

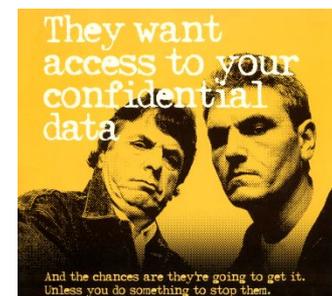
Аутентификационный центр -
решение для
интернет-банкинга



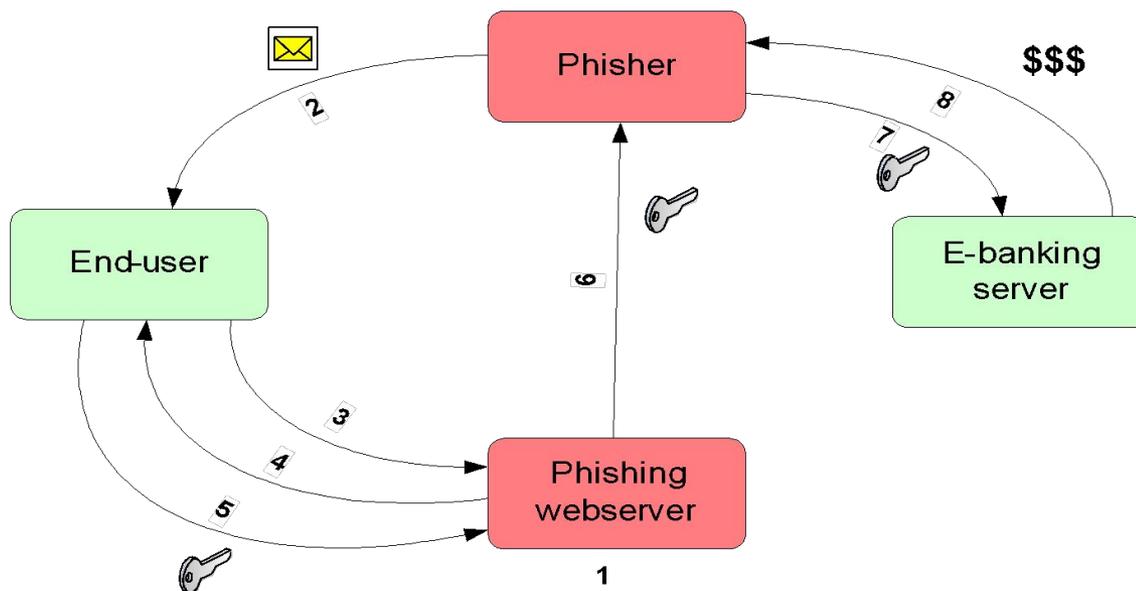
Чернышев Антон
anton@computel.ru

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

- 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 ...



- ❑ 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

FW: Citibank PIN Update Required - Message (HTML)

Fifth Third Bank informs you! - Message (HTML)

[PHISHING] - BB&T: account secure confirmation procedure - Message is a scam email phishing http...

Альфа-Клиент On-line - Message (HTML)

[PHISHING] - attention to all Bank of America clients. [Fri, 05 Jan 2007 09:48:43 -0800] - Message is a scam ...

From: Rivero, Konitzer
To: Konitzer
Cc:
Subject: FW: Citibank PIN Update Required

From: Fifth Third Bank
To: Atchernys
Cc:
Subject: Fifth Third Bank informs you!

From: Branch
To: atch
Cc:
Subject: [PHISHING] - BB&T: account secure confirmation procedure

From: ibank@alfabank.com
To: annalise58@...
Cc:
Subject: Альфа-Клиент On-line

From: Bank of America [operator-num92209136933ib@bankofamerica.com]
To: Anton
Cc:
Subject: [PHISHING] - attention to all Bank of America clients. [Fri, 05 Jan 2007 09:48:43 -0800] - Message is a scam email phishing [http://www...](http://www.bankofamerica.com/onlinebankingid742073411/session.cgi)

Sent: Пт 05.01.2007 20:49

Dear Fifth Third Bank customer,
Fifth Third Bank Protection Department requests you to start the client details confirmation procedure. By clicking on the link at the bottom of this letter you will get all necessary instructions how to start and complete the confirmation procedure. The following steps are to be taken by all customers of the Bank of America.

