

D03 订购与支付域 · 设计文档

本域总览见《账号计费中心 · 结构大纲》。全文分六段：定位与边界 / 角色与依赖 / 数据模型 / 核心流程 / 接口契约 / 关键约束与验收标准。

1. 定位与边界

定位：把「用户想买的东西」变成「账上可用的钱」。本域回答买什么、多少钱（商品与价目）、怎么付（渠道与下单）、钱何时算到账（回调、人工确认、关单与查单自愈），并承载订阅套餐账本与密钥台账。

核心概念

概念	口径
商品	<code>kind</code> 只取 <code>recharge</code> ；商品行不承载售价，只有规格（ <code>meta</code> ）与可见性（ <code>status</code> 取 <code>listed</code> / <code>unlisted</code> ）。
售价版本	<code>product_prices</code> 的有效区间快照：当前价 = 区间未闭合那条；调价 = 关旧价 + 落新价。
价目规则版本	<code>price_rules</code> 按整版本发布，供计量方读单价；本域不二次核算扣费。
订单	购买意图事实行，幂等键 = <code>order_no</code> ；下单定格商品与渠道快照，调价下架不回改历史单。
支付渠道	<code>pay_channel_configs</code> ：四道闸门齐备且灰度放行才对客户可见；模式取 <code>mock</code> / <code>sandbox</code> / <code>production</code> / <code>manual</code> 。
账户访问密钥	<code>account_api_keys</code> ：明文仅创建时返回一次，库存哈希，消耗归因落到组。
订阅套餐账本	每客户每商品至多一个在营订阅；周期额度以新发额度包承载，到期即过期，等同于额度重置。

边界

- 不管扣费与资金口径：余额、流水与欠费判定属钱包与账务域；本域只管「钱进得来」，入账后触发一次准入状态发布（读侧契约属账户状态与准入域）。
- 不管退款审批、渠道出款与退款对账：门户只留「申请」入口，其余语义详见 D07。
- 不管发票（D08）、身份凭证与登录（D01，本域只写扫码支付的商户凭据与回调）、用量计量与计费（D05）、风控规则与处置（D09）、工作区与成员组的增删改（D02，本域只消费归属列并做密钥联动失效）、运营面人员与权限模型（D11，只用「在册平台员工」事实作灰度判据）。

关键口径

- 金额：元、6 位小数、字符串传输；目录定价以分存放，下单时换算为元。渠道收银台按 2 位小数比对，故下单与退款定额都要求等效 2 位小数，有效 3 位以上一律拒绝。

2. 幂等两层：订单级 `order_no`（全局唯一）与下单意图级 `client_request_id`（同客户唯一，重复提交返回原单）。
3. 「已入账」唯一判据：流水中 `ref_order` 等于订单号且类型为 `recharge` 的那行；赠金等类型同键不阻断入账。
4. 在营态唯一：订阅按客户 × 商品在营唯一；渠道配置按渠道 × 模式唯一、按渠道至多一行启用。

2. 角色与依赖

参与角色：客户（门户下单人，订单与密钥归属工作区、操作人为成员本人）、组织 Owner / Admin（可处置全组织密钥行）、组管理员（密钥可见范围收窄到其管理的组与本人名下）、运营（带运营令牌与操作人标识）、在册平台员工（灰度判据，非权限体系）、数据面网关（以明文密钥现取校验台账）、计量方（读价目规则版本）、渠道（外部支付网关与对公资金账户）。

能力矩阵（组织角色与组内角色相互独立）

操作	Owner / 组织 Admin	组管理员	普通成员	运营
创建密钥（归属本人）	✓ 可指定本工作区任意启用组	✓ 限本人所在组	✓ 限所在组或默认组	✗
改 / 停用 / 启用 / 软删密钥	✓ 全工作区任意行	仅本人名下	仅本人名下	✗
商品与价目维护	✗	✗	✗	✓
渠道配置、探活与灰度放行	✗	✗	✗	✓
对公人工确认 / 强制查单	✗	✗	✗	✓ 须在册且具出款范围

上游依赖

上游	依赖内容
账号与身份域	门户令牌解析出的用户；协议同意版本（下单出口按当前版本比对）
租户与组织域	工作区、成员与角色、组（含默认组）、组启停状态
钱包与账务域	入账原语（充值 → 现金余额）、流水幂等键、余额位数与欠费重算
运营管理域	平台员工在册事实与运营面配置权限范围

下游被引用

引用方	引用内容	语义
计量与计费域	<code>price_rules</code> 版本快照	按 <code>model_glob</code> 匹配，重叠取 <code>priority</code> 高者；无匹配即未定价
钱包与账务域	订单与 <code>order_no</code>	入账幂等键（ <code>ref_order</code> ）与流水归属

