Анатомия интернет-банка

Российские интернет-технологии

2010

Артем Вольфтруб

www.gramant.ru

О чем этот доклад?

Интернет-банк

Процессинг

Безопасность

Оплата услуг

Рост числа пользователей* интернет-банков за 2009 год

Райффайзенбанк	+ 27,3%	30%
ВТБ24	+ 100%	
Промсвязьбанк	+ 350%	50%
Банк 24.ру круглосуточный банк для деловых людей	+ 150%	

*Среди физических лиц

Причины роста популярности ДБО

- Рост числа пользователей интернета в России
- Улучшение качества связи
- Рост доверия к услугам электронной коммерции
- Увеличение числа услуг
- Снижение комиссий

Доля коробочных продуктов

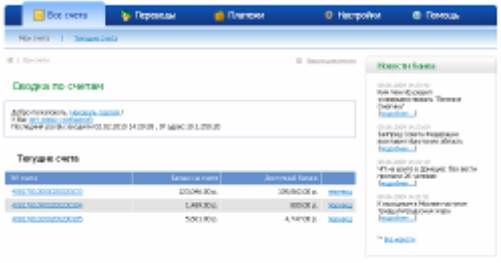
Источник: CNews Analytics, 2009

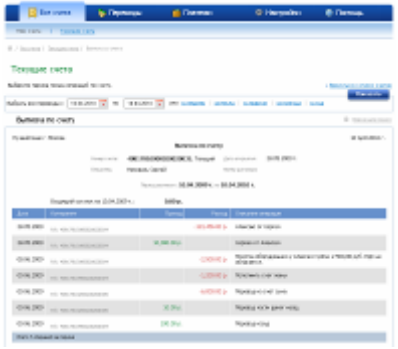
Базовые функции Интернет Банка

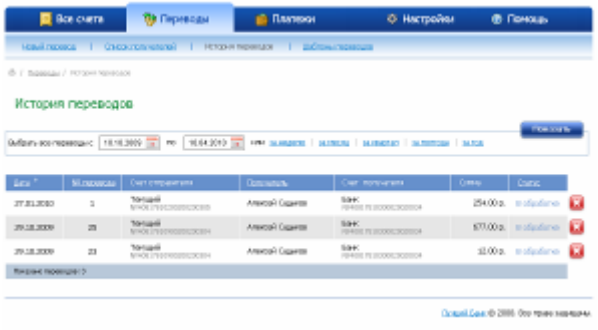
- Баланс счетов
- История операций
- Перевод денег
- Оплата услуг

А сколько это экранов?

Российские интернет-технологии 2010





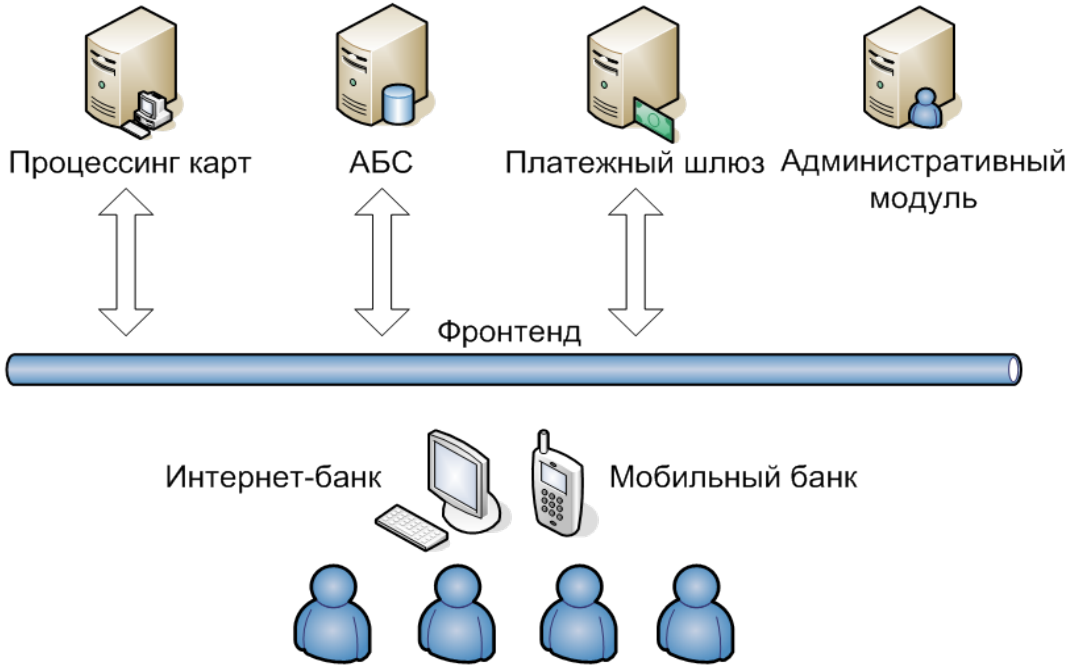


?

