



QCon 全球软件开发大会
INTERNATIONAL SOFTWARE
DEVELOPMENT CONFERENCE

BEIJING 2017

淘宝开放平台网关技术解密

顾风胜

目录

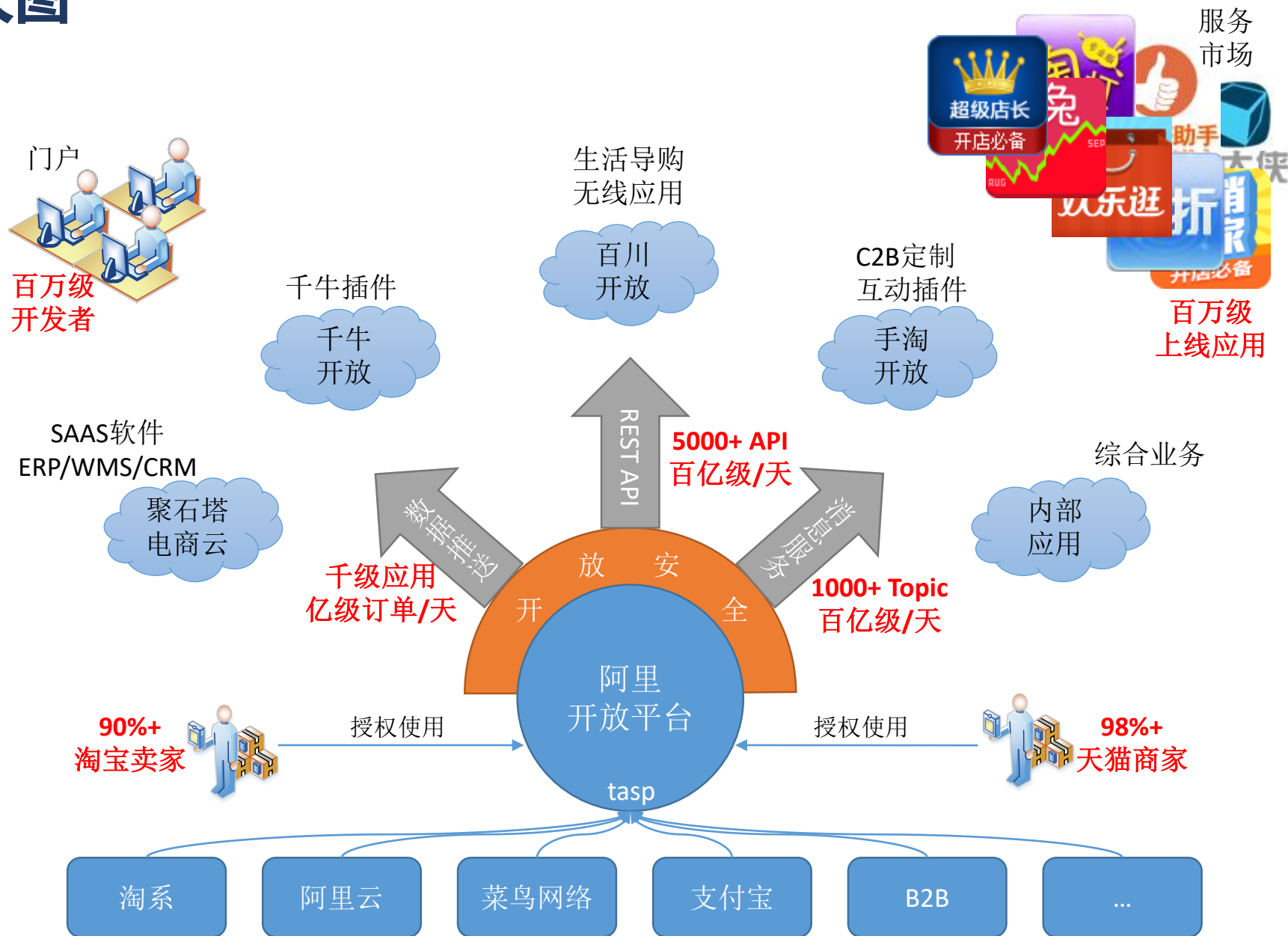
- 01 | 开放平台概览
- 02 | API网关介绍
- 03 | API接入自动化
- 04 | 开放平台工厂
- 05 | 开放平台安全