Dear Bank of America customer,
Bank of America Protection Department requests you to start the client details confirmation procedure. By clicking on the link at the bottom of this letter you will get all necessary instructions how to start and complete the confirmation procedure. The following steps are to be taken by all customers of the Bank of America.

Bank of America Department apologizes for the inconveniences caused to you, and is very grateful for your cooperation.

To start the confirmation procedure, click the following link:
<http://www.bankofamerica.com/onlinebankingid742073411/session.cgi>

Bank of America, N.A. Member FDIC. Equal Housing Lender.
© 2006 Bank of America Corporation. All rights reserved.

Генеральная Альфа-Банк (С) 2001-2006

Copyright © 2006 Bank of America Corporation. All rights reserved.

Copyright © 2006 Bank of America Corporation. All rights reserved.

Строгая Аутентификация пользователей

Действительно ли перед нами тот кто мы думаем?

Проверка целостности транзакций

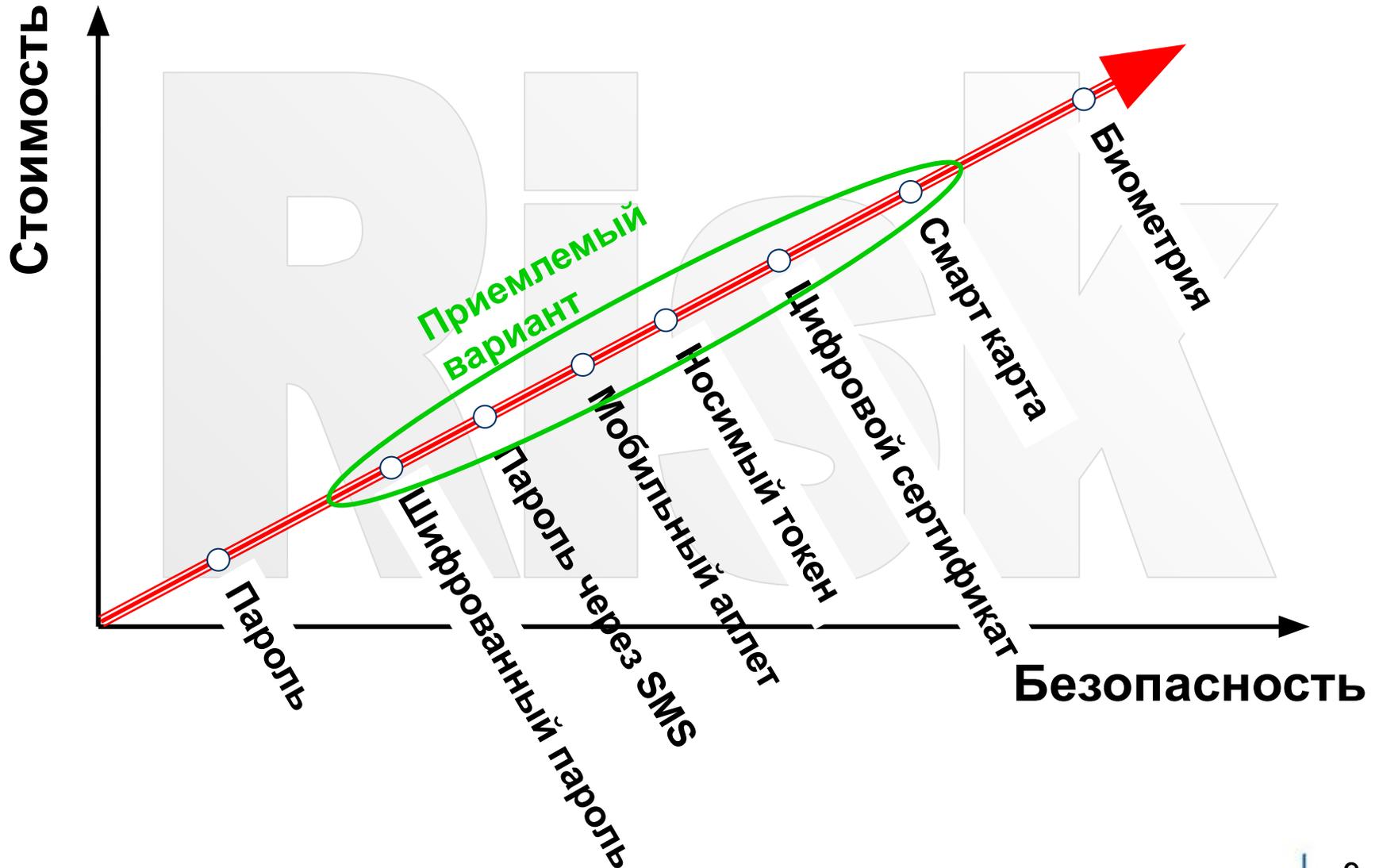
Соответствует ли пришедшая транзакция запрошенной клиентом?

