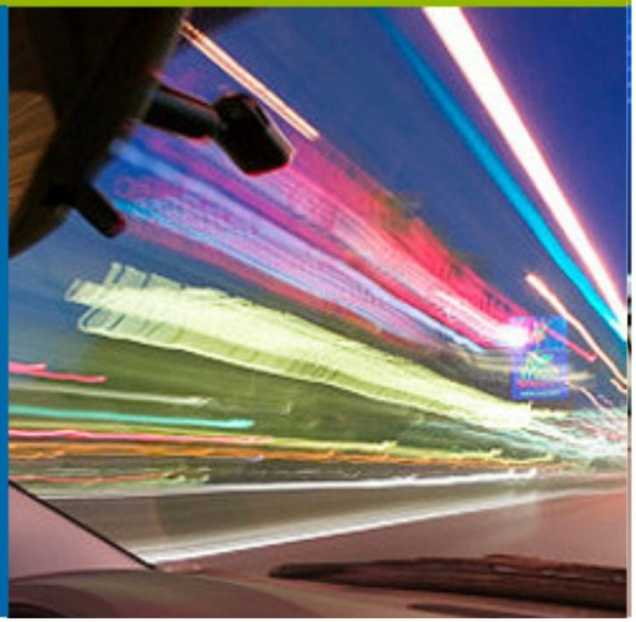
Аутентификационный центр - решение для интернет-банкинга



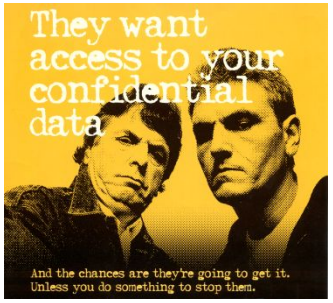
Чернышев Антон
anton@computel.ru

Содержание

- Типовые угрозы в реальной среде
- Механизмы защиты
- Способы аутентификации
- Аутентификационный центр
- Архитектура решения
- Пример EMV-аутентификации
- Подпись транзакции
- Свойства решения
- Вопросы

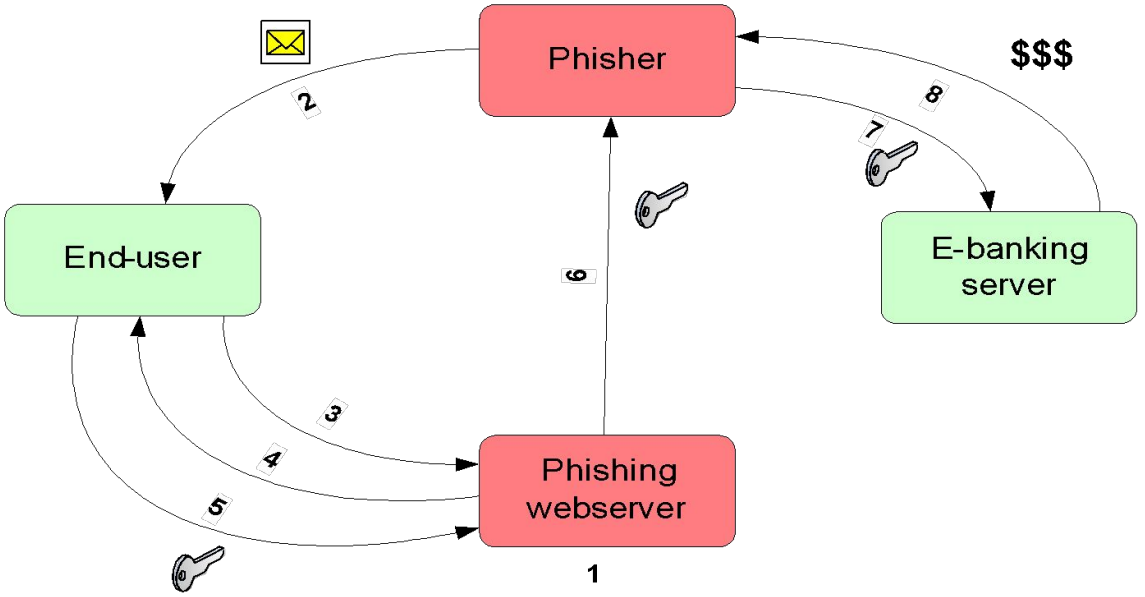
Типовые угрозы в реальной среде

- Работа в открытой среде Интернет
  - Компьютер клиента не является доверенной средой
  - Вся передаваемая информация не тайна
  - Вся передаваемая информация может быть изменена по пути
- Выманивание информации с использованием методов социальной инженерии
  - Фишинг
  - Подставные сайты
  - Специально разработанные вирусы – трояны
- Угрозы для серверной части
  - Инсайд, коммерческий подкуп, шантаж …