01

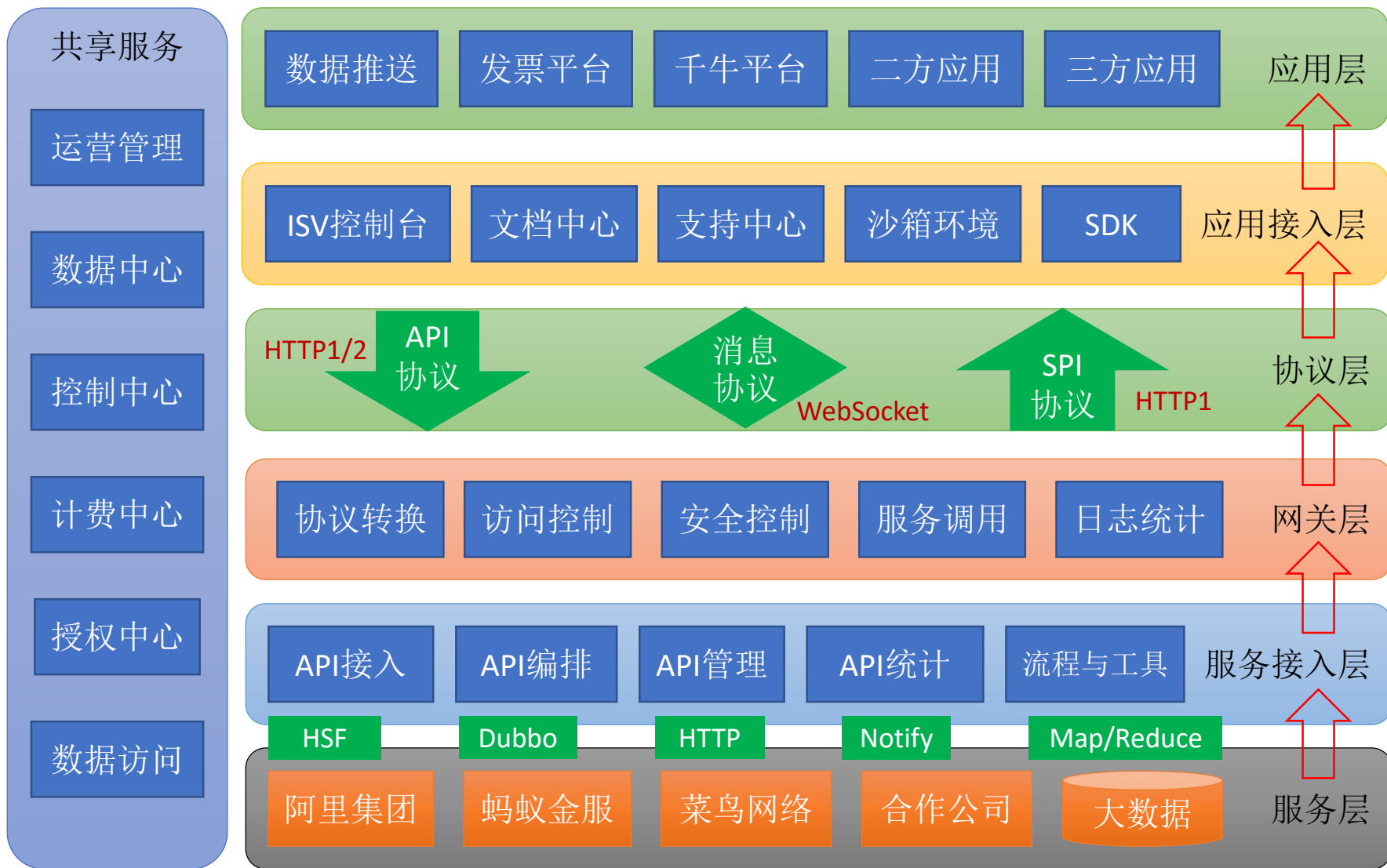
第一部分

开放平台概览

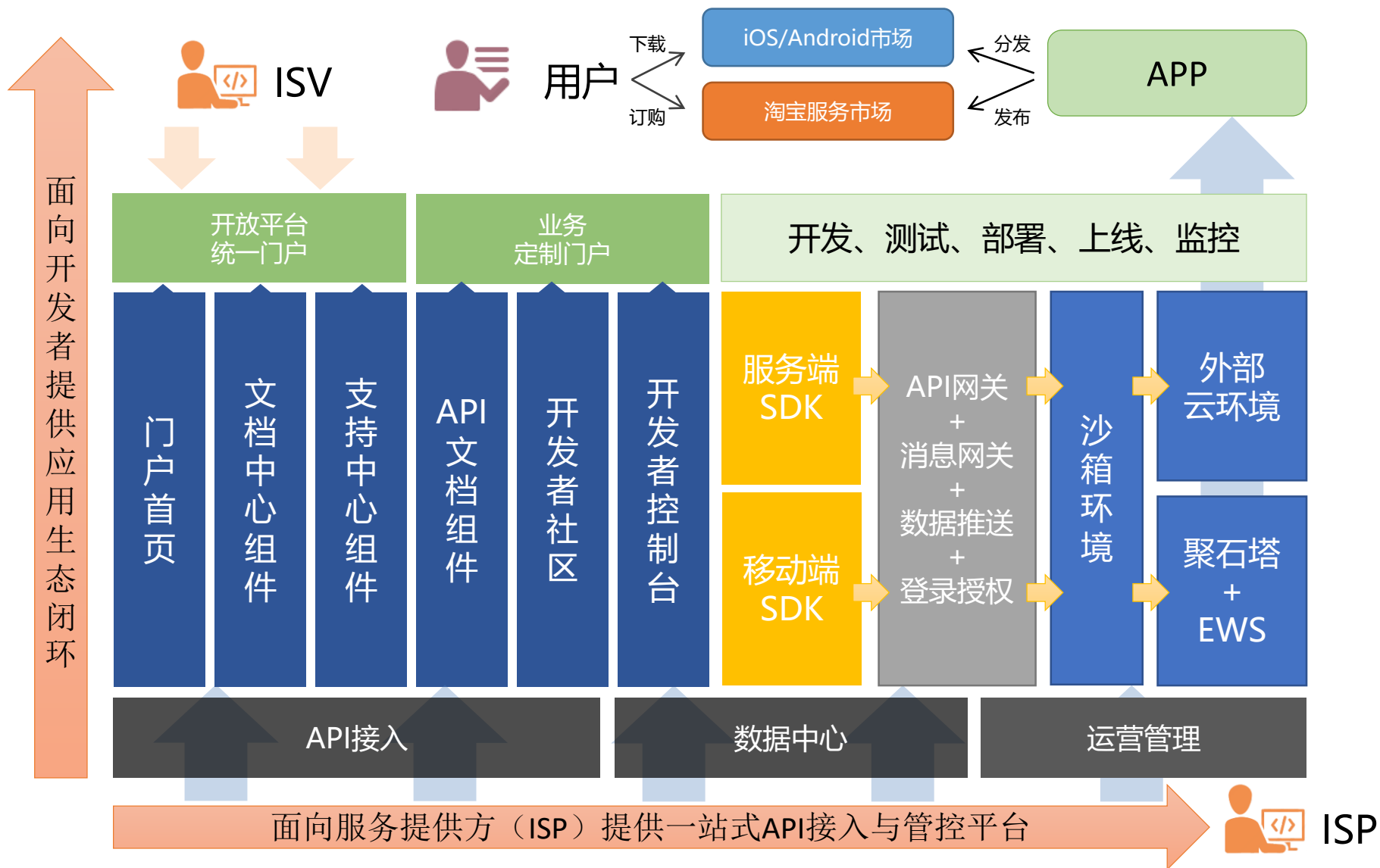
开放平台大图



开放平台技术架构



开放平台产品架构