Аргументы в пользу собственной разработки

- Высокая стоимость внедрения и поддержки готовых систем
- Специфичная инфраструктура банков
- Наличие собственных ИТ специалистов, готовых сделать систему под конкретного заказчика, но за меньшие деньги

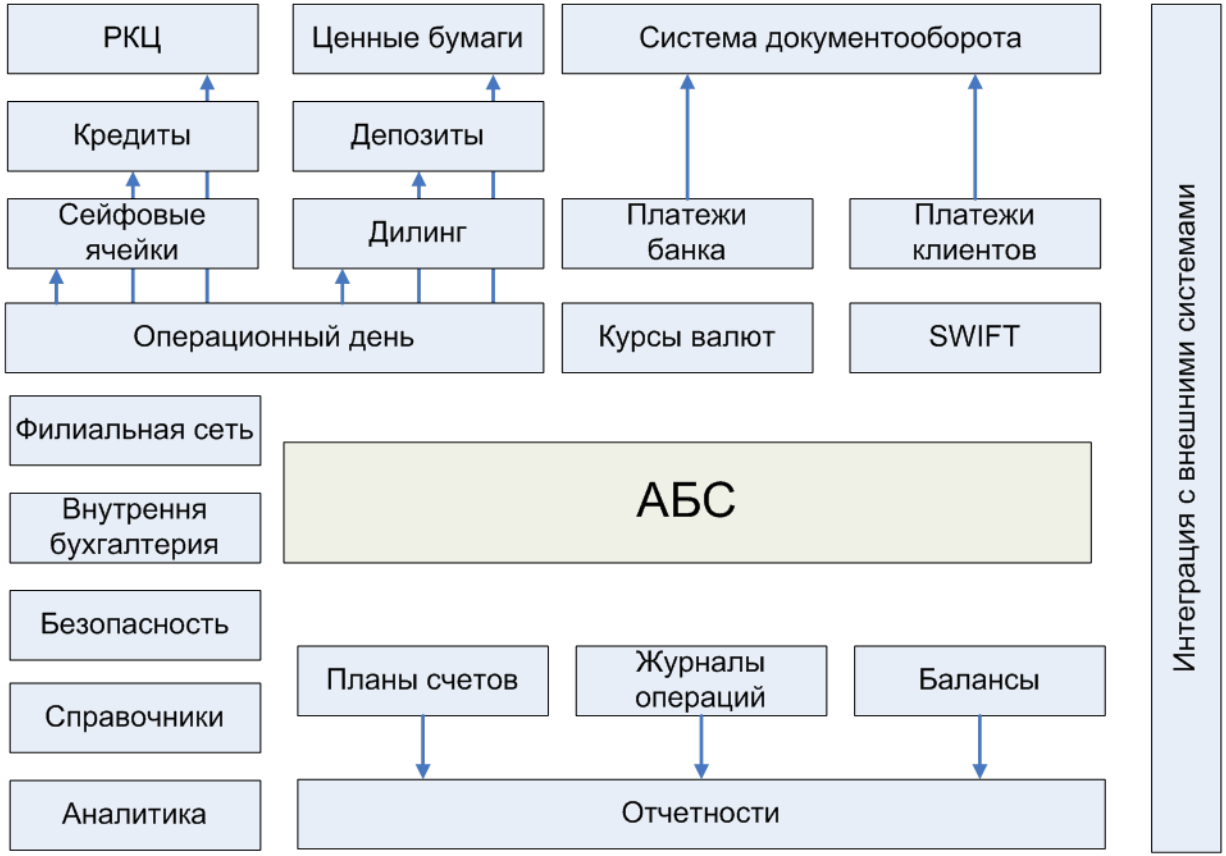
Основные компоненты ИБ



АБС

АБС – основная составляющая программной инфраструктуры банка

- Учетные функции
- Документооборот
- Аналитика


РКЦ
Ценные бумаги
Система документооборота
Кредиты
Депозиты
Сейфовые ячейки
Дилинг
Платежи банка
Платежи клиентов
Операционный день
Курсы валют
SWIFT
Филиальная сеть
Внутрення бухгалтерия
АБС
Безопасность
Справочники
Планы счетов
Журналы операций
Балансы
Аналитика
Отчетности
Интеграция с внешними системами

Варианты интеграции с АБС

- Прямая взаимодействие через СУБД
- Шлюз обмена файлами
- Web-сервисы

Сложности интеграции

- АБС – продукт, не предназначенный для интеграции с внешними системами
  - Старый legacy код
  - Несколько банков – несколько АБС
  - Один банк – несколько АБС

Где хранить данные ИБ?