Фишинг

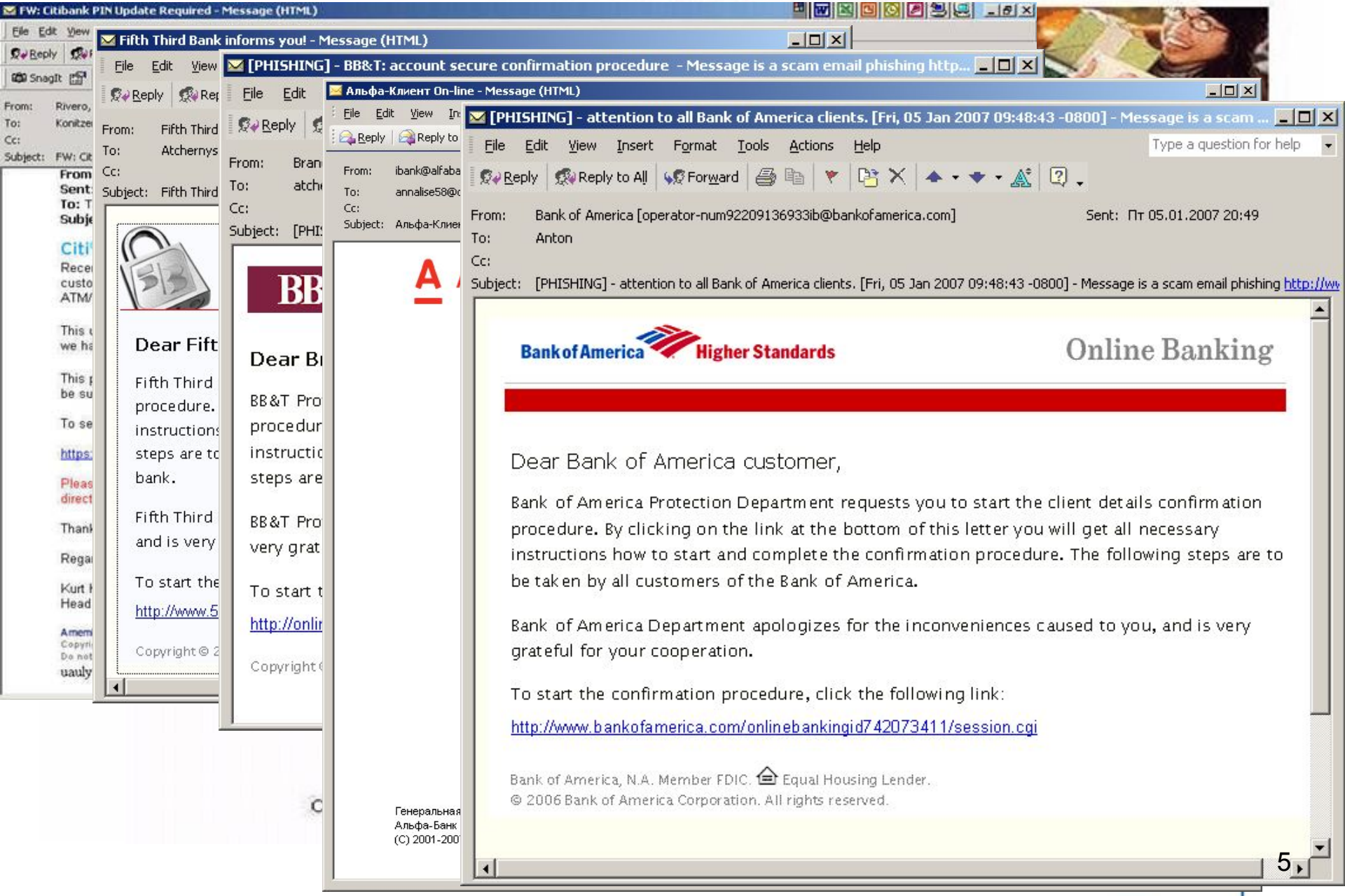
- Попытка мошенническим путем получить важную информацию, такую как имя пользователя, пароли или данные о параметрах платежных карт, путем представления мошенника в качестве заслуживающей доверия организации с использованием электронных каналов



А также:

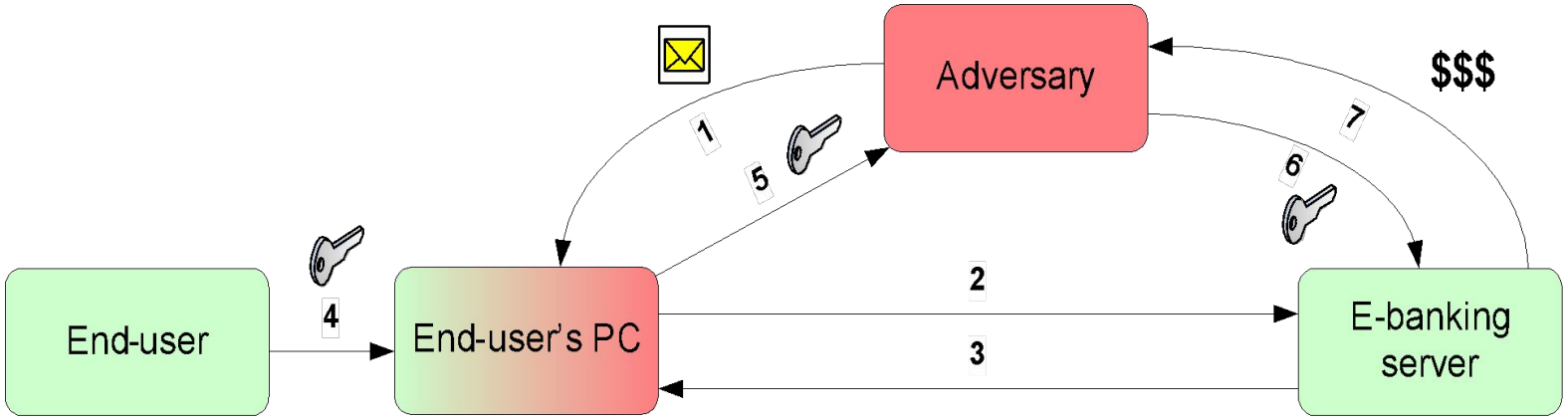
- **Голосовой фишинг**
- **SMS фишинг**
- **Вмешательство в работу DNS серверов**

Примеры выуживания паролей



Шпионское ПО

- Попытка незаконным путем получить доступ к важной информации, как-то: имена пользователей, пароли, номера платежных карт путем скрытого перехвата информации, передаваемой во время информационного обмена



Механизмы защиты

- Строгая Аутентификация пользователей

  Действительно ли перед нами тот кто мы думаем?

