聚合支付平台介绍

Tim

大纲(上)

- 聚合支付平台介绍
  - 业务背景及系统功能介绍
  - 支付接口对接时序介绍
  - 聚合支付系统架构及技术栈介绍

- 无spring实现
  - http服务
  - DB 操作
  - 其他组件集成

大纲(下)

- 支付接口对接技术点
  - 加签 / 验签
  - JAVA Base64/MD5/RSA 加解密&数字签名实战

- 后台管理系统概览
  - 数据库设计概览
  - 业务功能概览
  - Vue介绍
  - 前后端full stack概览

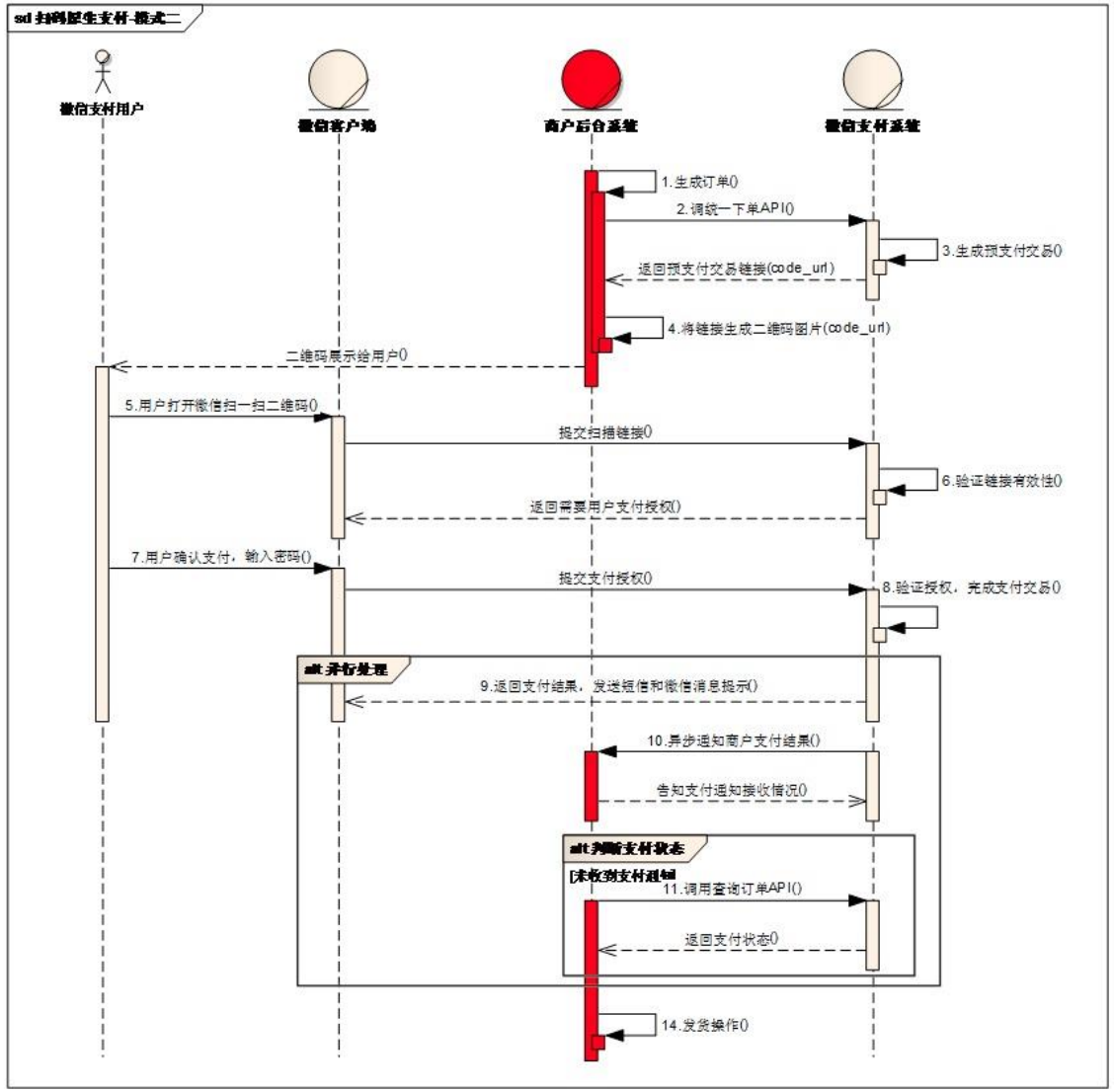
Web页面支付流程


您的订单 请记住您的付费账户是微信登录的，其他登录平台不能共享付费信息。
2小时 会员
价格：1元 数量：1
一次最多只能购买3份
总金额：1元
支付方式：
支付宝 ALIPAY
微信支付
上一步
提交订单