- Информация о пользователях
- Создаваемые документы
- Явки, пароли

Данные внутри АБС

- Упрощается инфраструктура
- Нет дублирования
- Усложняется реализация
- Появляется зависимость от АБС
- Возрастает нагрузка
- Снижается безопасность

Данные во внешнем хранилище

- Снижается нагрузка на АБС
- Проще в реализации
- Нет зависимости от АБС
- Улучшается безопасность
- Сложный механизм синхронизации данных
- Задержки в обновлении

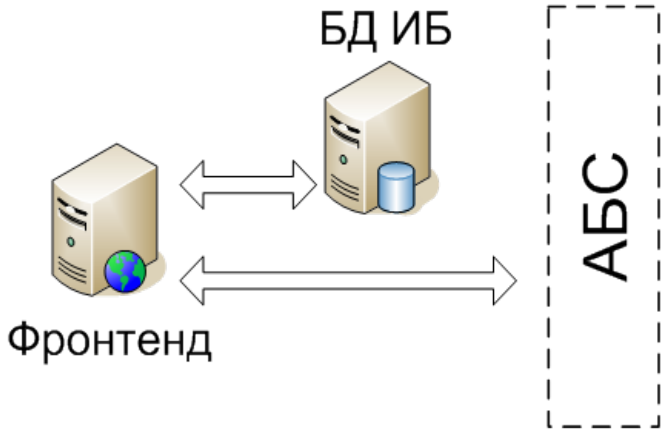
Гибридный вариант

Информация в БД

- Клиенты
- Справочники

Информация в АБС

- Счета
- История операций



Безопасность

Три парадигмы обеспечения безопасности

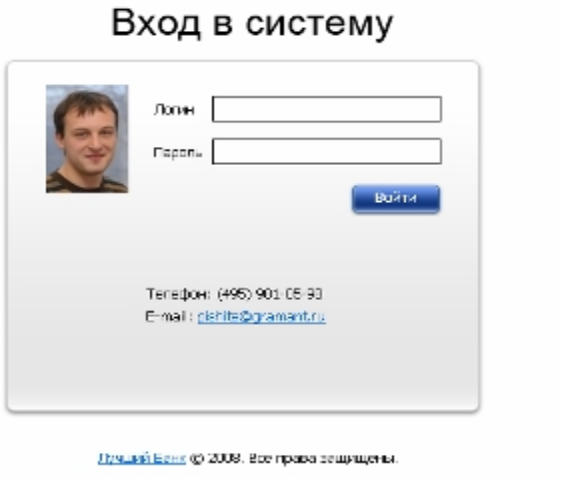
- Something you know
- Something you have
- Something you are

Something you know

- Самый распространенный метод аутентификации
- Не создает лишних проблем пользователю
- Самый ненадежный метод
  - Простой пароль – проще запомнить, проще подобрать
  - Легко украсть (кейлоггер, фишинг, скрытое наблюдение)
- Смена пароль требует участия пользователя

Something you know

Виртуальная клавиатура для защиты от кейлоггера. Кнопки располагаются случайным образом



Персонализированная форма логина для защиты от фишинга

Something you have

- Смарт-карта
- One-Time Password
  - Скетч-карта
  - SMS
  - Генератор паролей (токен)