Аудит операций

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

- 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







- Универсальное решение строгой многофакторной аутентификации!



□ Решение обеспечивает выполнение трех наиболее важных требований:

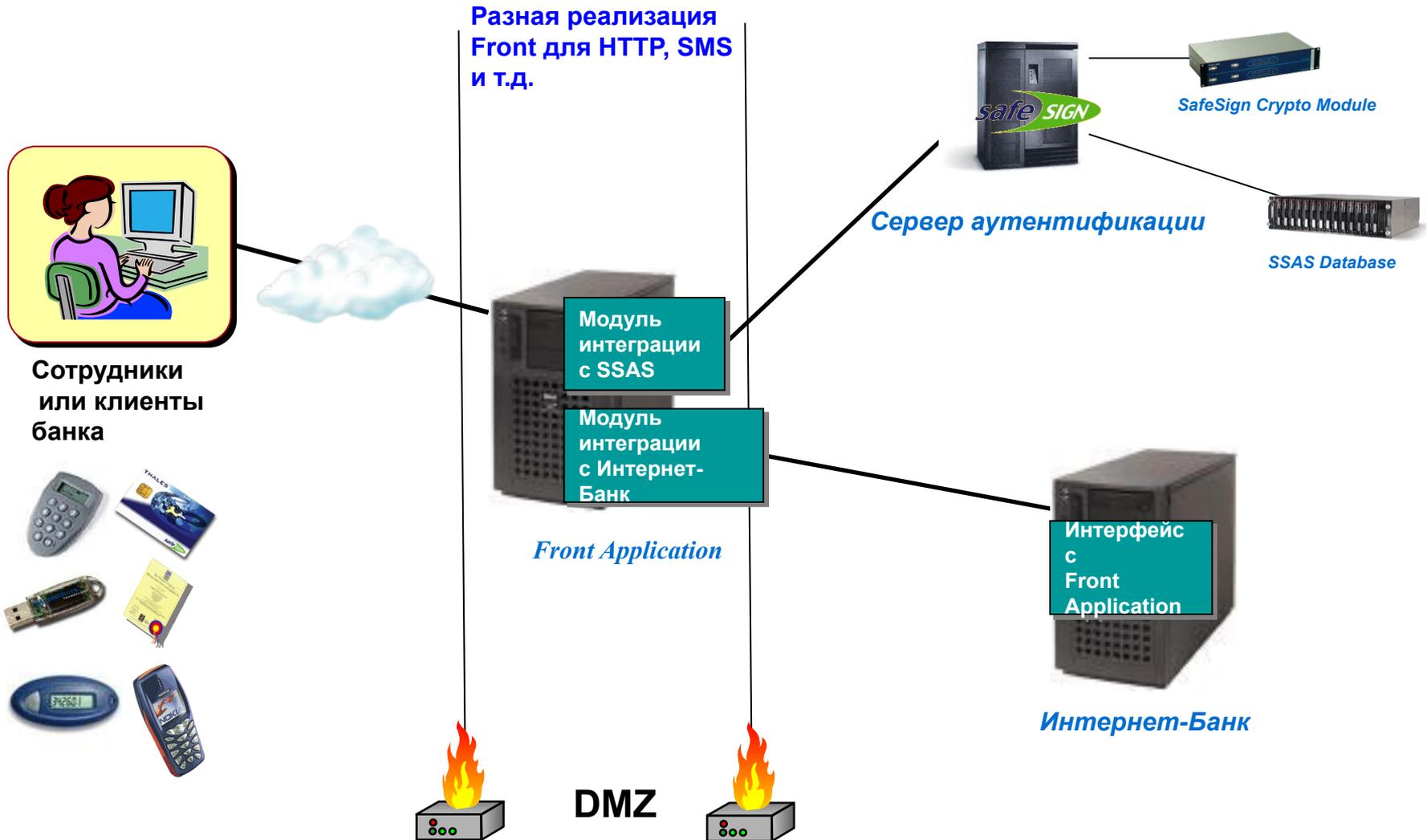
- Реализацию разнообразных механизмов строгой многофакторной аутентификации;
- Контроль целостности транзакций;
- Ведение аудит-журналов для юридического подтверждения операций.