- Проверка целостности транзакций

  Соответствует ли пришедшая транзакция запрошенной клиентом?

- Аудит операций

  Кто, когда, какую выполнял операцию и по какому праву?

Множество механизмов аутентификации

–Простой пароль - однозначно нет

–Одноразовые пароли на основе времени/события

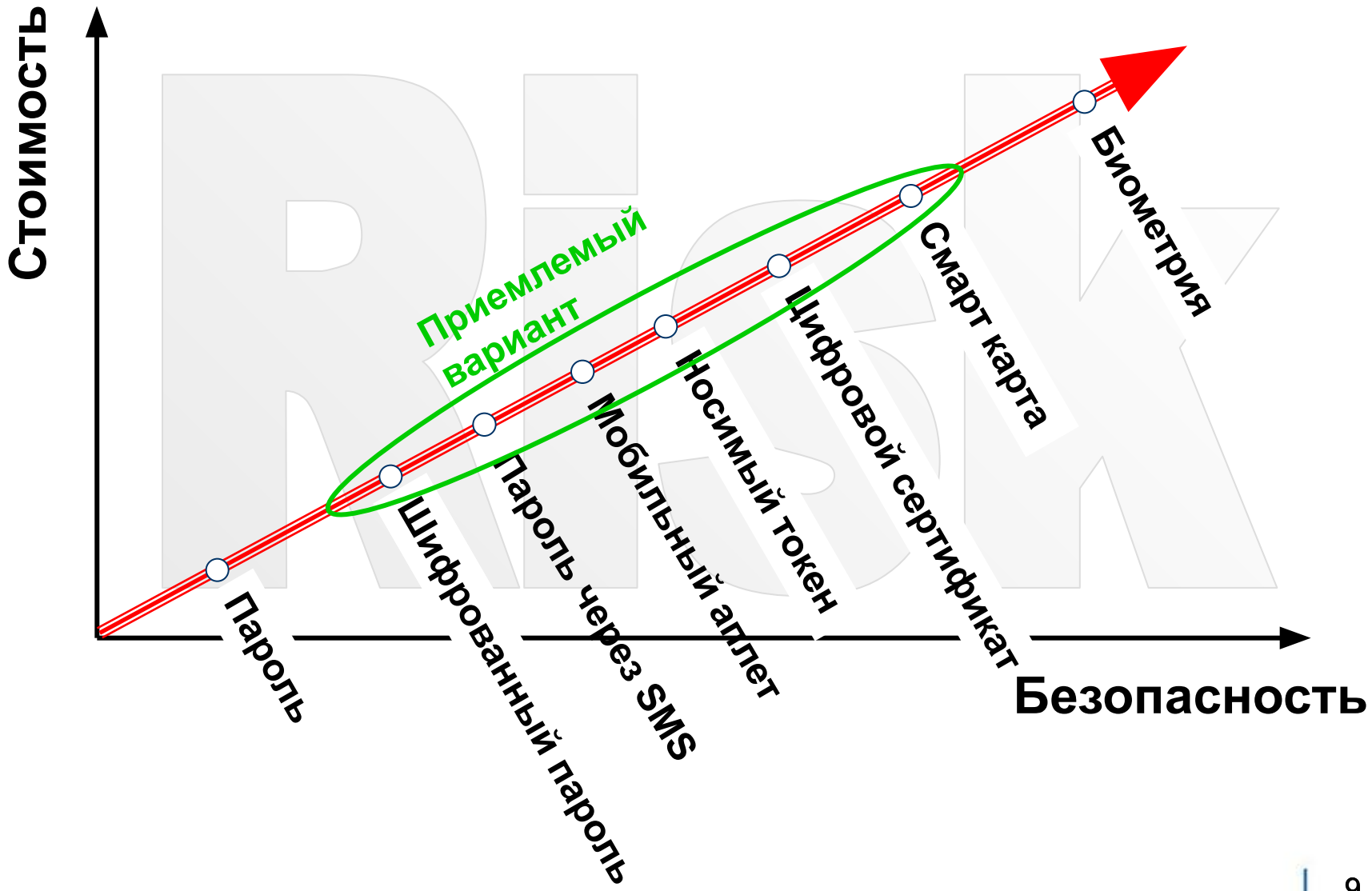
–Запрос – ответ, обеспечение целостности транзакции

–EMV механизмы, CAP

–На основе несимметричных алгоритмов (PKI)

–Специфические механизмы привязки к мобильным устройствам

Механизмы аутентификации



Аутентификационный центр

Computel

safeSIGN

- Универсальное решение строгой многофакторной аутентификации!

identrus COMPLIANT

❑ Решение обеспечивает выполнение трех наиболее важных требований:

- Реализацию разнообразных механизмов строгой многофакторной аутентификации;
- Контроль целостности транзакций;
- Ведение аудит-журналов для юридического подтверждения операций.