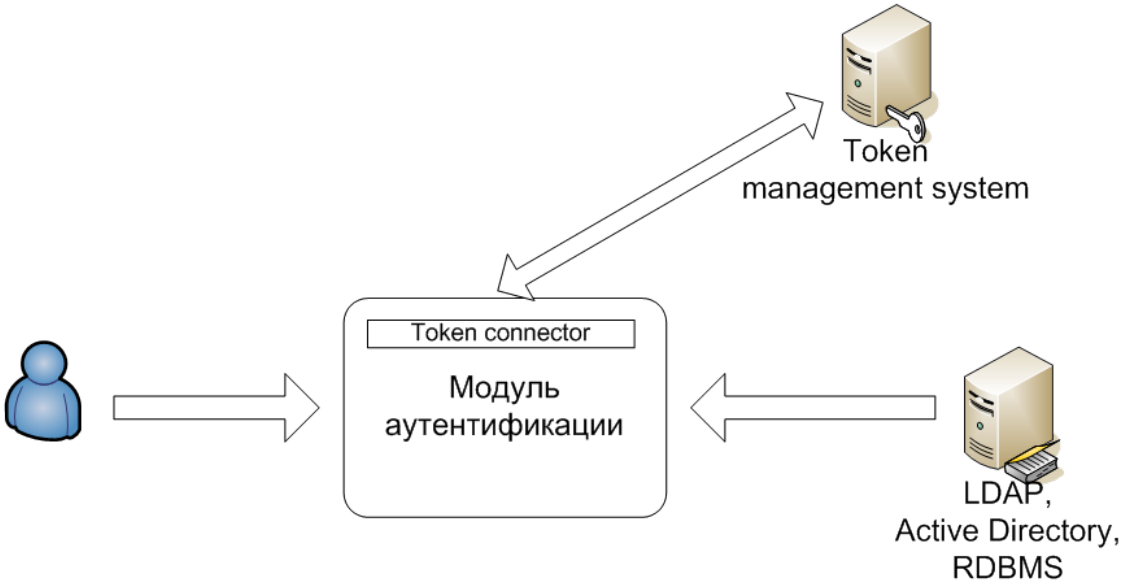
Аутентификация с помощью токена

- Может дополнять аутентификацю паролем
- Основана на принципе OTP
- Независимый модуль

Принцип работы токена

- Пароль = F(секретный ключ, значение счетчика)
- Счетчик устройства и счетчик сервера должны быть синхронизированы
- PIN код для дополнительной защиты

Аутентификация с помощью токена



Something you are

- Все свое ношу с собой
- «Пароль» не может устареть

- Существенно увеличивает стоимость
- Люди боятся машин
- Вероятность ошибочного срабатывания (FAR и FRR)

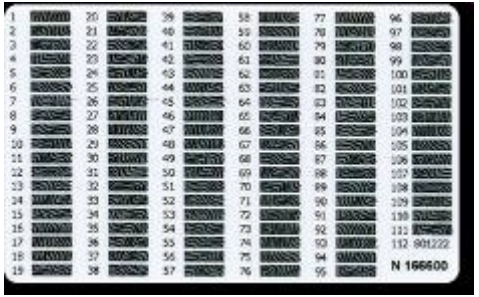
Разделение по уровню операций

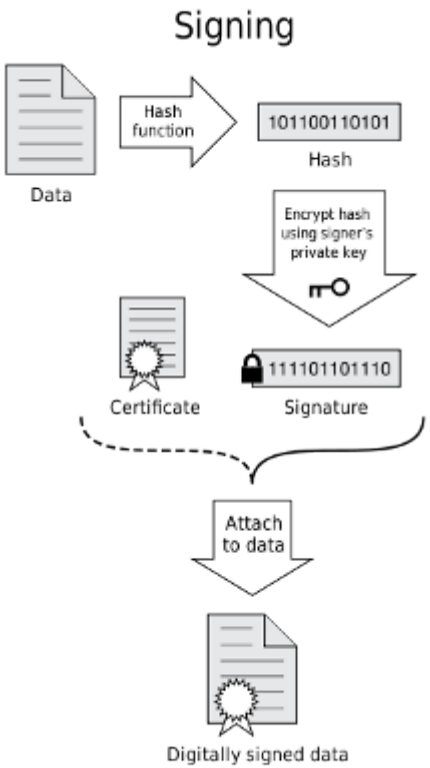
- Активные операции
- Пассивные операции

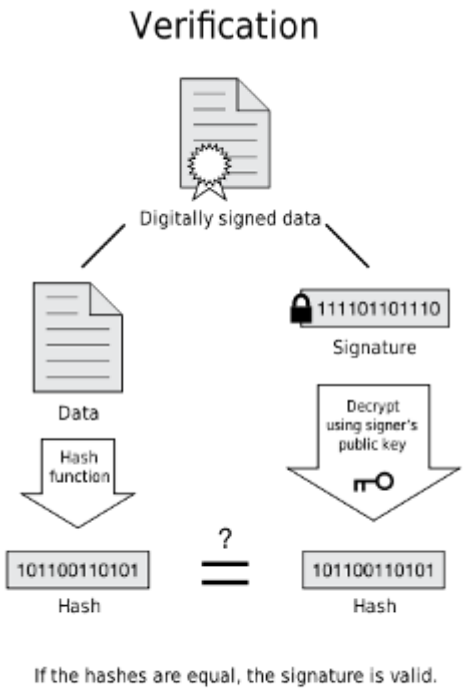
- Экономит время пользователя
- Упрощает реализацию

Защита активных операций

- Скетч-карты
- ЭЦП




Signing
Hash function
101100110101
Hash
Data
Encrypt hash using signer's private key
Certificate
111101101110
Signature
Attach to data
Digitally signed data