扫一扫付款（元）
1.00
扫一扫
打开手机支付宝
扫一扫继续付款
首次使用请下载手机支付宝
< 登录账户付款


付费注意事项
请在付费完成前不要关闭此窗口。
请在付费完成后，根据付费结果选择下面的按钮。
付费失败
付费成功
您的订单
2小时 会员
价格：1元 数量：1
总金额：1元
支付方式
支付宝
上一步
确认支付

微信 二维码支付时序图


sd 扫码原生支付-模式二
微信支付用户
微信客户端
商户后台系统
微信支付系统
1.生成订单()
2.调统一下单API()
3.生成预支付交易()
返回预支付交易链接(code_url)
4.将链接生成二维码图片(code_url)
二维码展示给用户()
5.用户打开微信扫一扫二维码()
提交扫描链接()
6.验证链接有效性()
返回需要用户支付授权()
7.用户确认支付，输入密码()
提交支付授权()
8.验证授权，完成支付交易()
alt 异常处理
9.返回支付结果，发送短信和微信消息提示()
10.异步通知商户支付结果()
告知支付通知接收情况()
alt 判断支付状态
[未收到支付通知]
11.调用查询订单API()
返回支付状态()
14.发货操作()

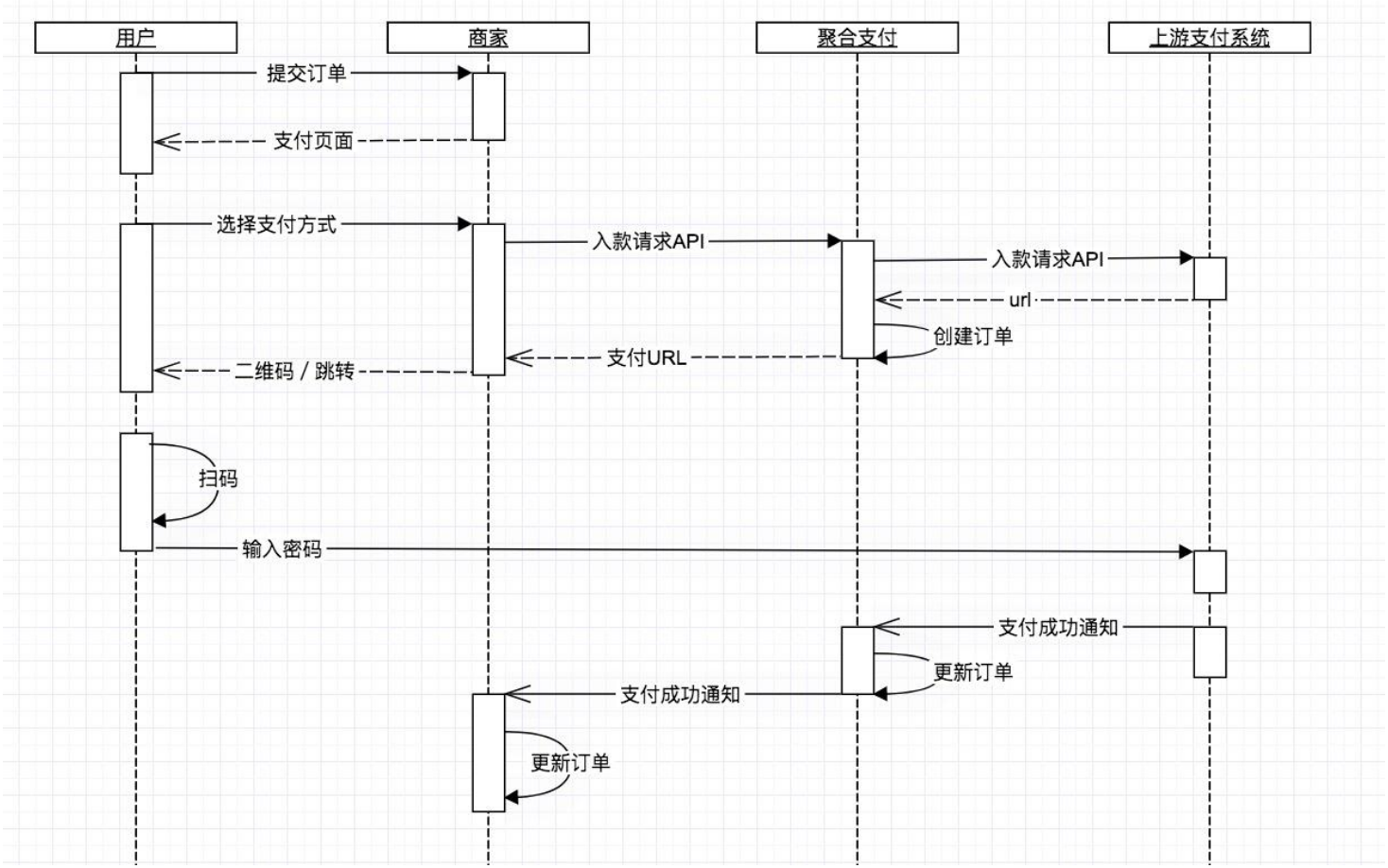
背景基础介绍

- 支付系统基本角色
  - 商户
  - 支付接口
  - 支付渠道
  - 清结算系统

- 支付对接流程
  - 商务对接
  - 技术对接
  - 测试&上限
  - 对账&提现 / 下发

- 聚合支付系统的特点
  - 为什么需要聚合支付?
  - 如何盈利?