eema www.eema.org Award for Excellence

The Banker TECHNOLOGY AWARDS 2006 WINNER FRAUD PREVENTION PROJECT RETAIL BANKING

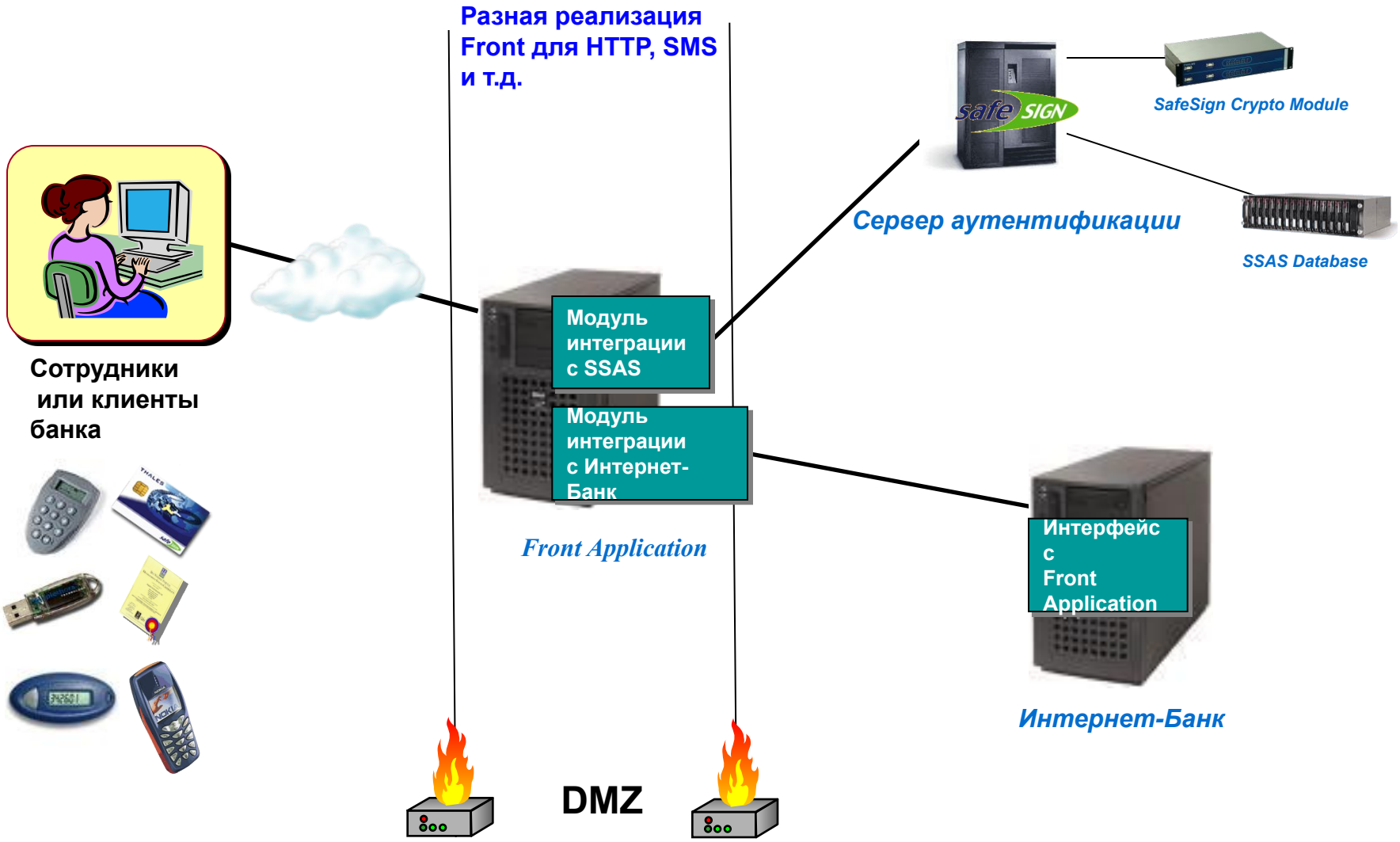
The Banker TECHNOLOGY AWARDS 2003

"Online Security solution of the year"