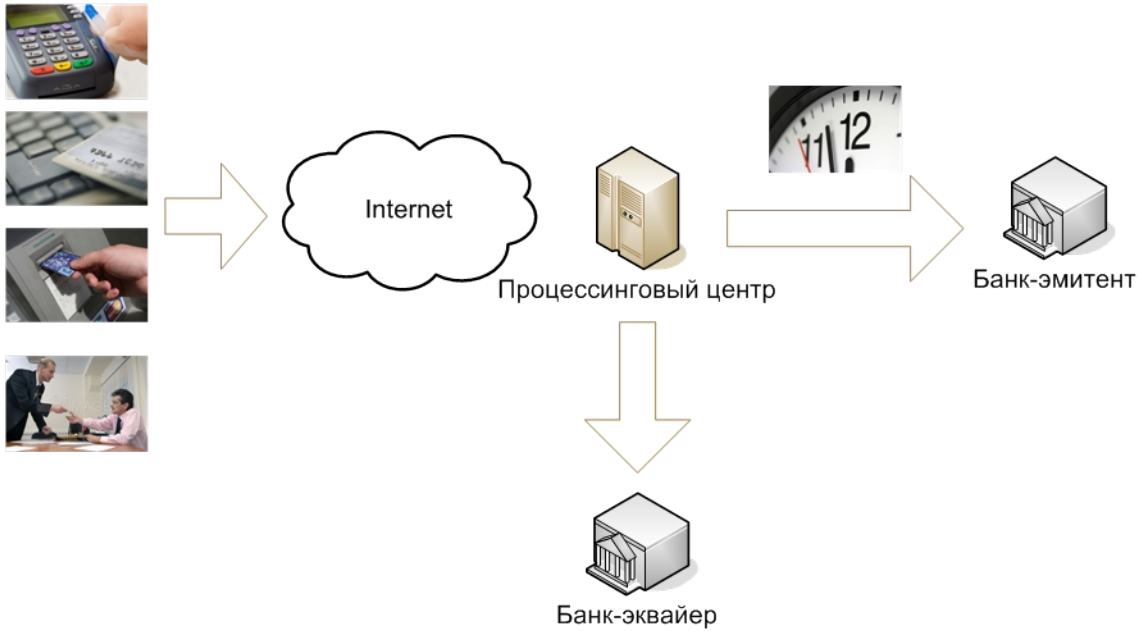

Verification
Digitally signed data
111101101110
Signature
Data
Decrypt using signer's public key
Hash function
?
101100110101
Hash
101100110101
Hash
If the hashes are equal, the signature is valid.

Защиты операций с помощью ЭЦП

- Высокий уровень безопасности
- Идентификация пользователя, подписавшего сообщение
- Передача данных по открытым каналам

Процессинг банковских карт

Базовая схема работы



Важные моменты

- Любая транзакция идет через процессинговый центр
- Обмен данными между процессинговым центром и банком-эмитентом может происходить в офлайне

Магнитные карты

- Дешевы в производстве
- Широко распространены
- Невысокая защита
- Ограниченные возможности
- Требуют соединения с ПЦ

Смарт-карты

- Улучшенная защита
- Не требуют соединения с ПЦ
- Широкие функциональные возможности
- Дороже в изготовлении
- В некоторых местах не работают

Работа в офлайне

- Баланс записывается на карту
- Транзакции сохраняются на карте
- Синхронизация при наличии соединения

Как не уйти в overdraft?

- Лимиты на общую сумму операций
- Лимиты на число операций
- Overdraft – проблема клиента

Обработка карт в интернет-банке

- Информация о картах хранится в карточной системе
- Синхронизация остатков с процессинговым центром
- Внешний шлюз (обмен файлами, веб-сервисы)
- Объединение информации, получаемой от АБС (счета) и ПЦ (остатки, журнал транзакций)

Оплата услуг

Зачем нужна оплата услуг в ИБ

Для пользователя

- Экономия времени
- Сниженный размер комиссий
- Возможность использовать средства на банковском счете