支付流程时序图


用户
商家
聚合支付
上游支付系统
提交订单
支付页面
选择支付方式
入款请求API
入款请求API
url
创建订单
支付URL
二维码 / 跳转
扫码
输入密码
支付成功通知
更新订单
支付成功通知
更新订单

一个聚合支付平台的基本需求

- 支付相关:
  - 支付API（出 / 入 款，查询， 异步支付回调通知）
  - 对接不同的支付通道（支付方式）
  - 订单系统 扣费系统
- 管理系统:
  - 商户账户管理
  - 渠道管理
  - 订单管理
  - 对账
  - 权限
  - 其他（权限，结算，统计..）

聚合支付系统架构介绍

- 架构介绍
- 技术栈:
  - JAVA8
  - Node.js
  - Vue
  - Mysql

- 为什么去spring化?
  - Spring 悖论?
  - 面临的挑战?

第二部分 无spring实现

Simple HTTP API Endpoint

- 为什么这个业务场景只需要简单的http服务:
  - 对B端系统用户
  - 使用签名技术而非普通session认证
  - 接口变化非常缓慢
  - 基本无复杂前端相关业务

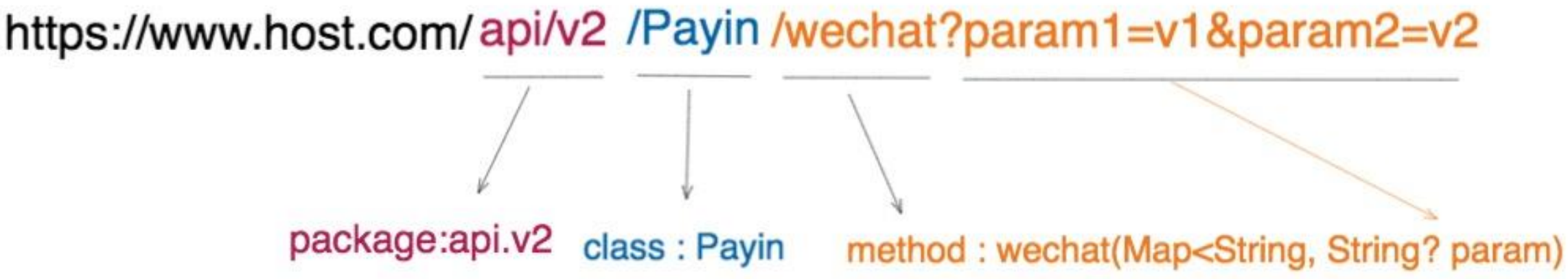
- 我们需要的是:
  - HTTP 协议服务器
  - HTTP 请求分发器
  - 支持不同HTTP 响应
  - 提供业务代码框架
  - Cookie 及其他http常用方法

Simple HTTP API Endpoint

- NanoHttpd
- Beetle

Request dispatcher

- url -> method
- convention over configuration
- Reflections : 基于反射实现



Mybaties 集成

- 编程方式获取SqlSessionFactory
- 提供事务管理及封装模版代码
- 挑战：事务嵌套?

其他技术点

- 系统初始化
- 队列
- 模版
- 一些业务细节的实现

第三部分 支付接口对接

对接接口一览

- https://pay.weixin.qq.com/wiki/doc/api/native.php?chapter=9_1
- https://opendocs.alipay.com/apis/api_1/alipay.trade.page.pay/
- 共性:
  - 商户号 / 账号
  - 订单信息
  - 金额
  - 回调地址
  - 签名类型&签名

支付接口的安全相关技术

- 签名与加密的区别?
- 支付接口常见签名 / 加密相关用语:
  - Base64
  - MD5
  - SHA1, SHA256
  - RSA
  - AES/DES

消息摘要（MD5, SHA1, SHA256）

- 作用：验证原消息是否有改变
- 优点：简单，摘要长度固定
- 缺点：攻击者可猜测使用的摘要算法进行撞库攻击
  - 所以业界一般都需要加盐（salt）

数字签名（SHAWithRSA/MD5WithRSA）

- 数字签名=消息摘要+非对称加密
- 生成公钥 / 私钥
- PKCS1 & PKCS8 区别
- RSA1(SHA1WithRSA) & RSA2(SHA256WithRSA)
- RSA encrypt/decrypt & RSA sign/verify sign

后台管理功能介绍

- 基本功能介绍
- 数据库表设计
- Vue 基础介绍

支付路由模块介绍

- 渠道账户池
- 硬性条件规则
- 排序&权重
- 规则冲突后的“保底”池

总结 & 提问