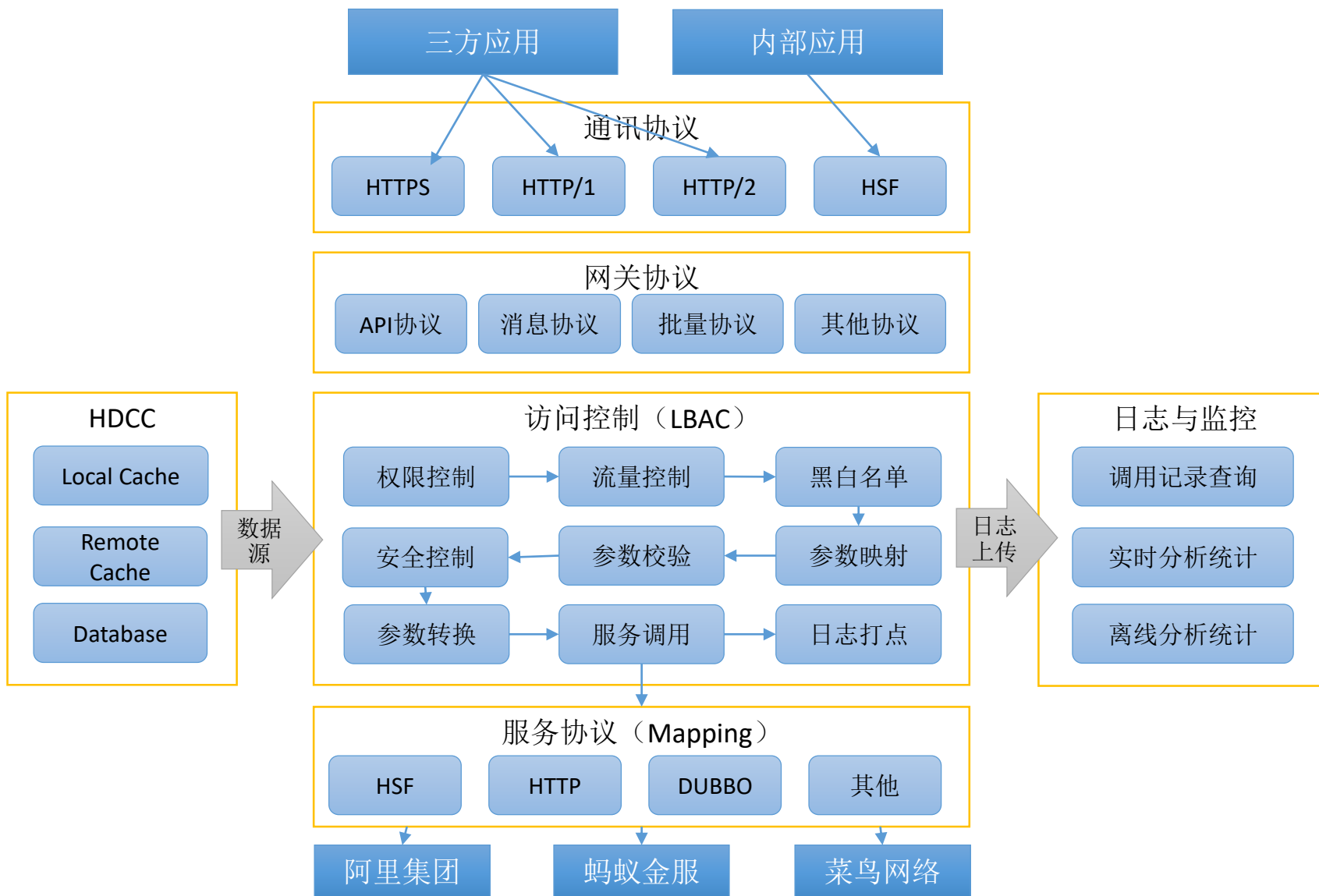
02

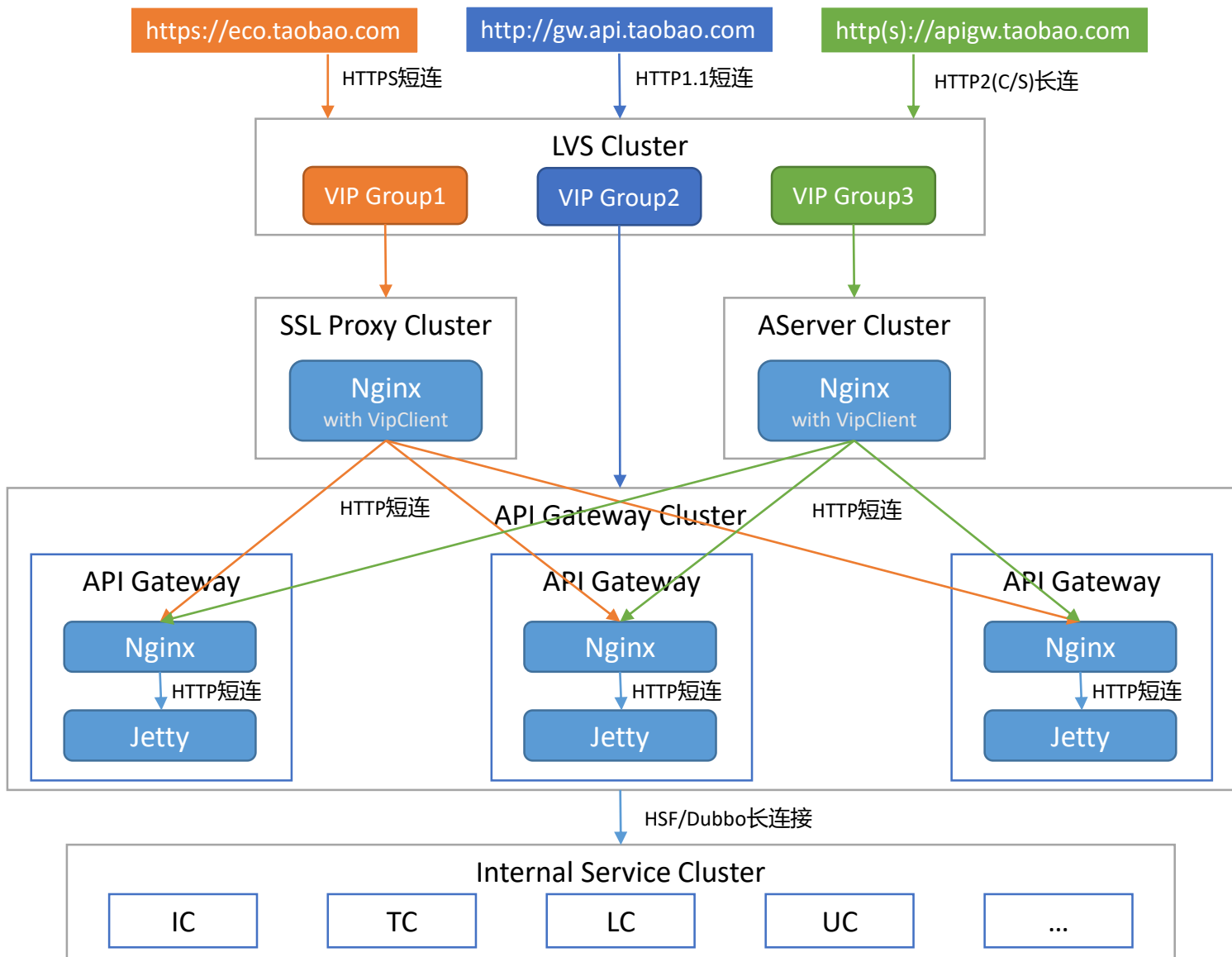
第二部分

API网关介绍

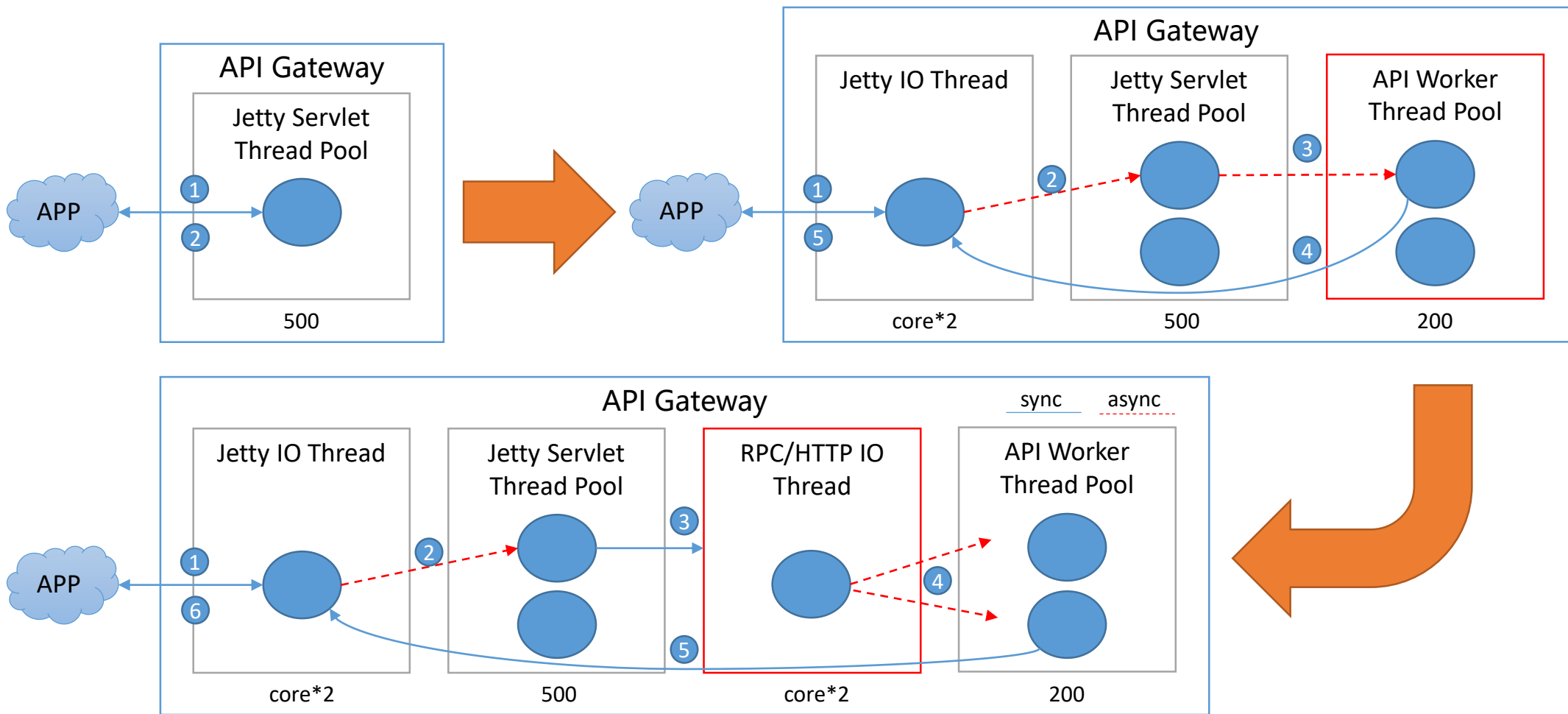
如何打造高可靠的API网关