Зачем нужна оплата услуг в ИБ

Для банка

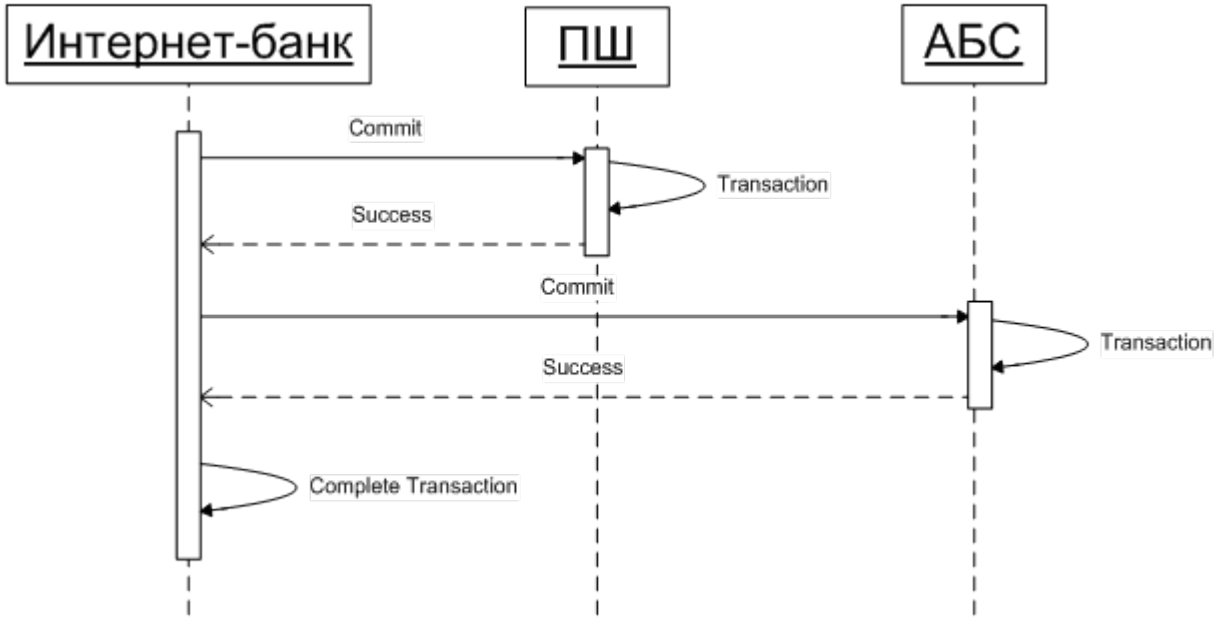
- Средство повышения лояльности клиентов
- Увеличение денежного оборота
- Возможность заработать на трафике


Платежный шлюз
АБС
Интернет-банк
Процессинговый центр

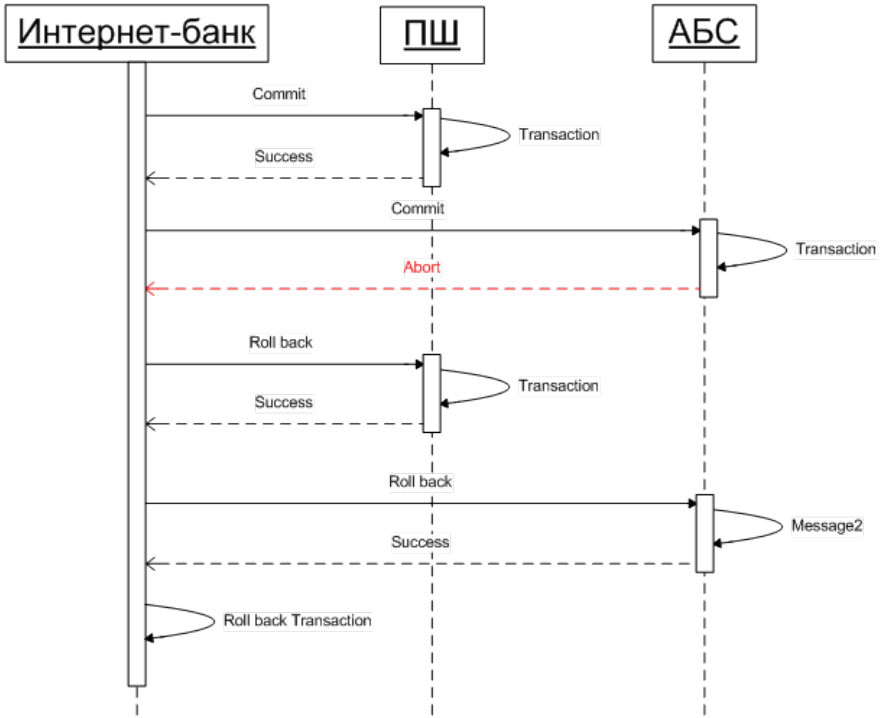
Особенности реализации

- Взаимодействие с разнородными системами в рамках единой транзакции
- Разный механизм работы в зависимости от источника
- Разные типы банковских документов для услуг
- Нельзя использовать универсальные формы для оплаты

Протокол двухфазного коммита



Протокол двухфазного коммита



Практика

- Блокирующий протокол
- Не работает при выходе из строя координатора

Иногда приходится работать руками

Административный интерфейс

- Максимальная независимость от основной системы
- Работа с платежными документами, восстановление документов
- Аудит данных и операций
- Управление пользователями
- Основной инструмент службы поддержки