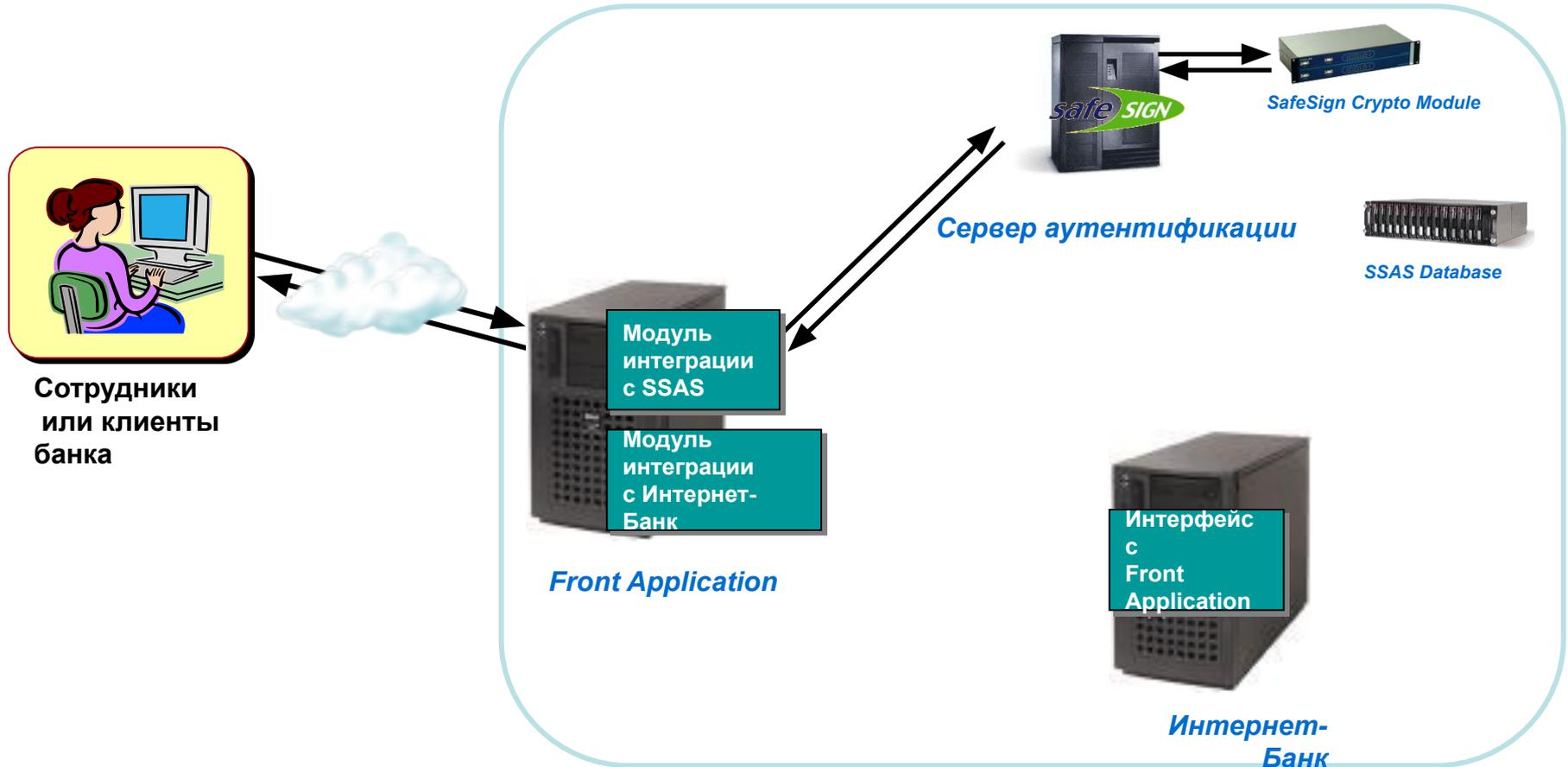


“Online Security solution of the year”



“Best use of B2B e-Commerce”