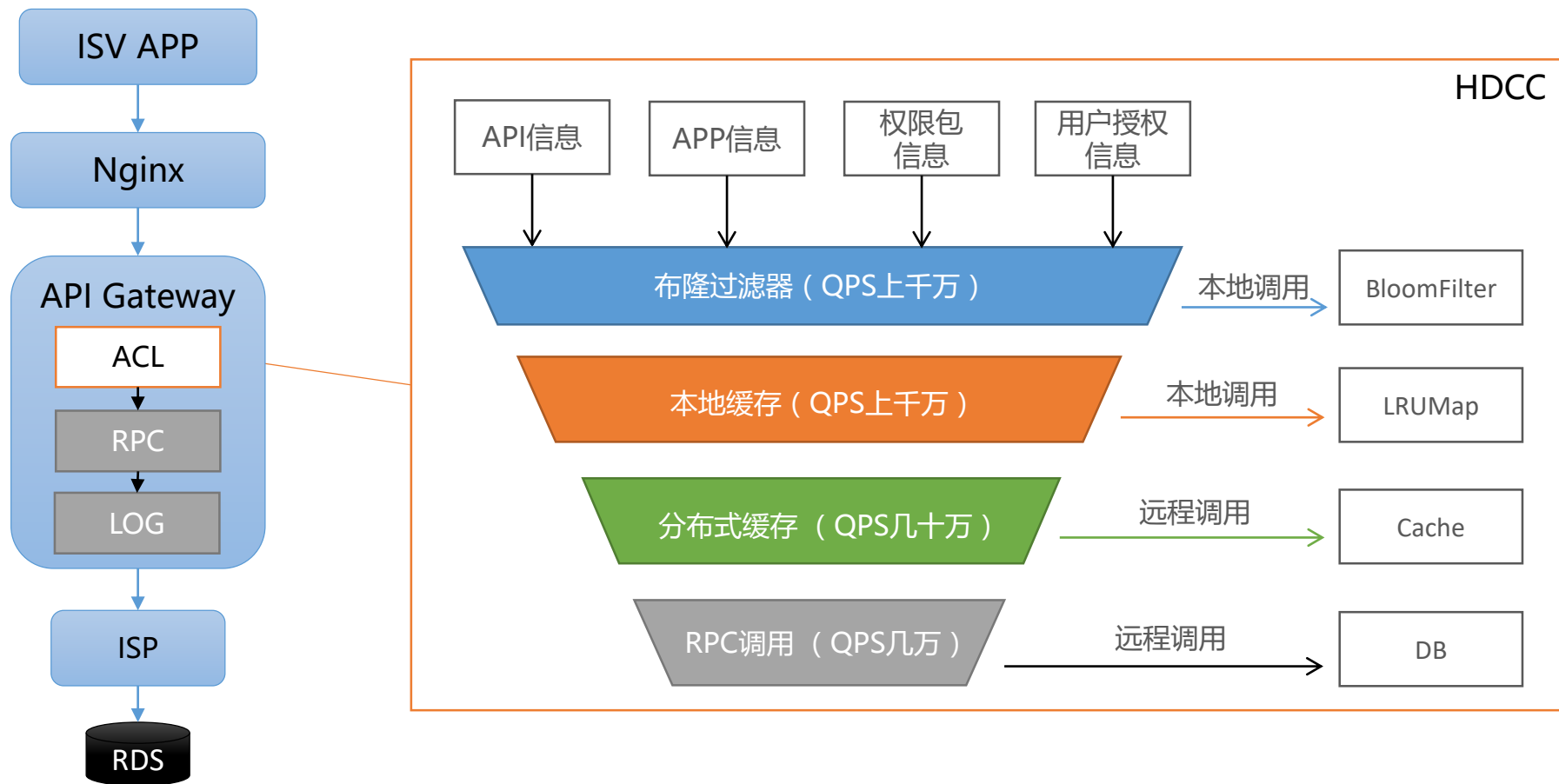


API请求全异步化



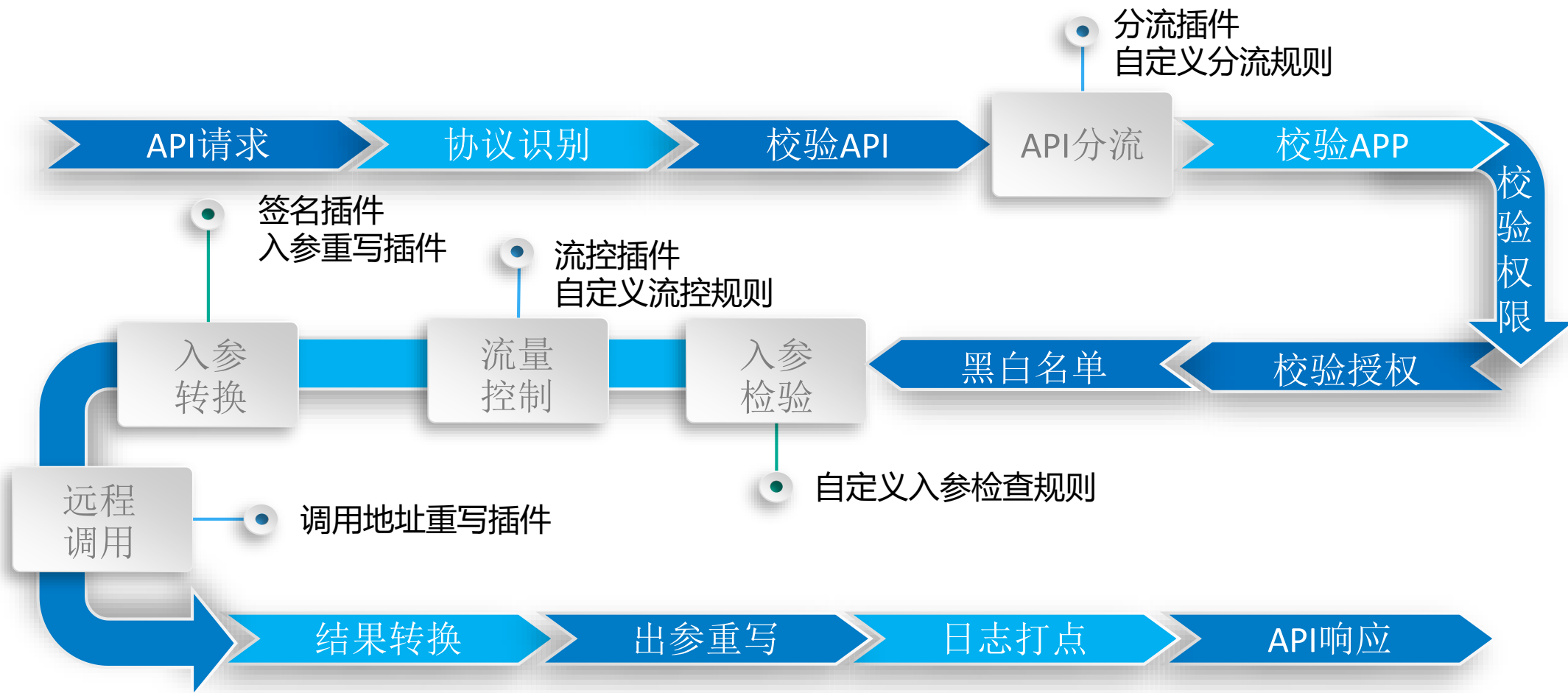
释放网络等待引起的线程占用，线程数不再成为网关的瓶颈
彻底隔离API请求之间的影响，慢API不会引起网关的不稳定