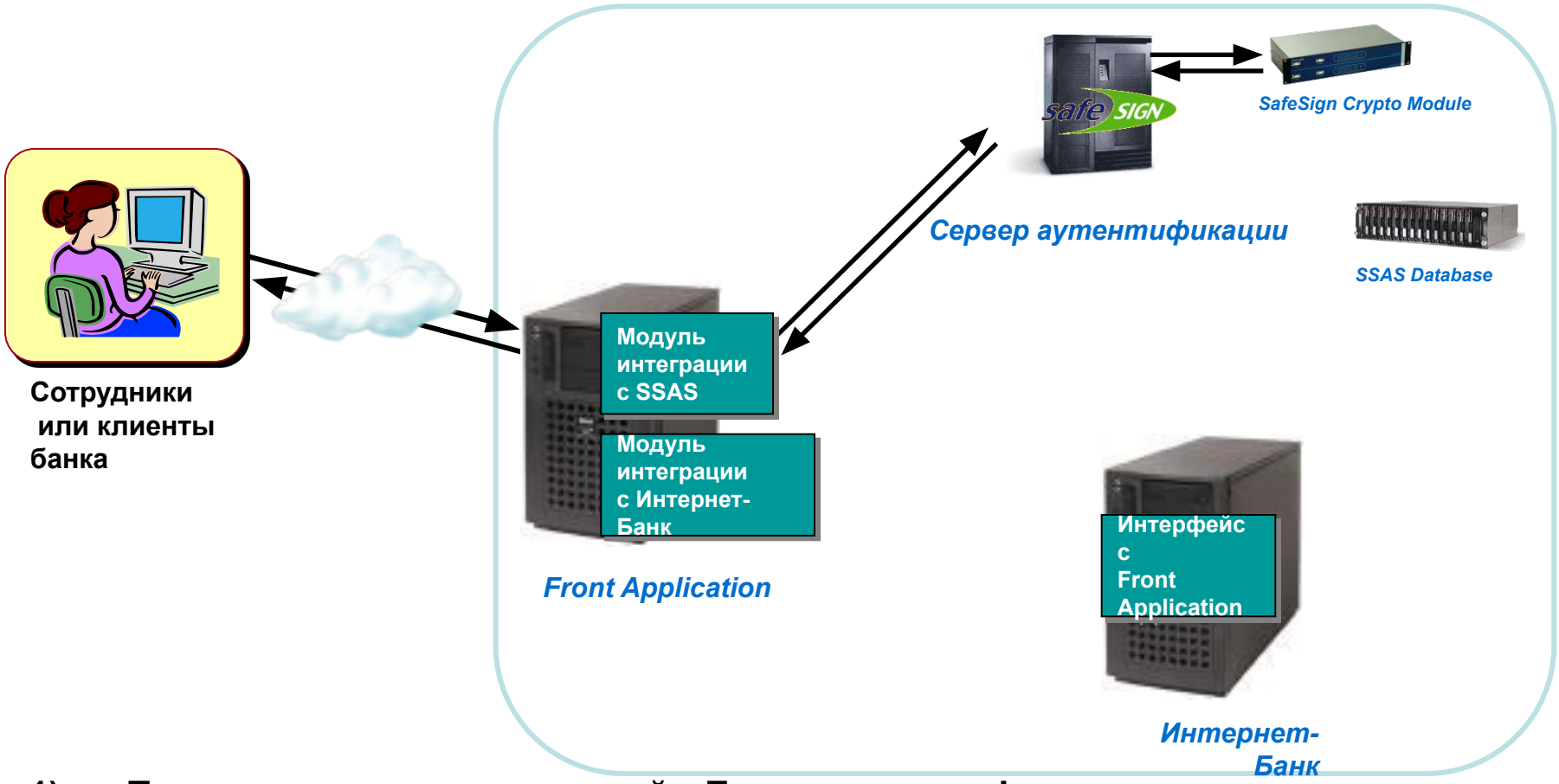
Awards FST Financial Sector Technology 2003

"Best use of B2B e-Commerce"

Архитектура решения

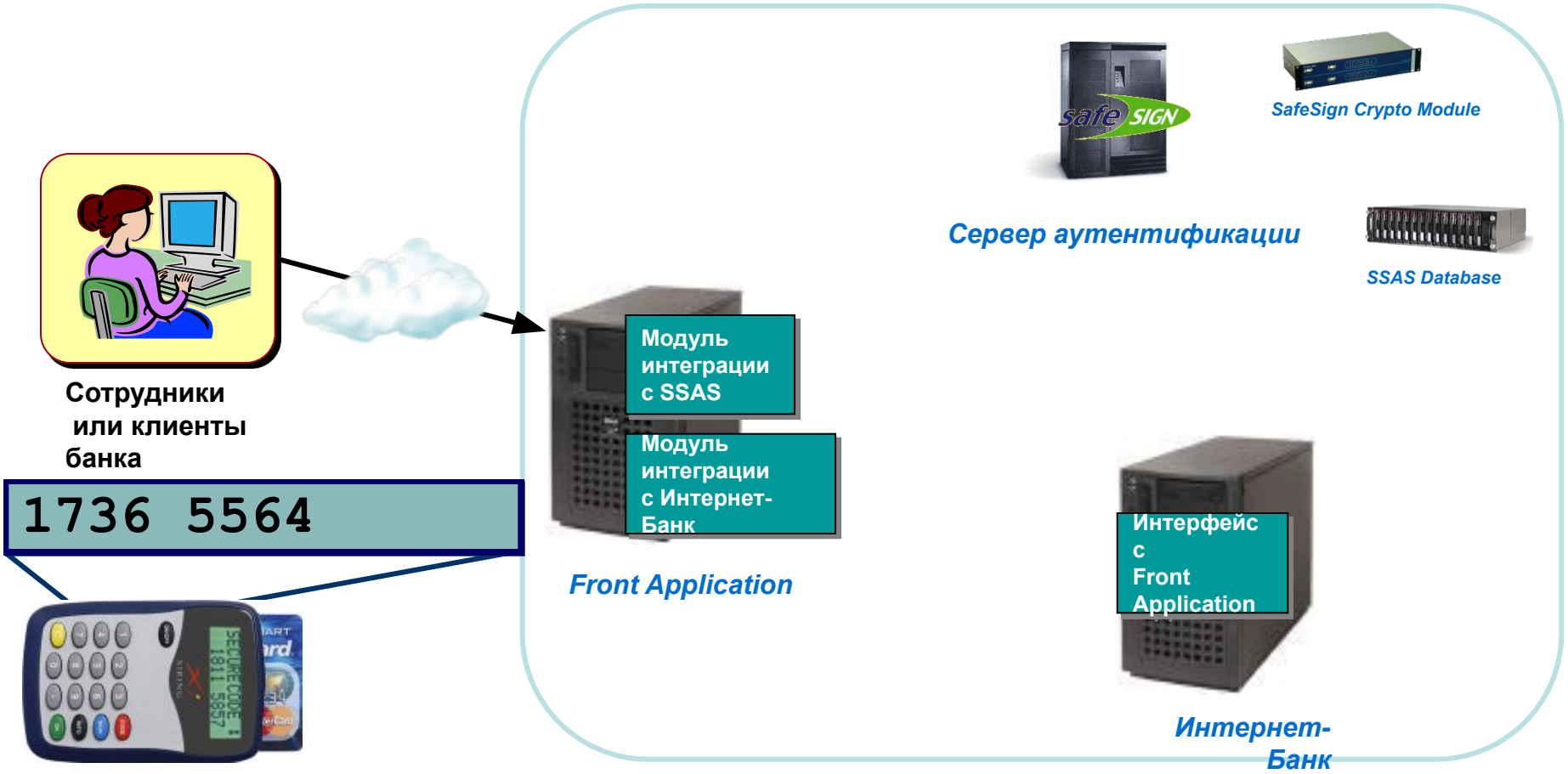


EMV-аутентификация (режим «Запрос-Ответ»)



