Доверенная среда в системах ДБО для юридических и физических лиц

Опыт реальных проектов и новые разработки

Денис Калемберг
Генеральный директор

Москва
29 мая 2013г.

Немного о компании SafeTech

- Была основана в 2010г., как разработчик средств безопасности систем ДБО
- Первые внедрения считывателя смарт-карт с возможностью визуализации подписываемых данных SafeTouch – 2012г.
- На сегодняшний день клиентами компании являются более 30-ти российских банков, в том числе, входящих в список ТОП-30
- В 2013г. в продуктовую линейку компании вошли новые решения класса «Доверенная среда» как для юридических, так и для физических лиц.

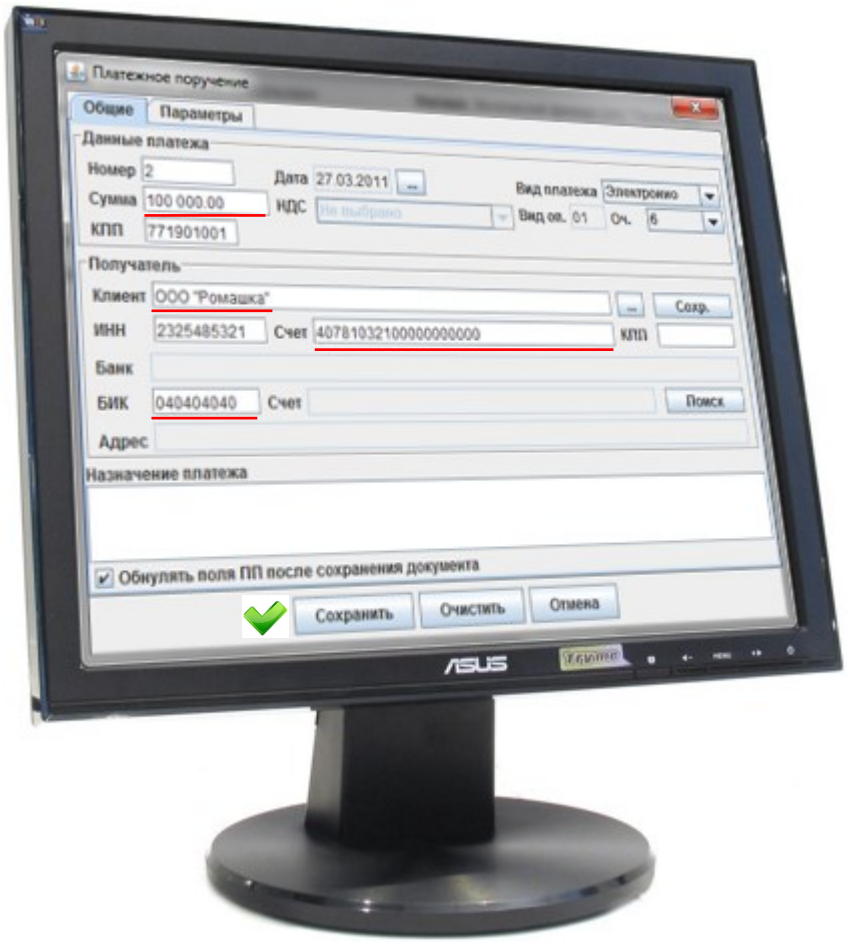
Системы ДБО для юридических лиц

Средства создания доверенной среды

Считыватель смарт-карт SafeTouch

- Защита от всех известных на сегодняшний день удаленных атак
  - Визуальный контроль данных, передаваемых в смарт-карту
  - Блокирование операции подписи до момента нажатия кнопки подтверждения
- Работа со смарт-картами, аппаратно реализующими российские криптографические алгоритмы
- Соответствие спецификации USB-CCID
  - работа без установки драйверов на современных операционных системах
  - Кроссплатформенность (Windows, MAC OS, Linux)