API元数据无阻塞调用

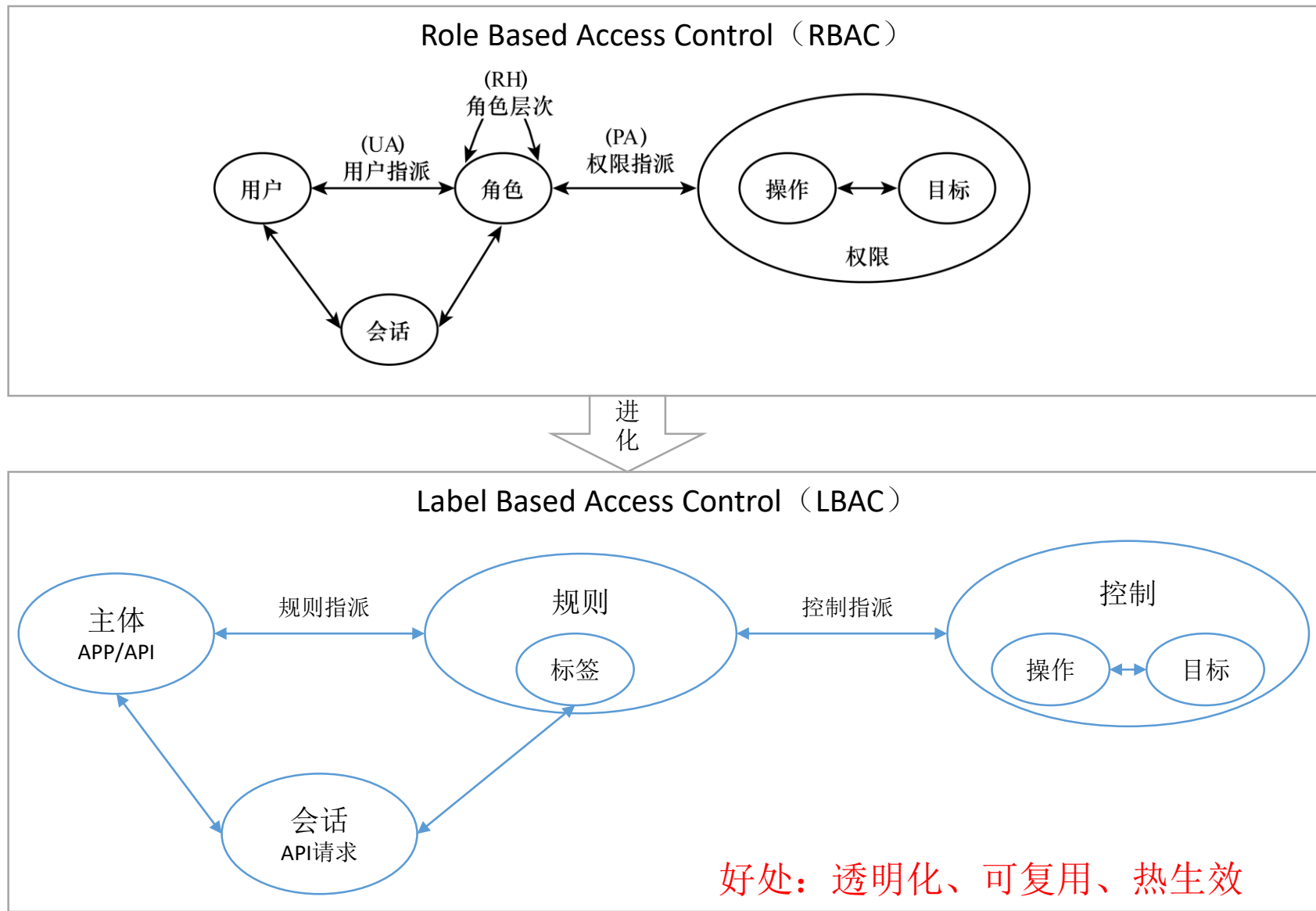


消灭99.9%的IO等待，CPU只用于计算资源
网关耗时降低到1~2毫秒，较少的DB资源支持高并发

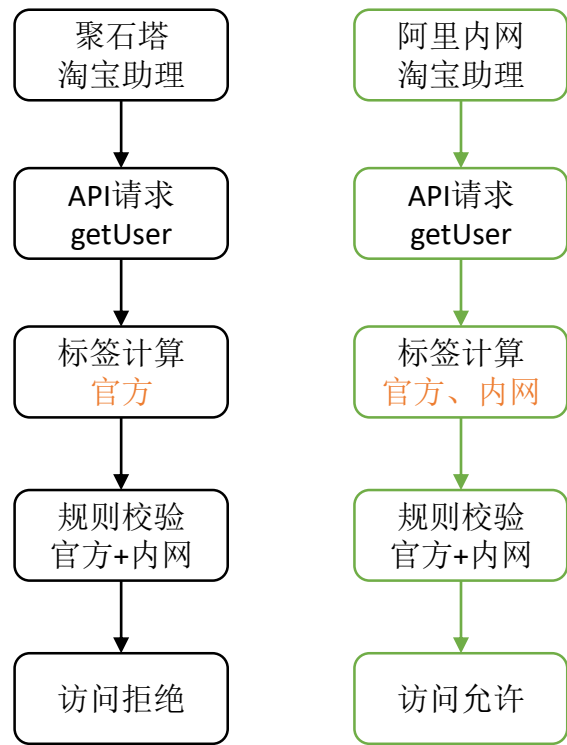
API插件化体系 — 运行时升级网关



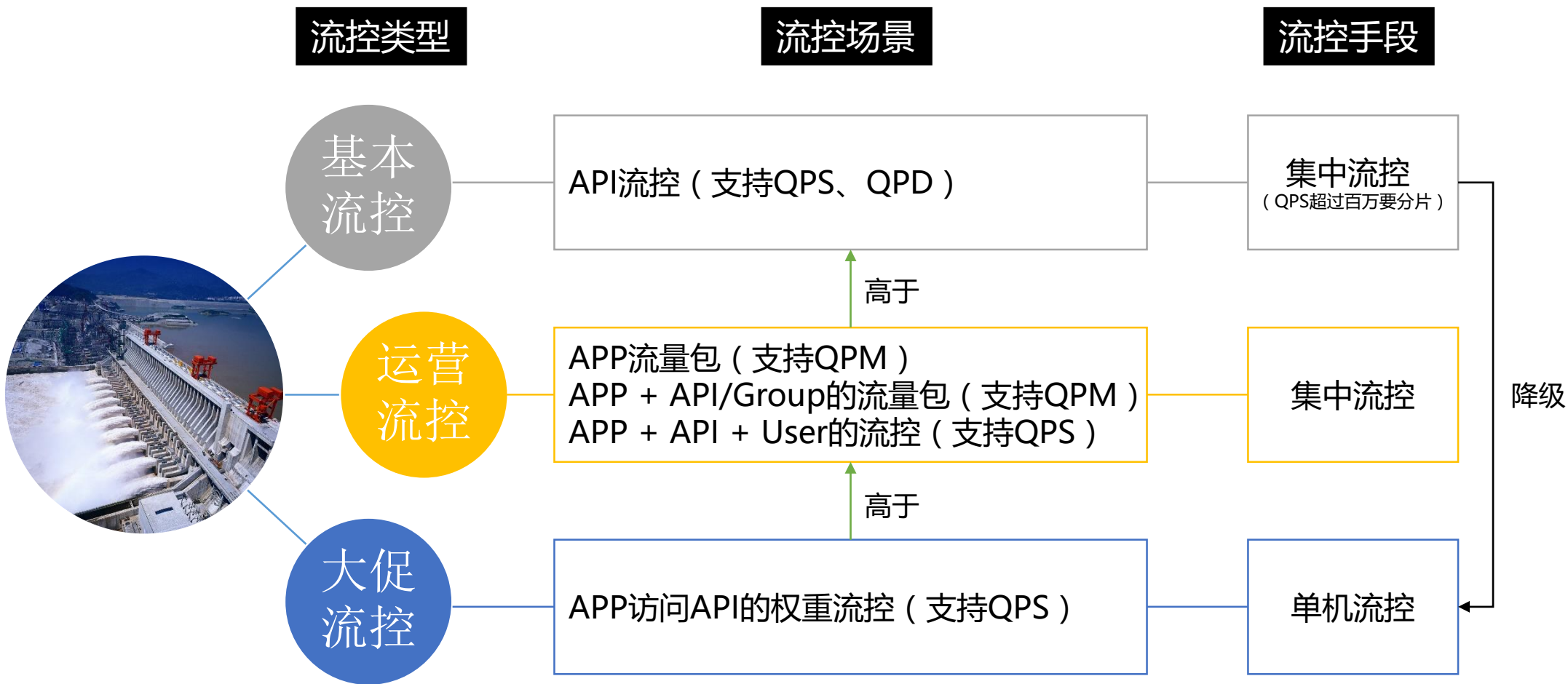
API访问控制体系 — LBAC



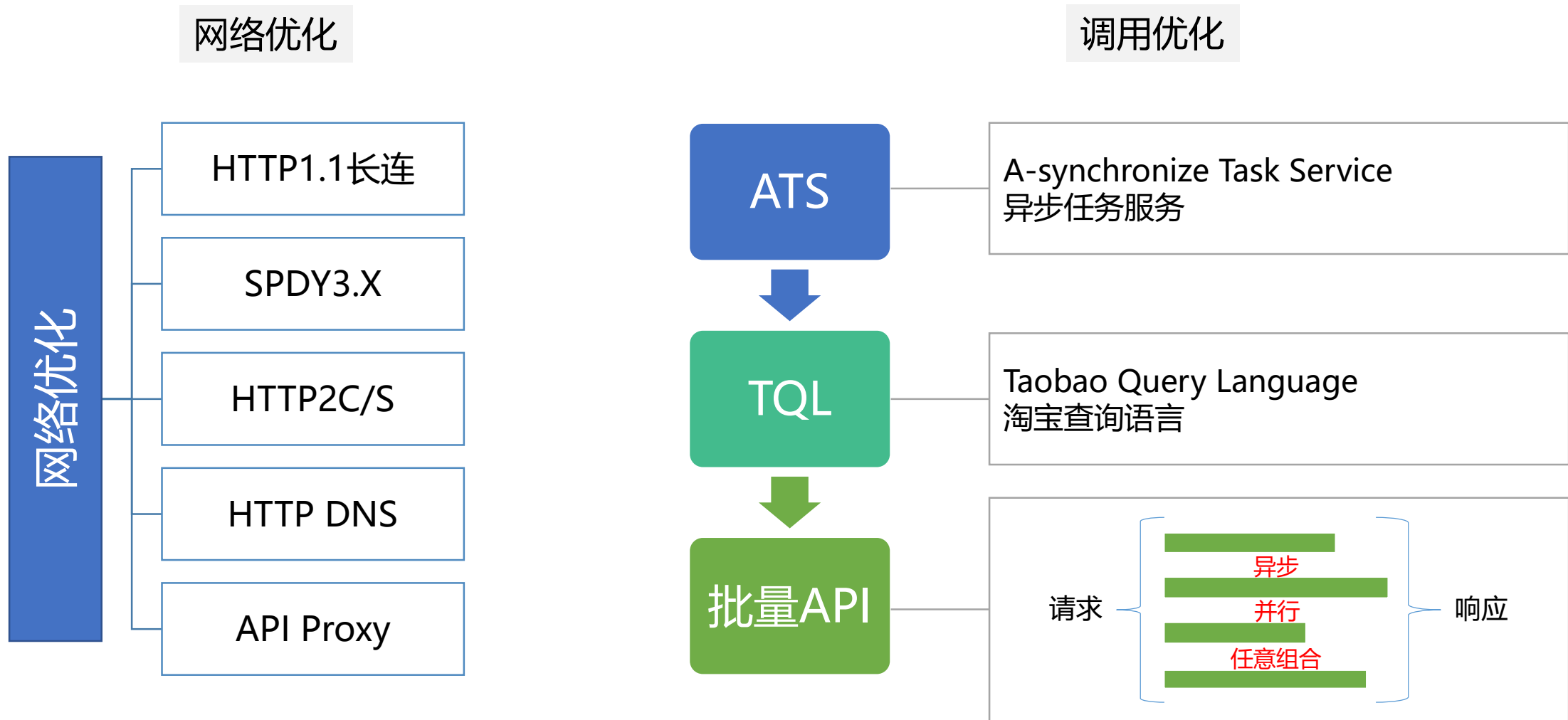
举例：getUser接口只允许官方应用从内网发起调用



API流量控制



API弱网环境调用优化



03

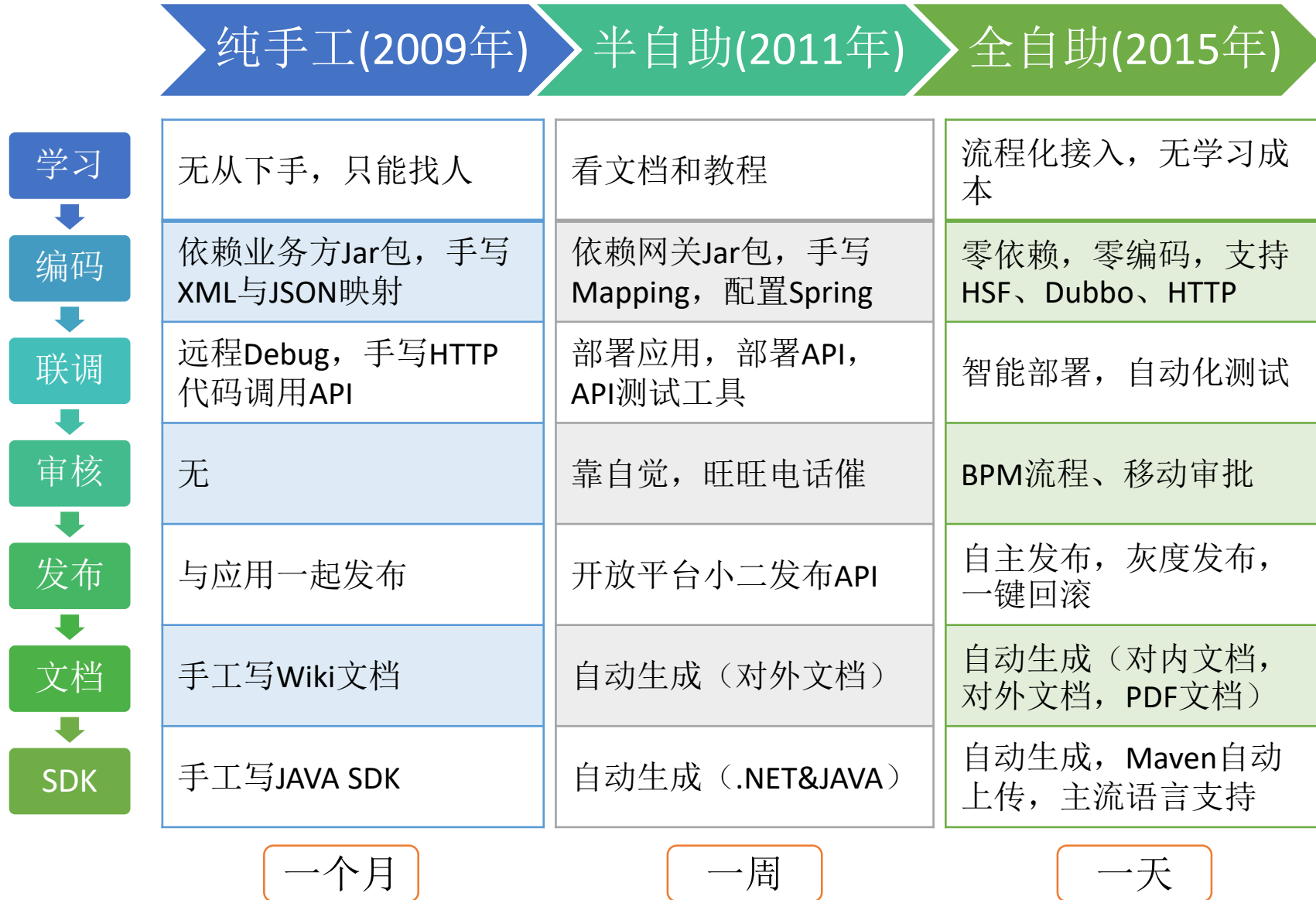
第三部分

API接入自动化

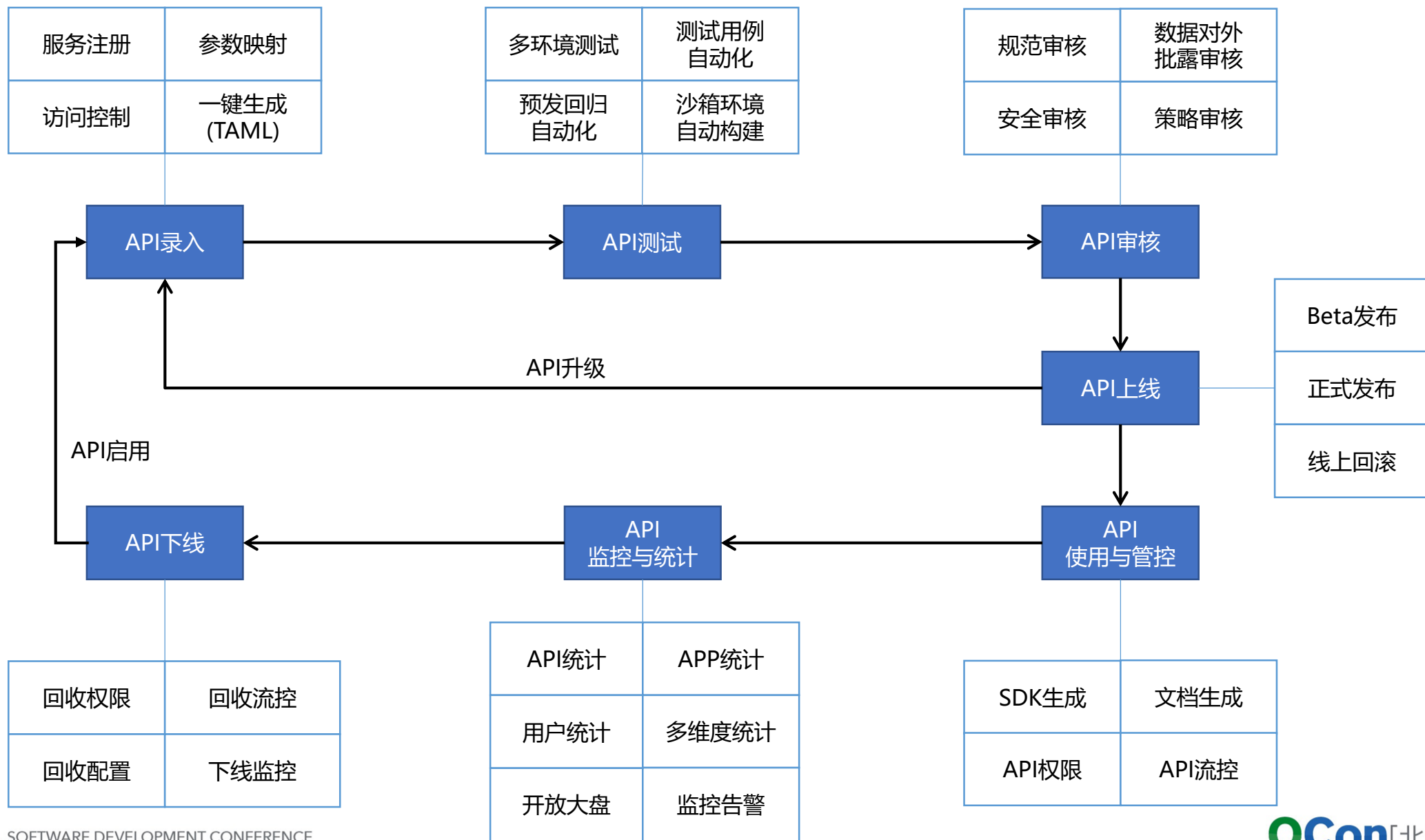
如何打造高效的API接入管理平台



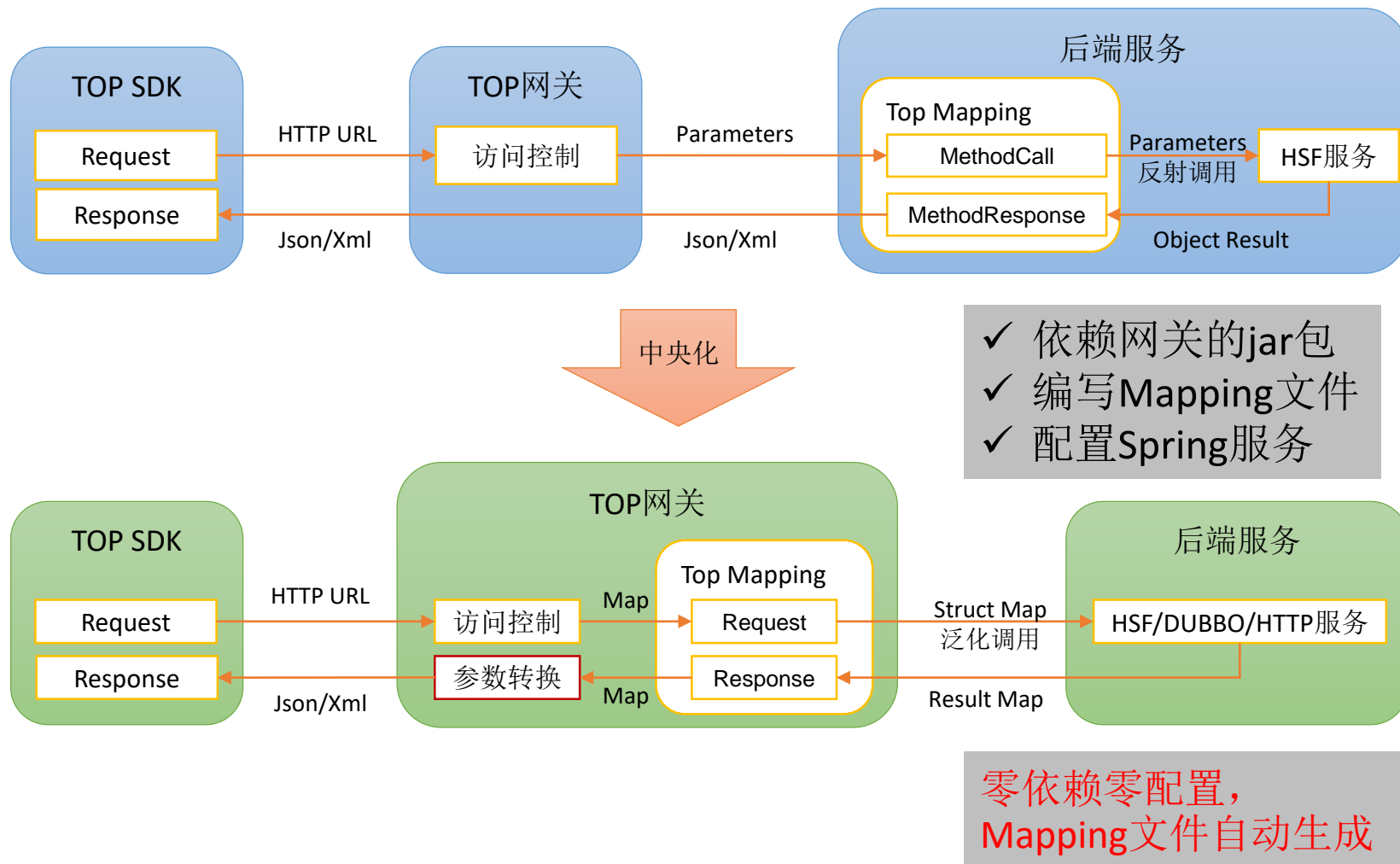
API接入自动化演进



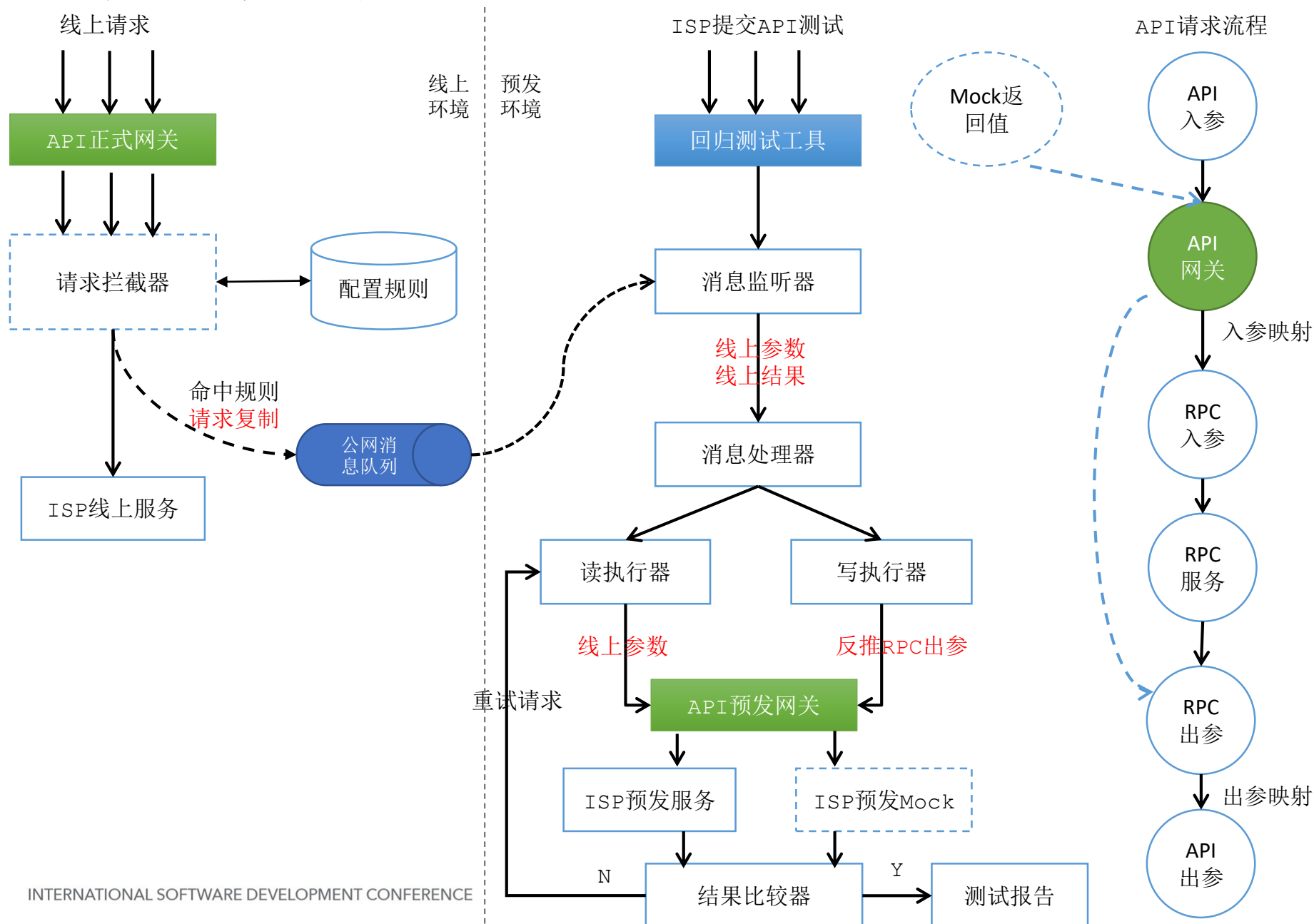
API接入低学习成本 — 流程化与自助化