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



Сотрудники
или клиенты
банка



Front Application



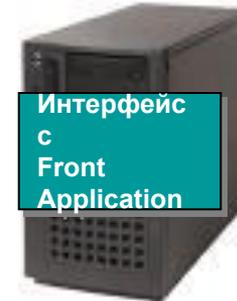
Сервер аутентификации



SafeSign Crypto Module



SSAS Database

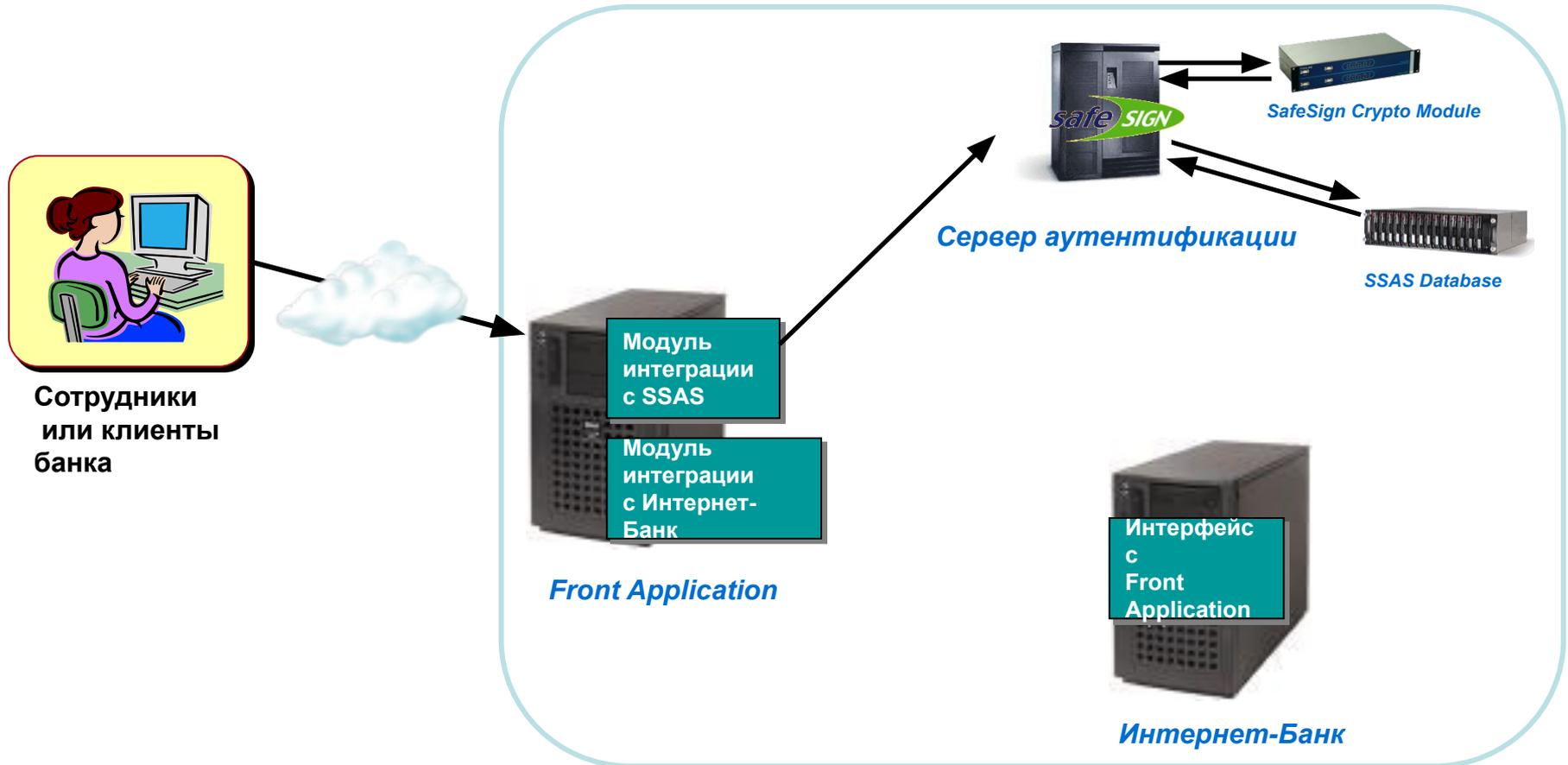


Интернет-Банк

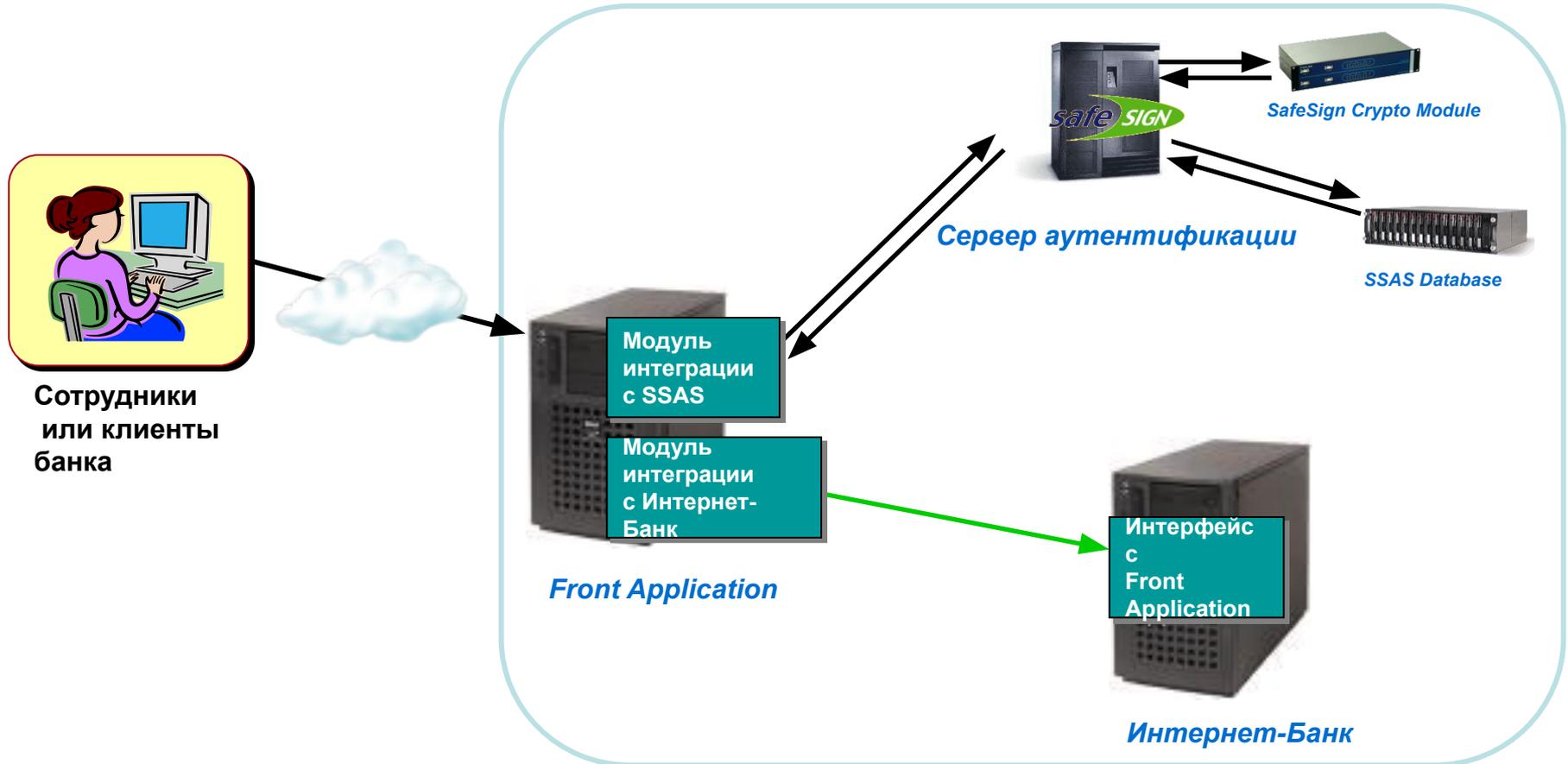
1736 5564



- 4) Пользователь использует карточку и кардридер, чтобы получить Ответ
- 5) Вводит Логин и ответ на web-странице и отправляет на сервер



- 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**



