四块程序各管自己的事，也只写自己的库

蓝线：服务调用。灰线：只写自己的库；跨线小桥表示没有连接。支付不经过公共服务。

平台管理员
管理品牌、登录、查看品牌码

品牌、门店与各操作端
19端清单：经营13＋供应链3＋企业3；其中5个小程序。PC统一Bootstrap / Blade。

管理与认证

日常营业

01 总平台管理
品牌登记 / 启用与关闭
管理员身份 / 部署绑定
签发和核验可信授权

02 品牌门店业务
成员 / 门店权限 / 终端
订单 / 商品 / 库存 / 报表
SaaS或品牌私有部署

发送短信

申请上传

03 公共服务
短信、文件等第三方能力
短信发送 / 文件授权与核验
短信与文件分队列、限额
其余已有能力归属另核

04 支付服务
收款 / 退款 / 渠道回调
验签 / 对账 / 结果投递
独立账号与渠道密钥

发起收款、申请退款或查结果

通知支付结果：可靠消息，去重并拒绝旧版本

保存记录

保存记录

保存记录

保存记录

总平台库
品牌 / 绑定 / 授权 / 审计

品牌业务库
SaaS数据或品牌私有数据

公共服务库
短信任务 / 文件控制记录

独立支付数据库
渠道事实 / 支付退款账

管理状态单独同步，不夹在每笔普通订单中
总平台 → 业务 / 公共 / 支付：可靠消息通知品牌启停；接收方去重、按版本拒绝旧状态，并定时主动核验。

平台直接调用公共发送验证码；私有业务数据留品牌侧。供应链、企业模块的后端归属另确认。

同一套品牌业务代码，两种部署路径

SaaS与私有化共享业务规则；私有初始化由总平台核验管理员短信码，公共服务只负责发送。

SaaS：总平台提供业务服务

操作端 → SaaS品牌业务 → SaaS业务库
每次请求核验成员、门店和品牌归属
手机号有5个SaaS品牌：只列这5个

私有化：品牌自己的业务与数据库

操作端 → 本品牌业务 → 本品牌私有库
实例固定绑定一个品牌，不允许前端切换
另有2个私有品牌：当前入口只列本品牌

需要时再调用总平台服务

业务 / 公共 / 支付 → 总平台核验授权
品牌业务 → 公共申请短信或文件能力
品牌业务 → 支付发起收款或查结果

私有部署首次绑定

1 私有业务
品牌码测试连接成功后
提交挑战、公钥和持钥证明

→

2 总平台认证
再发管理员手机验证码
绑定已登记手机号和挑战

→

3 公共发送
核验总平台专用身份
发送短信，不要求先绑实例

→

4 总平台认证
核验输入的短信码与挑战
一次完成消费、绑定和审计

→

5 私有业务
获得限定品牌和实例的授权
再开通获准的服务能力

验证码由总平台生成和核验；私有端不自行认定正确。短信不可用时暂停绑定，不绕过验证。

授权状态：定时核验＋可靠通知

总平台先保存启停状态，再可靠发送；下游故障不回滚关闭。
接收方去重、拒绝旧版本；漏版本时向总平台补查。
收到关闭立即限制对应新动作；断网未收到时有传播窗口。
展示最后核验时间，不能宣称全网瞬时关闭。

三个期限分别算，不能相互延长

调用凭证有效期：具体时长待定，只能在可信新鲜状态下签发。
私有24小时：从最后成功可信授权核验起算。
终端离线：范围另定，连接断联中的私有端不能重置24小时。
超过24小时的基础营业和旧单收尾，按待确认动作清单执行。

