Межбанковская конференция «Актуальные вопросы обеспечения информационной безопасности банков и защиты информации при осуществлении перевода денежных средств в национальной платежной системе Российской Федерации»

Trusted-платформы для электронного банкинга. Методология использования и оптимизация применения в iBank 2.

Компания «БИФИТ»

МОСКВА, 2013

Обеспечение доверенной среды в ДБО

Задача: использовать доверенную среду для формирования подписи (подтверждения) документов в системах электронного банкинга

Способ обеспечения:

1. **Решения типа «TrustScreen»**
2. **Аппаратные платформы дополнительного подтверждения**

TrustScreen

Назначение

1. Визуализация подписываемых документов в доверенной среде (trusted-платформе)
2. Формирование электронной подписи по ГОСТ
3. Неизвлекаемое хранение ключа подписи

TrustScreen

Особенности текущих устройств:

Плюсы:

- Использование сертифицированных СКЗИ
- Возможность подписи произвольных документов

Минусы:

- Разделение устройств на «ключ» и «экран»
- Необходимость замены текущих устройств
- Высокая стоимость

Аппаратные платформы доп.подтверждения

Требования к решению:

- защита критичных реквизитов платежа
- гарантированное получение кода подтверждения
- неуязвимость для вредоносного ПО
- использование совместно с имеющимися СКЗИ

Примеры таких решений:

- MAC-токены
- AGSES-карты

MAC-токены (Message Authentication Code)

Назначение:

формирование кода подтверждения документа во внешнем, защищенном устройстве

Способ ввода информации:

ручной ввод с клавиатуры

MAC-токены

Схема работы:

1. В устройство вводятся ключевые реквизиты документа
2. Устройство вычисляет код подтверждения
   как криптографическую функцию
   от введенных данных и «секрета» (ключа),
   зашитого в устройство на этапе производства

БИК
Счет
Сумма

➔ *Код подтверждения*

3. Пользователь вводит код подтверждения в систему ДБО
   для передачи на сервер вместе с документом
4. Сервер верифицирует код подтверждения
   (симметричный алгоритм)

BIFIT

MAC-токены

В системе «iBank 2» поддерживаются MAC-токены ActivIdentity Token V2 и Pocket Token

Области применения:

- **расширенная аутентификация (одноразовый пароль)**
- **подтверждение платежных поручений корпоративных и частных клиентов**
- **подтверждение произвольных документов (платежи, заявки) частных клиентов**

BIFIT

MAC-токены

Преимущества

- абсолютная неуязвимость устройства
- получение кода подтверждения сразу
  (по сравнению с вариантом получения SMS)
- дополнительные функции (аутентификация)

Недостатки

- «накладные расходы» на операции
  при большом количестве документов
- поддержка ограниченного набора типов документов

AGSES-карты

Назначение:

аутентификация и подтверждение документов (аналогично MAC-токену)

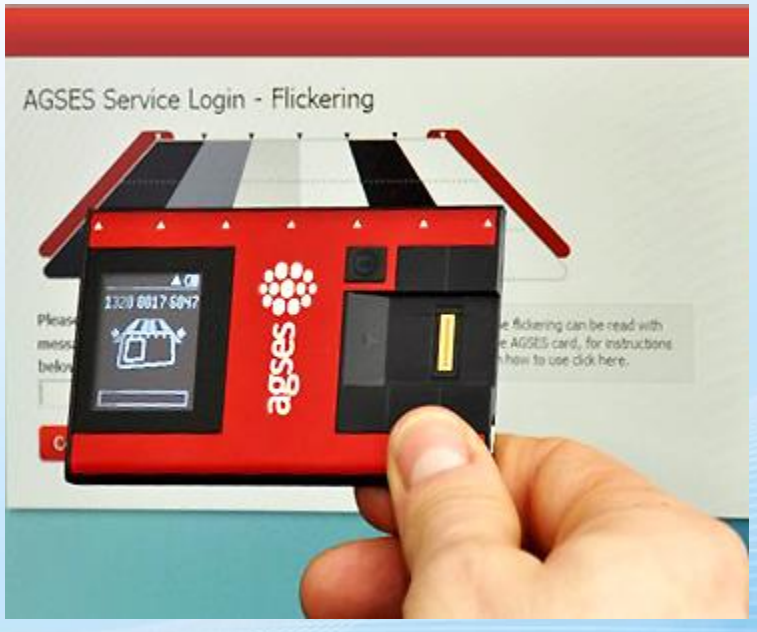
Особенности:

- **оптический ввод**
- **сканер отпечатка пальца**

AGSES-карты

Оптический ввод осуществляется через набор мигающих черных и белых полос (фликер-код), отображаемых на экране компьютера

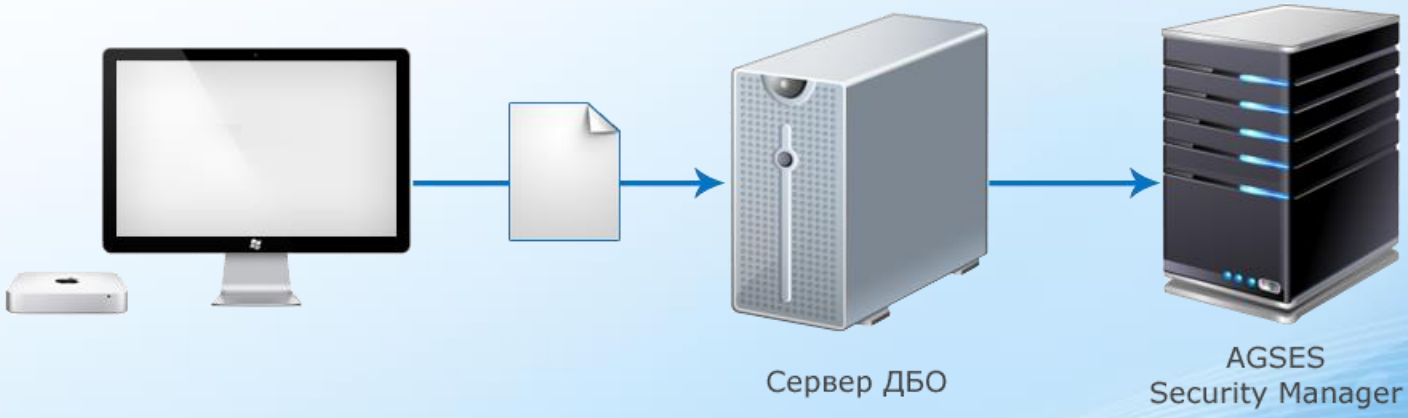
Фликер-код содержит закодированное содержимое транзакции и пароль (код подтверждения)



AGSES-карты

Принцип работы

1. Клиент создает в ДБО документ.
   Сервер ДБО передает реквизиты клиентского документа Серверу Аутентификации – AGSES Security Manager (SM)



AGSES-карты

Принцип работы

2. SM генерирует код подтверждения и вместе с реквизитами транзакции шифрует его на секретном ключе AGSES-кары. Информация передается на клиентское приложение для представления в виде фликер-кода

AGSES-карты

Принцип работы

3. Клиент считывает фликер-код AGSES-картой.
   После биометрической аутентификации AGSES-карта расшифровывает фликер-код и показывает на экране реквизиты транзакции и код подтверждения