1) Пользователь заходит на сайт. Еще не аутентифицирован
2) Сервер генерирует Запрос и сохраняет его в качестве сессионной информации
3) Сервер отправляет Запрос приложению

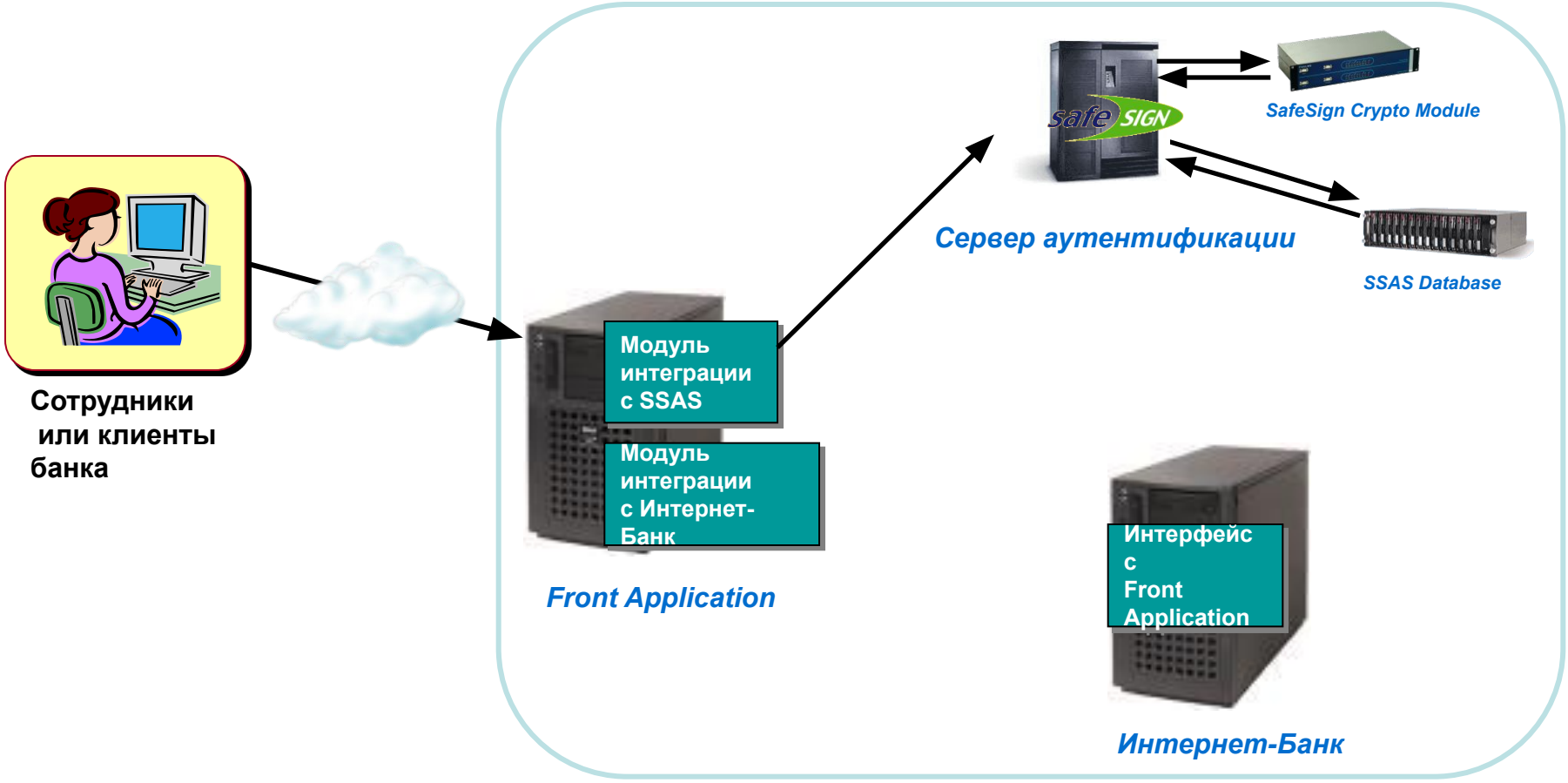
EMV-аутентификация (режим «Запрос-Ответ»)



4) Пользователь использует карточку и кардридер, чтобы получить Ответ

5) Вводит Логин и ответ на web-странице и отправляет на сервер

EMV-аутентификация (режим «Запрос-Ответ»)