API接入的零二次开发 — 映射中央化



API变更零测试成本 — 回归测试自动化



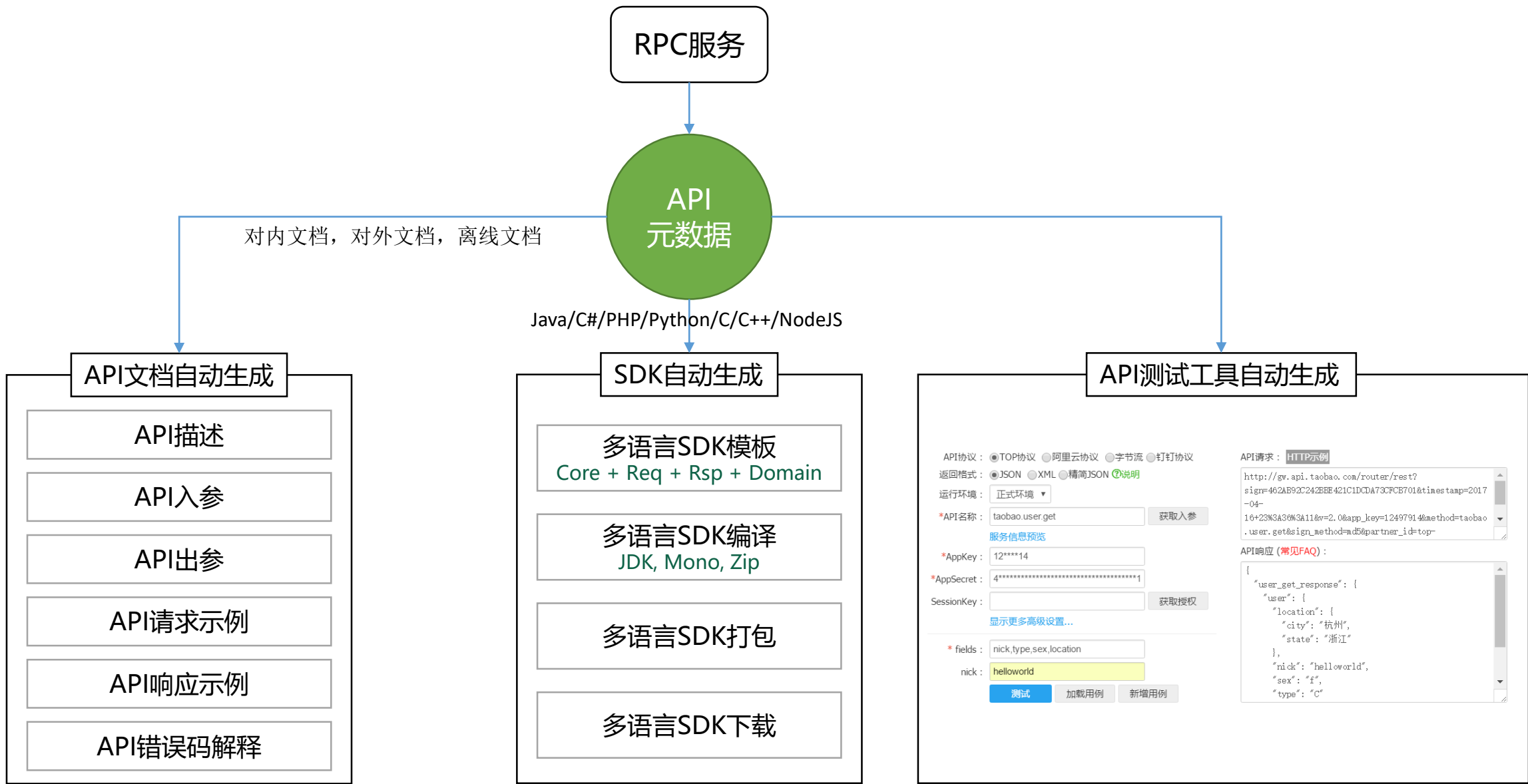
关键点:

- 线上请求复制到预发
- 自动生成测试用例
- API请求重放 (读API)
- API结果Mock (写API)
- API测试结果比较

优势:

- 测试用例全面
- 快速发现问题
- 零测试成本
- 变更稳定性保障

API元数据强一致性保证 — 自动化生成文档、SDK、工具



API接入自动化演示 — 三分钟接入一个API

阿里开放平台

开放 数据 运营 运维 帮助

关键字 风胜

- API
- 我的变更
- 我的项目
- 所有API
- 工具
- 权限
- 流程
- 文档

开放 / API / 我的变更

API类型: 所有 变更范围: 我负责的 变更状态: 进行中 所属项目: 搜索

+ 新建变更

变更原因	API名称	所属项目	负责人	进度	操作
支付宝收藏夹消息	taobao_mercury_Add	TOP专用日常	萧玄 承仙 风胜 似年	日常测试中-未审核	预览API 修改变更 关闭变更
taobao_cart_UnDelete	taobao_cart_UnDelete	TOP专用日常	萧玄 承仙 风胜 似年	日常测试中-未审核	预览API 修改变更 关闭变更
支付宝消息接入	taobao_cart_Delete	TOP专用日常	萧玄 承仙 风胜 似年	日常测试中-未审核	预览API 修改变更 关闭变更
支付宝消息接入	taobao_cart_Update	TOP专用日常	萧玄 承仙 风胜 似年	日常测试中-未审核	预览API 修改变更 关闭变更
支付宝消息接入	taobao_cart_Add	TOP专用日常	萧玄 承仙 风胜 似年	日常测试中-未审核	预览API 修改变更 关闭变更
TOP专用日常	taobao.item.rules.vip.check	API 3.0 TOP专用日常	萧玄 承仙 风胜 似年	录入中	预览API 修改变更 关闭变更
萧玄测试日常	taobao.sunshao.test.samservice	API 2.0 萧玄测试日常	萧玄 吴迪 风胜 溪行	录入中	预览API 修改变更 关闭变更
萧玄测试日常	taobao.xiaoxuanmock.getresult	API 2.0 萧玄测试日常	萧玄 吴迪 风胜 溪行	录入中	预览API 修改变更 关闭变更
萧玄测试日常	taobao.xiaoxuanmockone.test	API 2.0 萧玄测试日常	萧玄 吴迪 风胜 溪行	录入中	预览API 修改变更 关闭变更