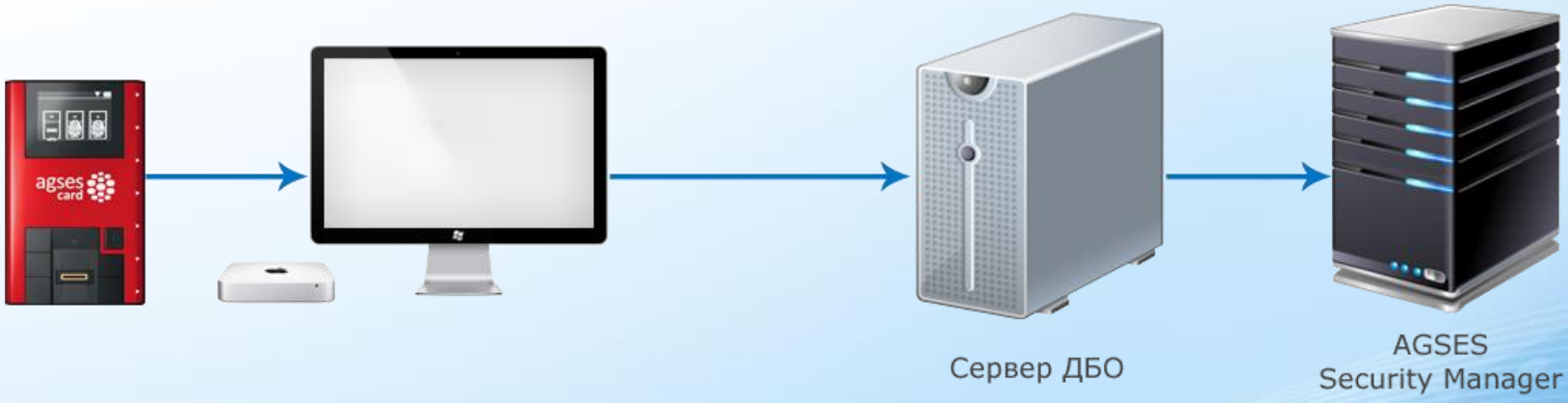
Сервер ДБО

AGSES
Security Manager

AGSES-карты

Принцип работы

4. Клиент вводит код подтверждения в приложение.
   Код подтверждения передается в SM для верификации



AGSES-карты

Преимущества

- все плюсы MAC-токенов, а также:
- простой и быстрый ввод данных
- физическая безопасность (биометрия)
- удобный размер и форм-фактор

Недостатки

- «VIP-решение по VIP-цене»

Trusted-платформы: недостатки

Принципиальная особенность Trusted-платформ – необходимость ручного подтверждения каждой операции с визуальным контролем ее реквизитов

Но такой подход имеет обратную сторону:

- неприменим при большом документообороте;

- создает угрозу атак с помощью социальной инженерии:

- **фродовый платеж с реквизитами, похожими на настоящие;**
- **фродовый платеж в пачке из 50 настоящих платежей.**

Эти же недостатки присущи и TrustScreen-ам

Trusted-платформы: оптимизация

Оптимизация использования: как уменьшить количество действий клиента?

Справочник доверенных получателей в iBank 2

- Каждая запись содержит: БИК, счет, лимит суммы операции

- Подтверждаются реквизиты только для новых получателей (БИК, счет, лимит суммы операции),

- Повторный платеж в пользу доверенного получателя в пределах установленного лимита не требует дополнительного подтверждения

Trusted-платформы: оптимизация

Справочник доверенных получателей в iBank 2

Важно!

1. Клиент управляет списком самостоятельно,
   без обращений к сотрудникам банка
2. Возможно плановое заполнение (изменение) списка
3. При поступлении на сервер iBank 2 платежа
   а) в адрес нового получателя
   б) на сумму свыше лимита для этого получателя

   пользователь (клиент) может:
   - подтвердить только этот платеж
   - нести нового получателя в список доверенных
     (или увеличить лимит для уже существующего получателя)

Trusted-платформы: оптимизация

Аналогичные подходы используются в промышленных системах Fraud-мониторинга

Пример: RSA Transaction Monitoring

Механизм Adaptive Authentication требует дополнительного подтверждения не всех транзакций, а только тех, которые превысили заданный в системе уровень риска

Межбанковская конференция «Актуальные вопросы обеспечения информационной безопасности банков и защиты информации при осуществлении перевода денежных средств в национальной платежной системе Российской Федерации»

Trusted-платформы для электронного банкинга. Методология использования и оптимизация применения в iBank 2.

Шилов Станислав
shilov@bifit.com

BIFIT