Подводя некоторые итоги

- Функциональность ИБ не заканчивается фронтендом
- Не существует универсальной архитектуры
- Безопасность можно улучшать бесконечно
- Разнородные системы никогда не работают без сбоев
- Не нужно забывать о тех, кто будет эксплуатировать систему

Вопросы?

artem@gramant.ru

Бонус-трек

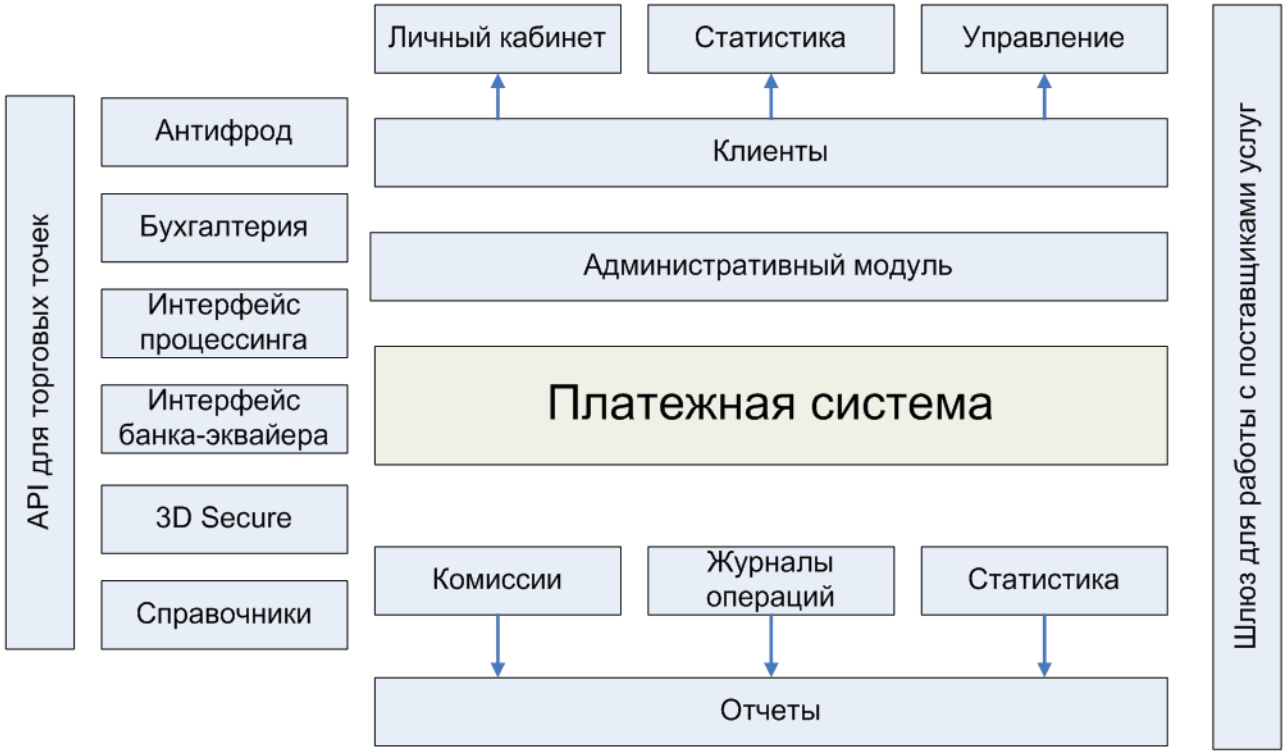
Немного о платежных системах

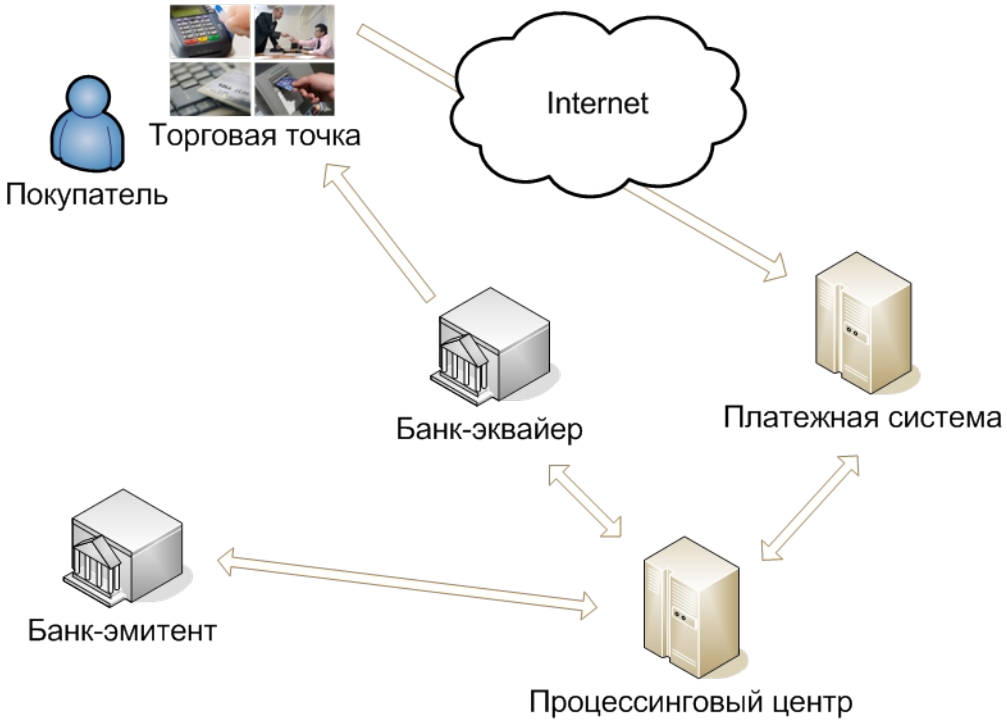
Зачем нужна платежная система

- Решение для малого бизнеса
- Сеть поставщиков услуг
- Разнообразные формы оплаты
- Реализованные механизмы безопасности

Функции платежной системы

- Гарантия безопасности