SafeTouch. Нормальная работа



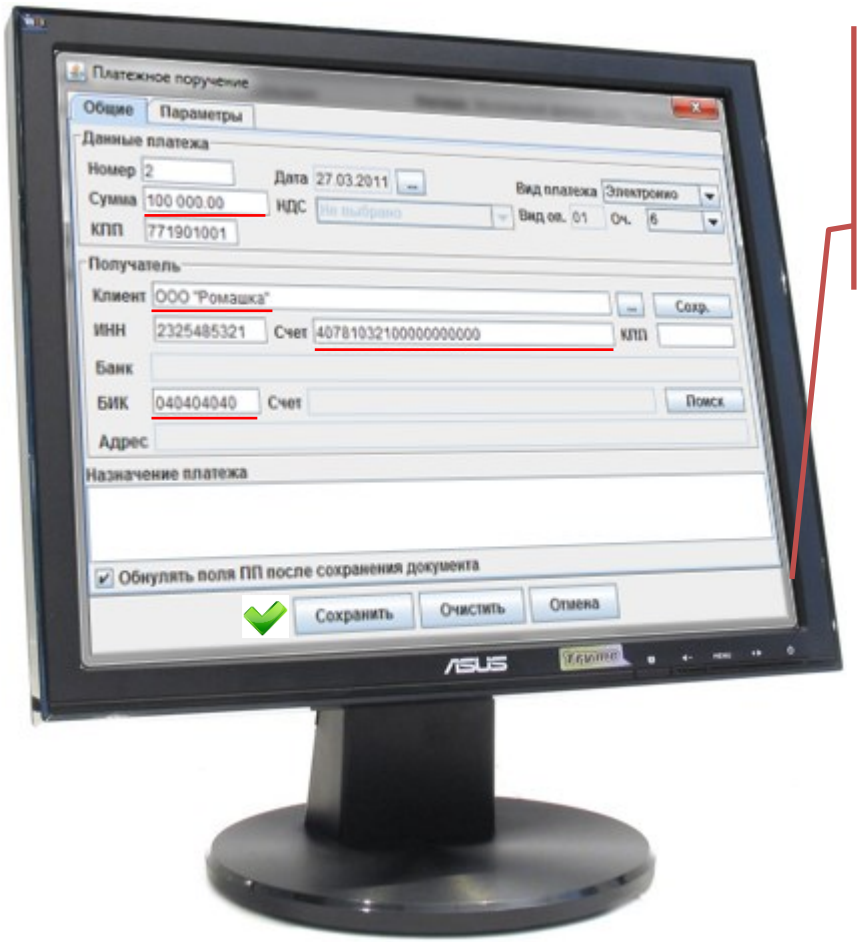
Данные

```
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
```

```
66 6F 72 20 61 20 62 6C
70 22 0D 0A 61 70 70 6C
```