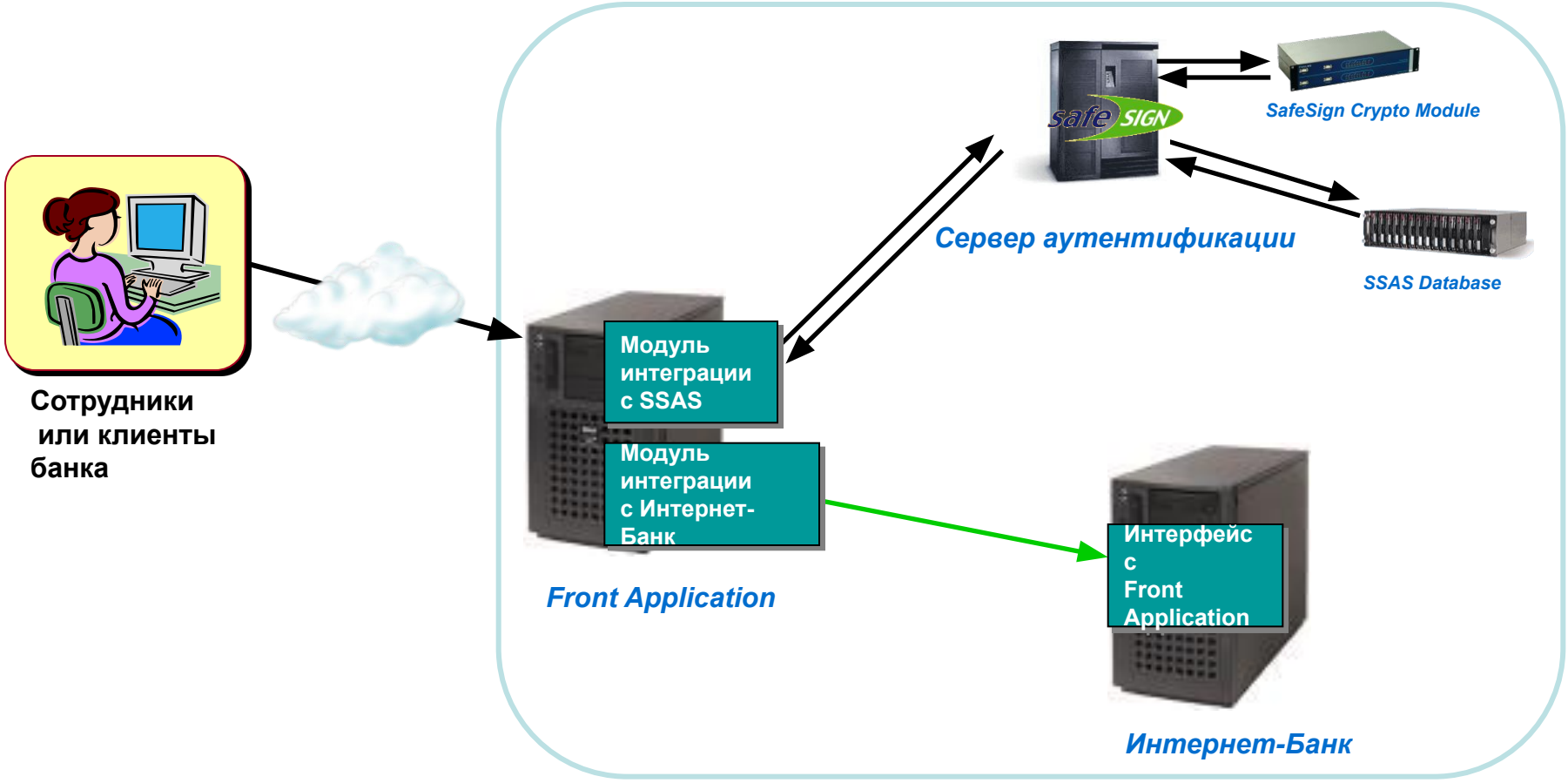
6) Логин, Запрос и Ответ посылаются на SSAS

7) SSAS проверяет параметры верификации для данного логина в базе данных

8) Если находит, то Запрос отправляется на SSCM

9) SSCM отвечает положительно или отрицательно на запрос аутентификации

EMV-аутентификация (режим «Запрос-Ответ»)



10) **Если ответ положительный, то пользователь получает доступ к своей странице в интернет-банке**

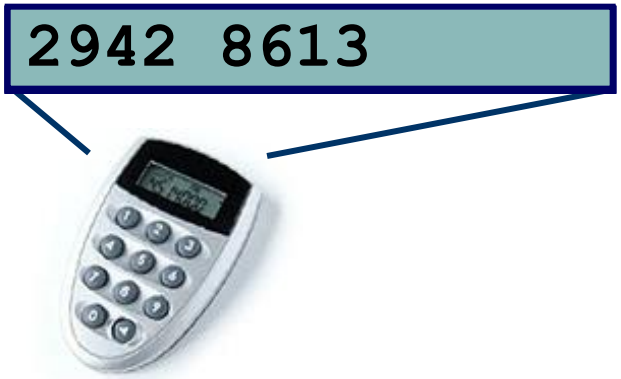
Подпись транзакции

Денежный перевод

Для перевода денег заполните форму. Все поля обязательны.

Схема аутентификации	**Vasco OTP**
Номер счета, на который должен быть выполнен перевод	9876 5432 1234
Сумма перевода	5000
Защитный код	2942 8613
	Выполнить перевод

Сервер аутентификации



1) **Вводятся данные транзакции на Web-странице**
2) **Пользователь использует токен для подписи транзакции. Вводится ПИН**
3) **Вводятся данные транзакции в токен**
4) **Токен вычисляет MAC по данным с использованием секретного ключа токена**
5) **MAC вводится на Web-странице**

Подпись транзакции

Денежный перевод

Для перевода денег заполните форму. Все поля обязательны.