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



Денежный перевод

Для перевода денег заполните форму. Все поля обязательны.

Схема аутентификации	Vasco OTP
Номер счета, на который должен быть выполнен перевод	<input type="text" value="9876 5432 1234"/>
Сумма перевода	<input type="text" value="5000"/>
Защитный код	<input type="text" value="2942 8613"/>
<input type="button" value="Выполнить перевод"/>	



Сервер аутентификации

2942 8613



- 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



Денежный перевод

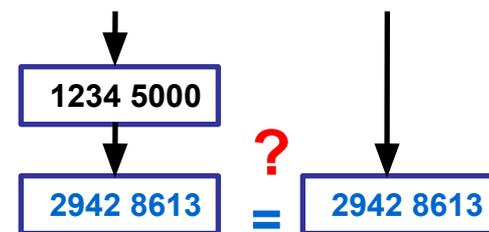
Для перевода денег заполните форму. Все поля обязательны.

Схема аутентификации	Vasco OTP
Номер счета, на который должен быть выполнен перевод	<input type="text" value="9876 5432 1234"/>
Сумма перевода	<input type="text" value="5000"/>
Защитный код	<input type="text" value="2942 8613"/>
<input type="button" value="Выполнить перевод"/>	



Сервер аутентификации

9876 5432 1234 5000 2942 8613



- 6) Данные транзакции и MAC отправляются на сервер аутентификации
- 7) Сервер аутентификации заново вычисляет MAC по данным транзакции и сравнивает с полученным.