Подпись

SafeTouch. Попытка подмены платежного 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
```

SafeTouch. Этапы проектов по внедрению в банках

I. Анализ количества платежей, которые подписывают клиенты.

Итог: Более 90% клиентов подписывают до 20 платежных документов в день.

II. Пилотное внедрение для VIP-клиентов, по результатам которого собирались отзывы об удобстве работы.

Итог: Зафиксирован всего один отказ у клиента, который подписывал более 100 платежей в день.

Вывод: Выполнена интеграция SafeTouch с «белыми» списками контрагентов, в результате на экран стали выводиться реквизиты только по новым получателям и количество нажатий сократилось в десятки раз.

III. Разработка маркетинговых материалов для клиентов, обучение менеджеров банка, подготовка тарифной сетки.

Итог: Как показал опыт, это самый важный этап проекта. От его проработки зависит, какими темпами клиенты будут переходить на новую технологию защиты.

Развитие линейки. SafeTouch PRO

- Одновременная работа с USB-токенами и со смарт-картами, аппаратно реализующими российские криптографические алгоритмы
- Увеличенный дисплей для более полного отображения реквизитов
- Более удобный механизм подтверждения

Системы ДБО для физических лиц

Второй канал подтверждения транзакций

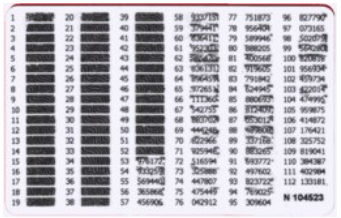
Одноразовые пароли

- **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.

- **Скретч-карты**

  - требуют регулярных визитов клиента в банк.



- **Аппаратные генераторы одноразовых паролей**

  - цена около 600 рублей.

(!) Ни одна из реализаций технологии одноразовых паролей не защищает от фишинга и подмены документа при передаче в банк

Коды подтверждения транзакций

- **Аппаратные криптокалькуляторы**
  - требуется вручную вводить реквизиты платежа;
  - стоимость от 700 рублей.

- **Оптические токены**
  - автоматически считывают с экрана реквизиты платежа;
  - стоимость около 1500 руб. (целевая аудитория – VIP-клиенты)

SafeNet eToken 3500

(!) Передача аппаратных средств безопасности большому количеству частных клиентов приводит к необходимости выстраивания в банке сложной логистической схемы и появлению дополнительных расходов

PayControl. Мобильное средство подтверждения платежей в системах Интернет-банкинга

Мобильное приложение для iOS и Android-устройств

- Считывание реквизитов платежа 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;
- Не зависит от наличия канала сотовой связи;
- Гарантированное уведомление клиента о совершаемой транзакции.

PayControl. Мобильное средство подтверждения платежей в системах Интернет-банкинга

Другому клиенту Банка → Подтверждение перевода → Статус

Шаблоны (2) Последние переводы

Номер счёта: 40817810904010727071
Введите номер счета, на который будет произведен перевод средств Подробнее

ФИО получателя: Иванову Петру Станиславовичу
Введите ФИО получателя Подробнее

Назначение перевода: За поставку экскаватора
Введите назначение платежа (например: "Оплата счета за проживание в отеле") Подробнее

Перевод со счета: Текущий зарплатный счет ...8202 784 504.27 р.
Выберите счет, с которого вы хотите перевести средства.

Сумма: 15000.00 р.
Введите сумму перевода. Подробнее

Сделать перевод: сейчас

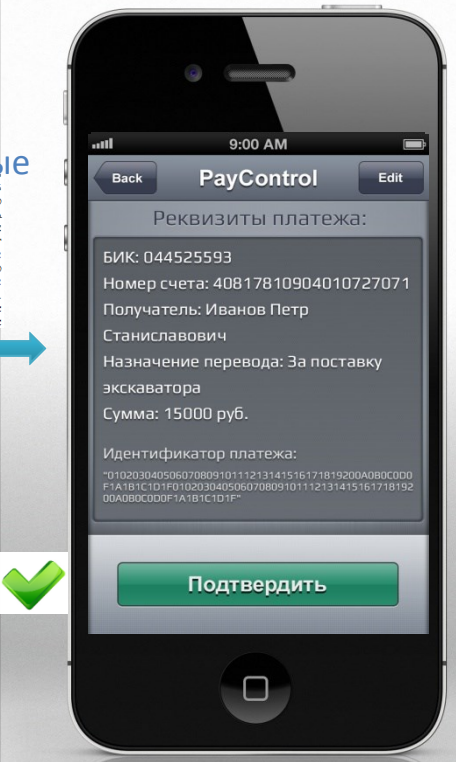
Идентификатор: 0102030405060708091011121314151617181920 0A0B0C0D0F1A1B1C1D1F0102 0304050607080910111213141516171819200A0B0C0D0F1A1B1C1D1F

Хотите сохранить этот перевод как шаблон?

Код подтверждения: 145896

Перевести

Данные



PayControl. Безопасность

- Документ создается и подтверждается на разных устройствах
  - Клиент видит реквизиты документа на экране телефона и имеет возможность проконтролировать, что его платеж не подменен;
  - Для совершения успешной атаки злоумышленник должен получить доступ и к компьютеру клиента и к его мобильному телефону
  - Данные транзакции подписываются как на стороне клиента (простая ЭП), так и на стороне банка (по сертифицированным алгоритмам ГОСТ)
- Разделение каналов передачи ключевой информации клиенту
  - В момент подключения услуги часть ключа подписи передается при помощи QR-кода, а часть – высылается при помощи SMS.
- Неотказуемость клиента от совершенного платежа
  - Клиент подтверждает не только реквизиты платежа, но и расписывается в получении уведомления о совершаемой операции.

PayControl. Применимость

- Приемлемая цена
  - Сравнимо со стоимостью отправки одноразовых паролей при помощи SMS.
- Нет зависимости от каналов сотовой связи
  - Работа в роуминге, вне зоны покрытия оператора и т.д.
- Просто для пользователя
  - Интуитивно понятный интерфейс;
  - Не требуется вводить реквизиты платежей вручную.

Спасибо за внимание

Вопросы?

Денис Калемберг

d.kalemberg@safe-tech.ru