待确认：关闭后的旧单付款与退款、终端离线范围、品牌码轮换及丢钥换绑恢复。

短信、文件与支付，按各自流程完成

箭头写明具体动作；业务程序先核验用户权限，支付不经过公共服务代理。

短信

总平台认证 / 品牌业务
平台发验证码；业务发通知

→ 请求发送 →

公共短信模块
登记任务、校验额度

→ 调用发送 →

短信供应商
发送并返回状态

→ 返回回执 →

公共短信模块
接回执并保存发送记录

平台账号验证码只由总平台生成核验，公共只发送。超时先查再安全重试；短信和文件分别限额。

文件

品牌业务
先查用户与对象权限

→ 申请上传 →

文件授权与核验方
发短时、限对象的授权

→ 返回上传授权 →

操作端 ↔ 选定对象存储
字节直传，上传完成仍须核验后才发布引用

A 品牌自有存储 品牌本地模块核验；长期密钥留品牌。此模块不是新增第五个总部服务。

B 总部托管存储 先确认内容和元数据外传范围；公共服务核验，业务只保存文件引用。

两种归属尚待选择。下载先验权限再给短时授权；已签链接不保证即时撤销。

支付

品牌业务
订单引用、金额和币种

→ 发起收款 →

独立支付服务
验商户、金额、签名和重复通知

→ 请求渠道收款 →

支付渠道
收款、退款及可信回调

← 通知支付结果 ←

← 可靠通知业务更新订单 ←

支付先保存可信结果，再通知业务；消息去重、版本去旧。私有侧不能接入站通知时，主动拉取并确认。
超时先查原交易，不换编号重扣。已知关闭拒绝新收款；可信旧回调继续接收，退款等规则另定。

建议四个后端仓库＋一个客户端工作区

五个主仓库是本轮建议，尚待确认。19个操作端不等于19个仓库，也不等于19套后端。

总平台仓库
Laravel平台管理
Blade / Bootstrap页面
品牌授权与身份测试

只构建受影响部分

独立检查与发布
固定依赖与版本
各自测试、发布、回退

品牌业务仓库
Laravel业务模块
品牌、门店PC页面
SaaS / 私有同一套代码

只构建受影响部分

独立检查与发布
固定依赖与版本
各自测试、发布、回退

公共服务仓库
Laravel公共能力
短信与文件分队列
各自限额与失败补偿

只构建受影响部分

独立检查与发布
固定依赖与版本
各自测试、发布、回退

支付仓库
Laravel目标方案
渠道适配、账本、对账
独立账号、密钥与数据库

只构建受影响部分

独立检查与发布
固定依赖与版本
各自测试、发布、回退

客户端工作区
5个原生小程序
Android / iPad工程
必要独立Web交互资源

只构建受影响部分

独立检查与发布
固定依赖与版本
各自测试、发布、回退

四后端统一 PHP / Laravel / Nginx / PostgreSQL；总平台、品牌和门店PC统一 Bootstrap / Blade。

共享的是接口说明和版本化调用包
接口由提供方维护：字段、权限、金额、错误码和事件版本。
消费者固定版本；公共包不放密钥，不擅自重扣款。
先提供兼容新接口，再升级调用方，最后退出旧版本。
一个服务更新，不要求其余服务同天一起更新。

开发与验收按真实调用关系协作
先定跨服务接口，再按相同样例并行开发和测试。
必须验证真实身份、跨品牌拒绝、重复、乱序和断网恢复。
代码回退不等于账务回退；数据库变更须兼容旧程序。
旧React / TypeScript支付资产先审计，尚未迁移或重写。

小程序、Android与iPad保留各自技术和构建方式。PC页面由所属业务服务提供，不经总平台中转私有数据。

DEV复用已购三台，建议再加一台总平台服务器

四块程序分开发布；要减少共同停机，还需看服务器、数据库、网络入口和恢复要求。

总平台服务器
规格 / 价格 / IP尚未产生
建议新增，待批准

品牌业务服务器
已购，拟部署业务

公共服务服务器
已购，拟部署公共

支付服务器
已购，拟部署支付

已有业务数据库实例：首期建议放三个独立逻辑库

总平台库＋独立账号

SaaS业务库＋独立账号

公共服务库＋独立账号

仍共同承担重启、资源争用与故障；三个库不等于三个独立数据库实例。

已有独立支付数据库
只给支付专用身份访问
其他三块不跨库写支付账
两台现有数据库均为基础版

DEV当前事实：已购3台均2核4GB；应用与网络尚未配置完成，公网IP为空、带宽0Mbps。

现有基础版不支持日志备份和按时间点恢复，须验证备份集恢复。Redis只作缓存，不能作为唯一账本。

DEV 开发
本轮先完善
测试数据 / 测试商户

→

TEST 自动回归
按测试窗口启用
独立数据与身份

→

UAT 业务验收
按验收窗口启用
冻结候选版本

→

SIM 生产演练
按演练窗口启用
接近生产拓扑与网络

→

PROD 正式运行
独立于非生产
按恢复目标确定隔离

生产与采购边界

生产优先四服务各自数据库实例；高可用副本和跨区安排，先按最长可停多久、最多可丢多少数据与预算决定。
五环境分期启用，不是现在买20台。保留25入口；共享入口仍有共同风险。已确认支出773.60元，非月预算。

公网1Mbps差价70.64元尚未支付；不计入773.60元。新增平台服务器也尚无报价，不按历史单价估成已付款。