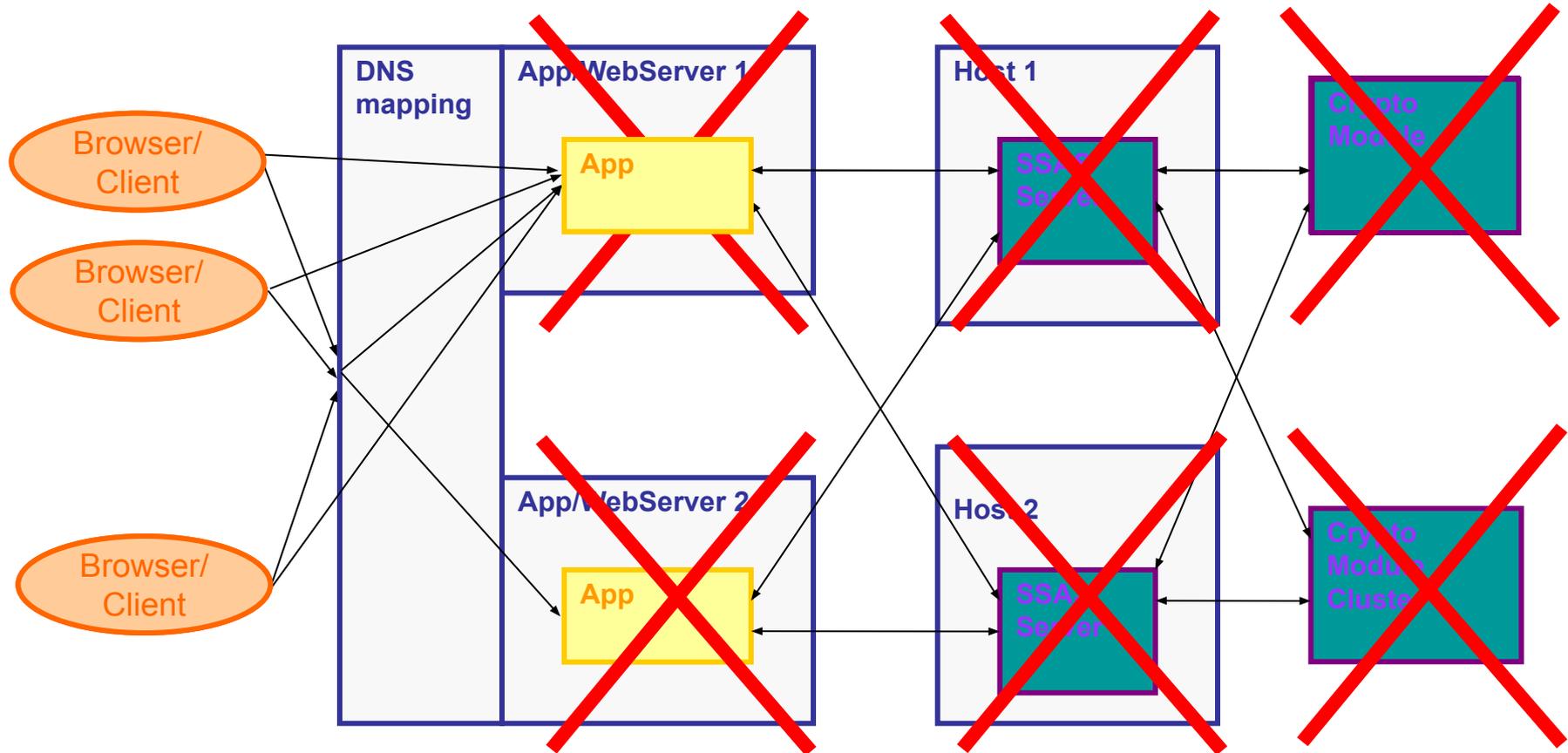
Если они совпадут, то транзакция принимается

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;

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



- ❑ 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??