- Учет торговых точек
- Подключение поставщиков

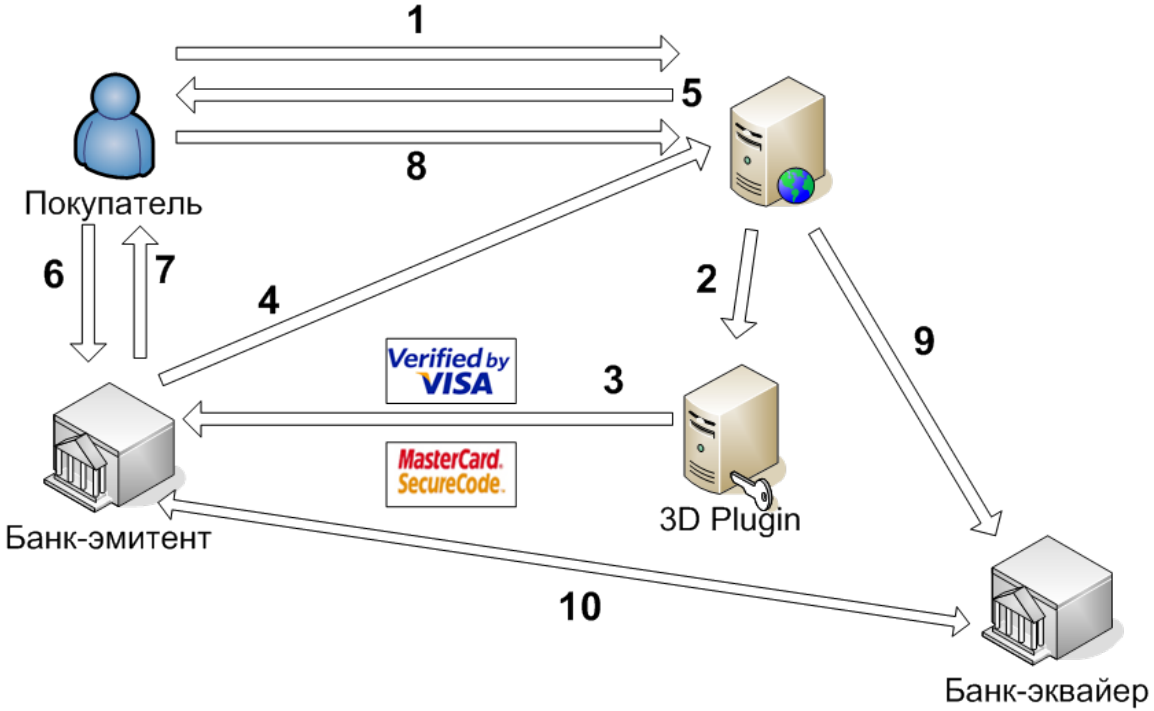

Личный кабинет
Статистика
Управление
API для торговых точек
Антифрод
Клиенты
Бухгалтерия
Административный модуль
Интерфейс процессинга
Платежная система
Интерфейс банка-эквайера
3D Secure
Комиссии
Журналы операций
Статистика
Справочники
Отчеты
Шлюз для работы с поставщиками услуг


Internet
Торговая точка
Покупатель
Банк-эквайер
Платежная система
Банк-эмитент
Процессинговый центр

Взаимодействие с ПС

- Использование встроенных модулей оплаты
- API
- Веб-сервисы

Дополнительные средства защиты



Вопросы?

artem@gramant.ru