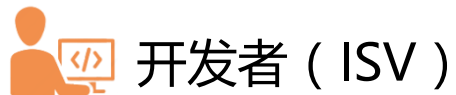
« 上一页 1 下一页 » 共1页 到 确定 页

04

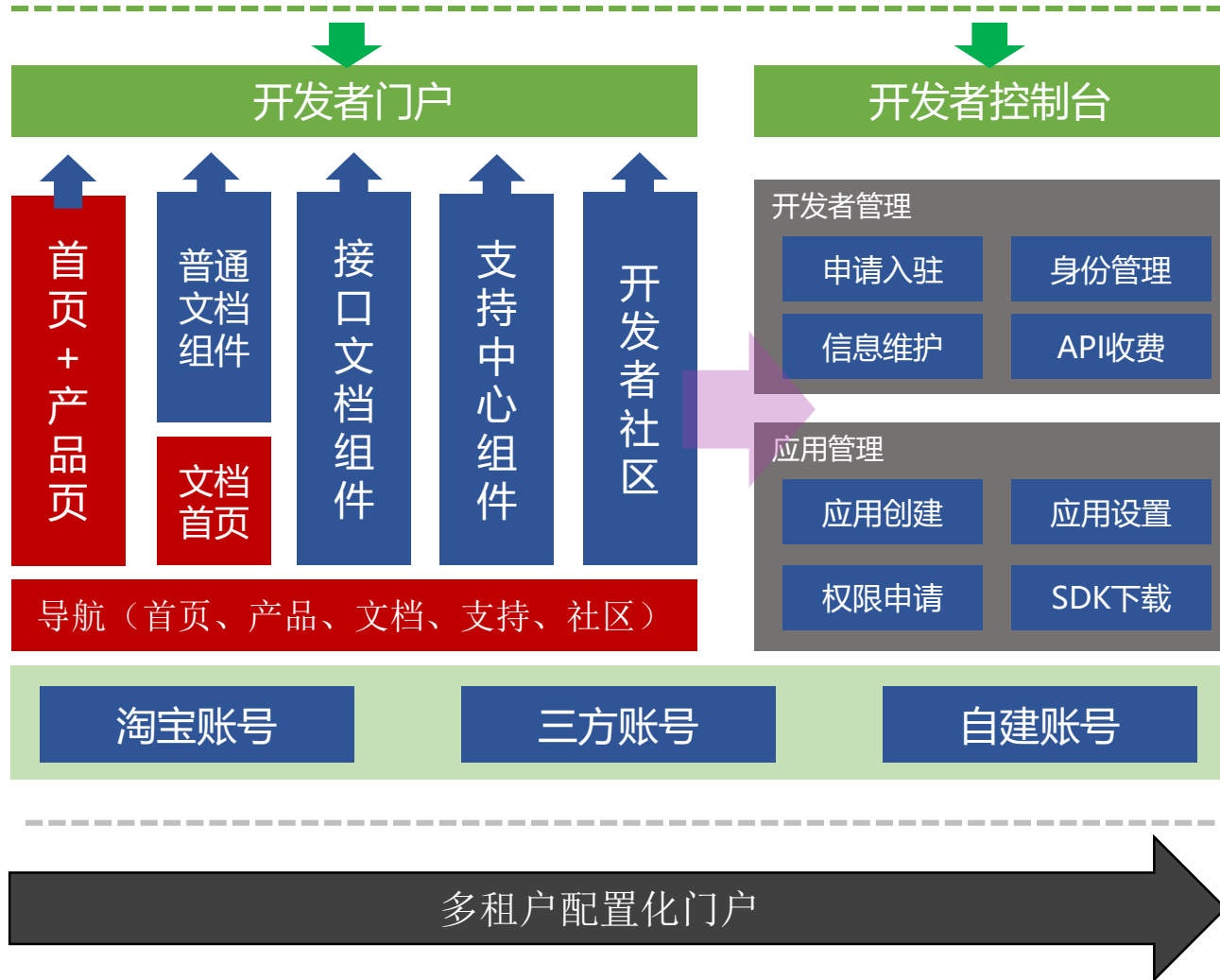
第四部分

开放平台工厂

开放平台工厂 — 多租户与配置化门户（前端）



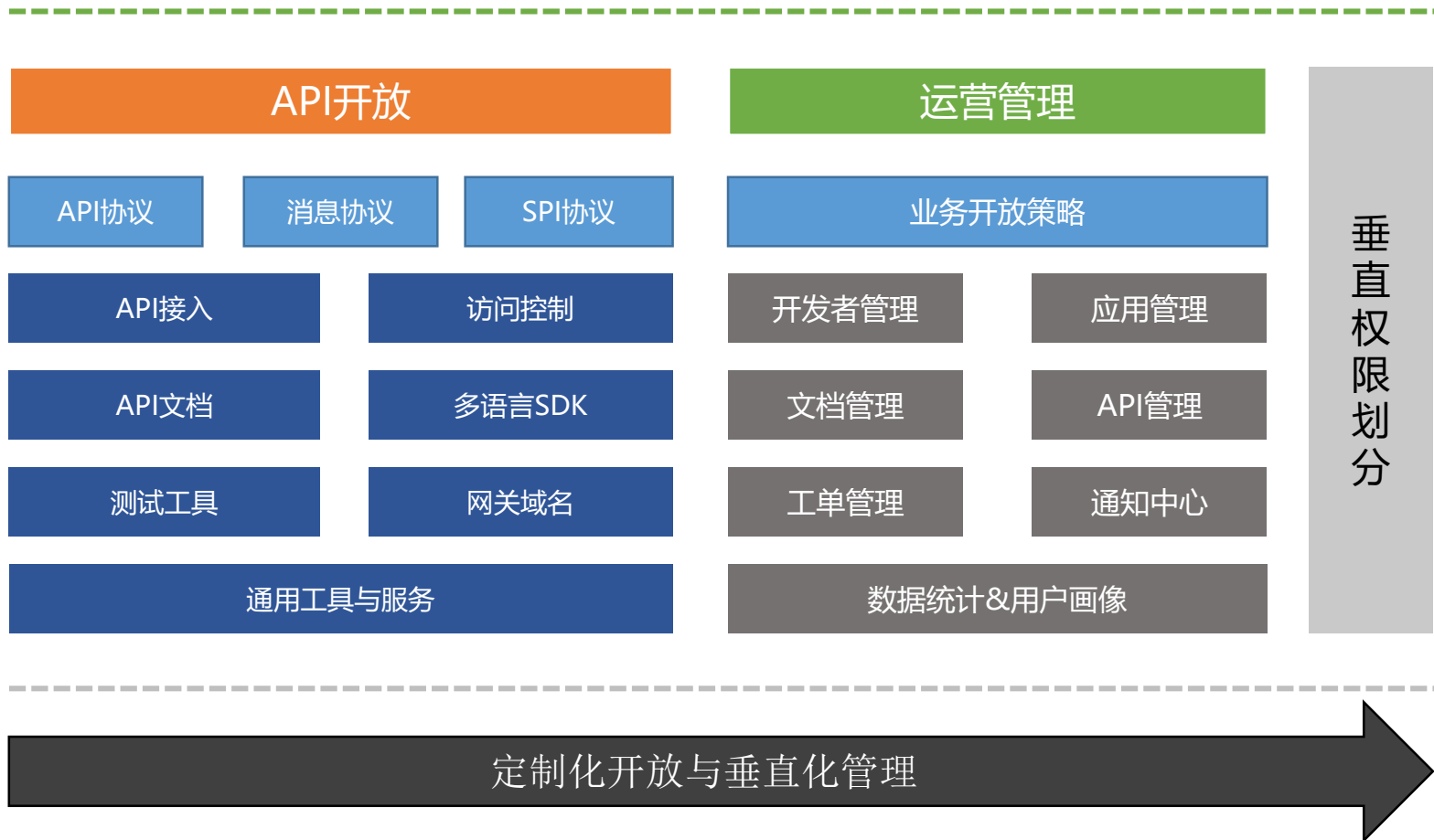
开发者 (ISV)



开放平台工厂 — 定制化开放与垂直化管理（后端）



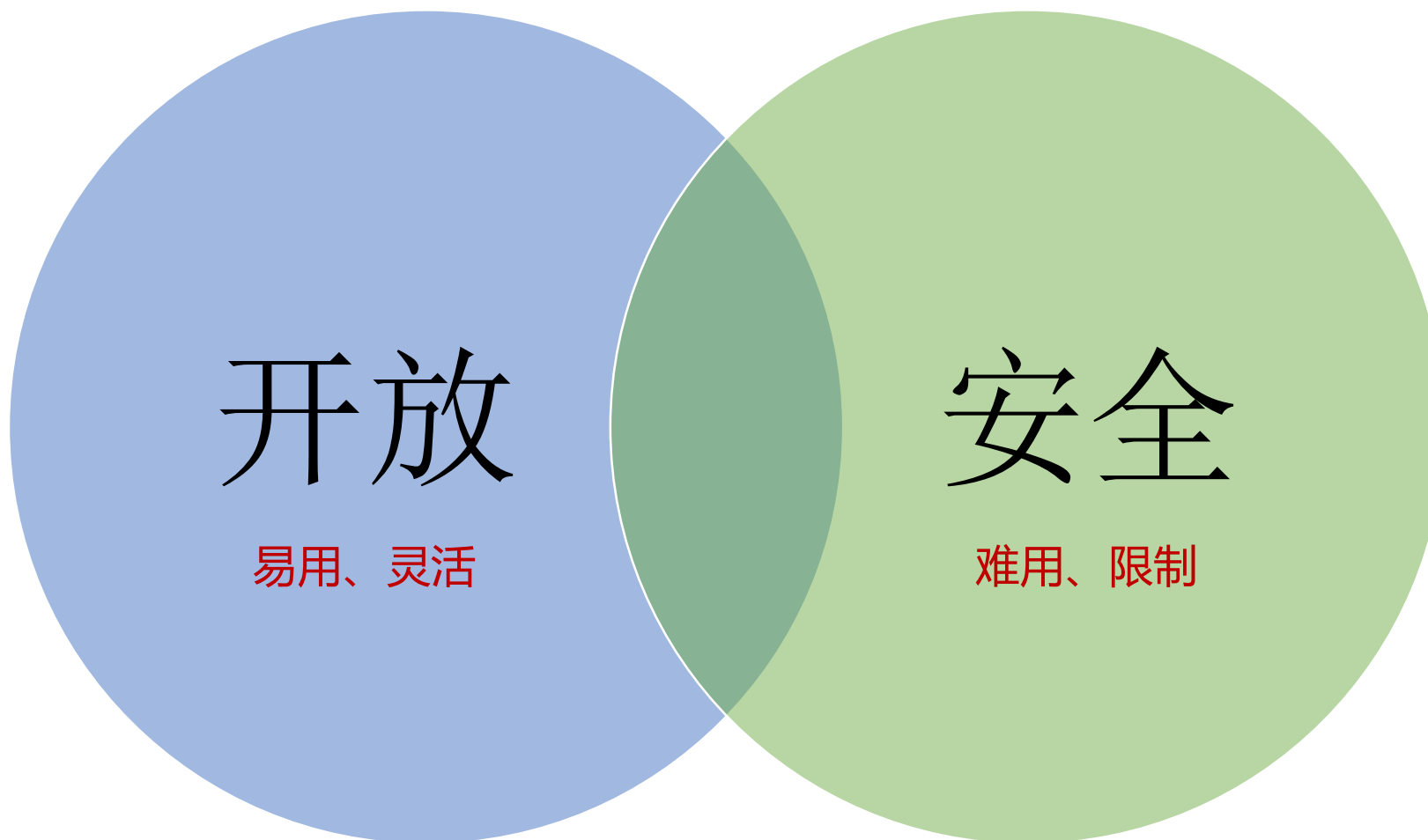
服务提供方（ISP）



05

第五部分

开放平台安全



网关安全

- 用户身份认证 (OAuth2)
- API协议安全 (SSL、防篡改、防重放)
- API权限控制 (APP级, 用户级)
- 多维度流控 (APP+API+User)
- 黑白名单控制 (应用级、用户级)
- 日志打点与分析 (API级、字段级)

数据安全

- 对外数据披露审批流程
- 数据分级 (API级, 字段级)
- 数据脱敏 (模糊化)
- 数据混淆 (Open Security ID)
- 数据加密 (API响应, RDS数据)
- 安全保镖 (行为监控, 异常报警)

应用安全

- ISV入驻规范、安全技术要求
- APP创建申请、API权限包申请
- 应用安全配置 (IP绑定、用户绑定)
- 应用安全扫描 (黑盒扫描、白盒扫描)
- 安全托管环境 (聚石塔、千牛、TAE)
- 人机识别防刷 (无线安全保镖)

《尽在双十一》





联系作者：winwindg

Thanks!



INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 **Geekbang**  **InfoQ**
极客邦科技

诚邀志同道合的朋友加入淘宝开放平台：fengsheng@alibaba-inc.com