Схема аутентификации	Vasco OTP
Номер счета, на который должен быть выполнен перевод	9876 5432 1234
Сумма перевода	5000
Защитный код	2942 8613
	Выполнить перевод

Сервер аутентификации

9876 5432 1234 5000 ….. 2942 8613

1234 5000

2942 8613 **?** **=** **2942 8613**

6) **Данные транзакции и MAC отправляются на сервер аутентификации**

7) **Сервер аутентификации заново вычисляет MAC по данным транзакции и сравнивает с полученным.**

Если они совпадут, то транзакция принимается

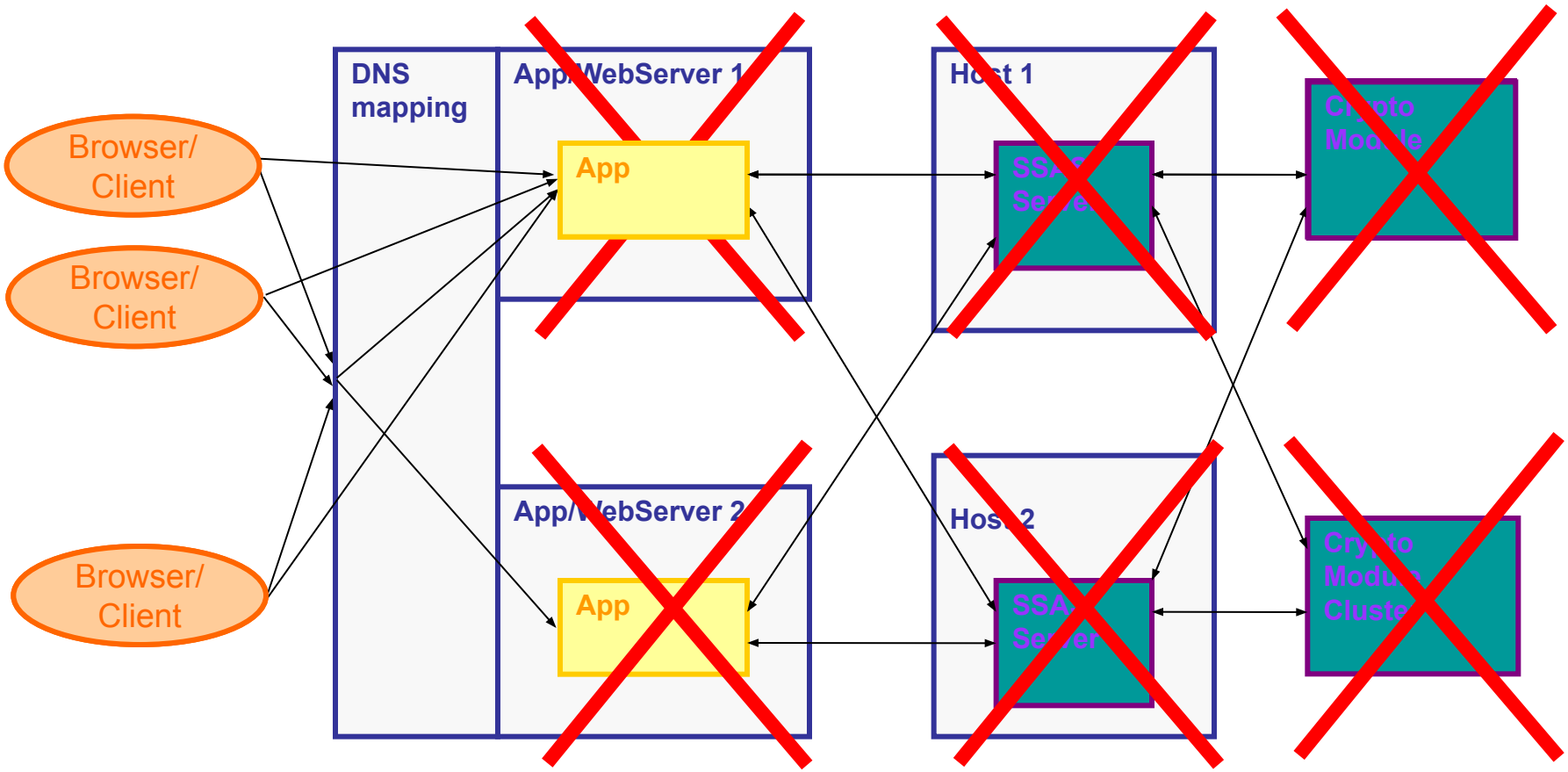
Аппаратная защищенность

Все криптографические преобразования и операции выполняются внутри аппаратного криптографического модуля HSM - SafeSign Crypto Module сертифицированного в соответствии с жесткими требованиями стандарта FIPS 140-2 Level 3;

- Безопасное хранение ключей и сертификатов;
- Защита аудит логов;
- Состоит из 2х модулей для отказоустойчивой кластеризации и балансировки нагрузки;

Отказоустойчивая кластеризация и балансировка нагрузки

- Нет единой точки отказа
- Прозрачно для приложений
- Статическая балансировка нагрузки
- Автоматическое опр. отказов



Свойства решения

- Представленное решение является универсальной единой платформой аутентификации в рамках всей интернет системы банка
- Соответствует настоящим и будущим потребностям в строгой многофакторной аутентификации
- Защита от мошенничества, в том числе со стороны сотрудников банка

Основные Преимущества

- Широкая гамма токенов и механизмов аутентификации
- Защищенный аудит-лог
- Высокая масштабируемость
- Отказоустойчивость и балансировка нагрузки
- Легкая интеграция с существующими и новыми системами
- Легкое управление
- Квалифицированная команда разработки и внедрения

Спасибо за внимание!

Вопросы??