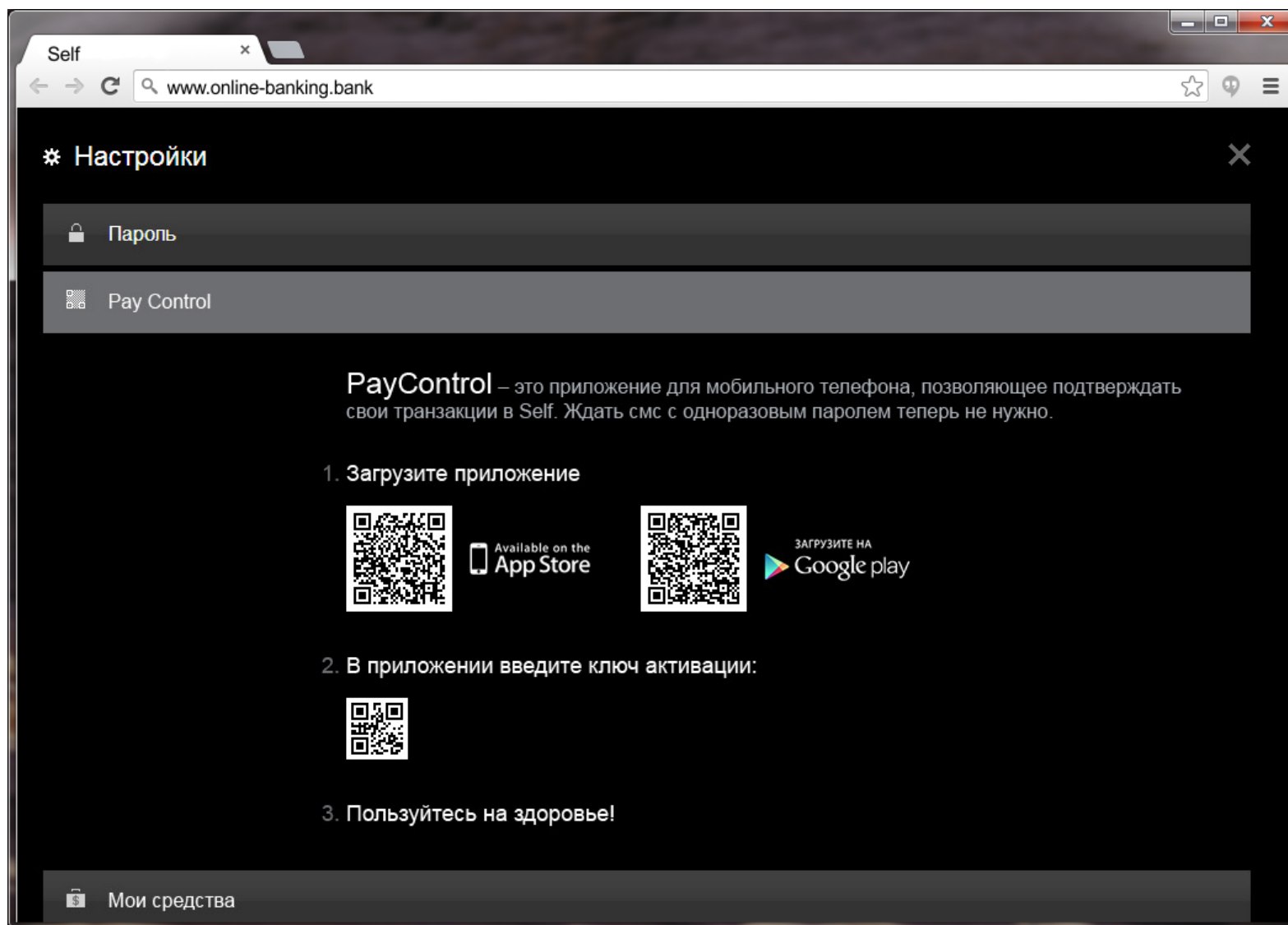
Действительно безопаснее и удобнее



Выше лимиты по операциям



PayControl. Как подключать пользователей



PayControl. Преимущества для банка

Снижение убытков от кибер-мошенничества

- Уменьшение количества инцидентов краж со счетов клиентов
- Выполнение требований ФЗ-161 в части гарантированного уведомления пользователей о совершаемых транзакциях (защита от «дружественного фрода»)

Быстрая монетизация проекта

- Повышение лимитов на совершаемые клиентами операции увеличивает комиссионный доход банка
- Стоимость старта проекта – \$5,000. Клиентские лицензии приобретаются по принципу пост-оплаты, уже после подключения пользователей
- Клиенты готовы платить за «продвинутый» сервис безопасности 30-40 рублей в месяц, что позволяет банку получать значительную прибыль

«Смотри, что подписываешь»

Для физических лиц



eToken 3500



PayControl

Для юридических лиц



SafeTouch для смарт-карт



SafeTouch для USB-токенов

Спасибо за внимание
Вопросы?

Денис Калемберг
d.kallemberg@safe-tech.ru