3.2 域间引用

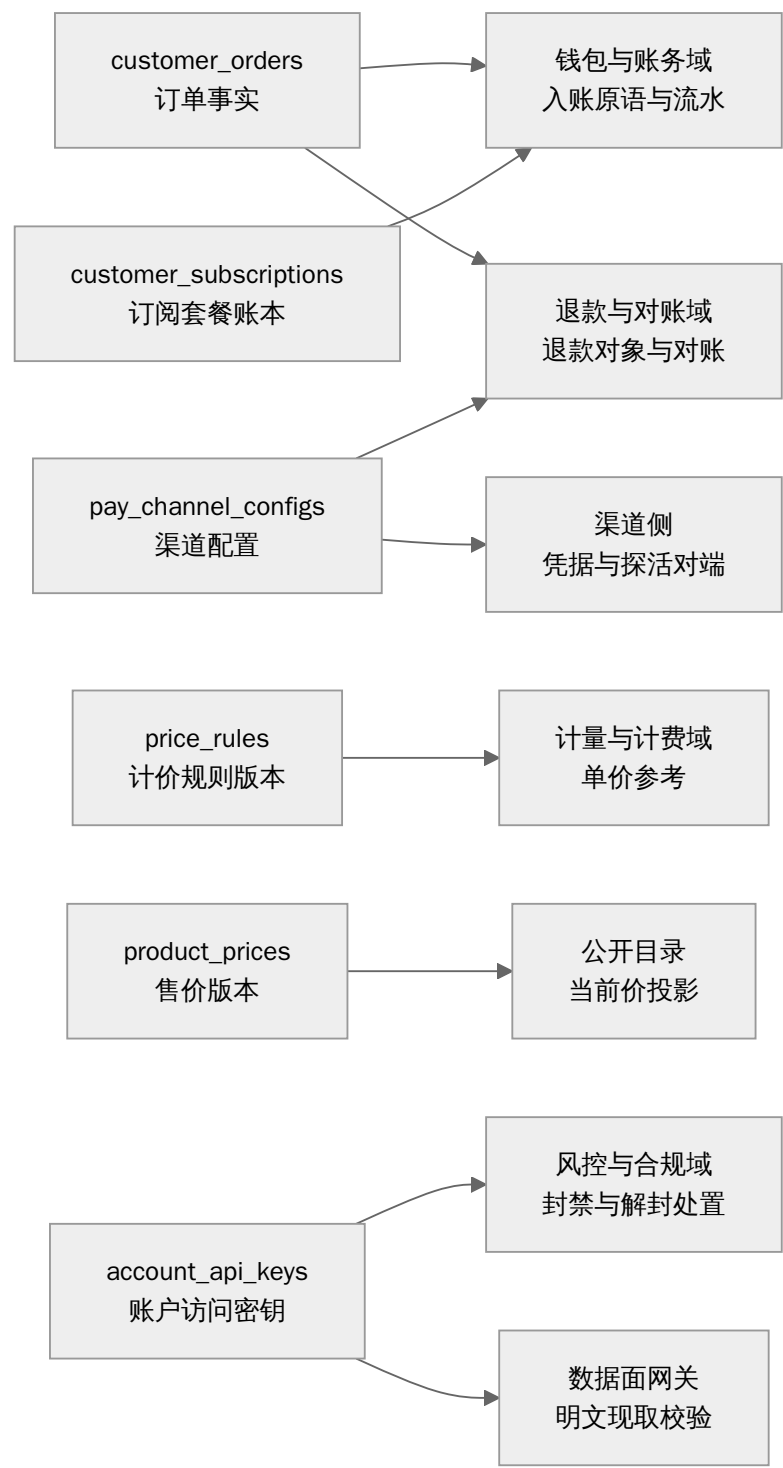


图 2

- 与计量域只走价目规则：单价是计量方的输入，本域不拉用量、不核算扣费；账户密钥与组级执行凭证不混用，执行凭证由数据面网关按组翻译，两者只经组关联。

3.3 表清单 (7 表)

表	职责	关键字段
products	商品定义：仅现金充值面额，只控可见性	code / kind / name / meta / status
product_prices	售价版本的有效区间快照	product_id / price_cents / effective_from / effective_to
price_rules	计价规则整版本（单价参考）	version / effective_from / model_glob / unit_price_cents_per_1k_tokens / tier / priority
customer_orders	订购订单事实，order_no 为业务幂等键	customer_id / order_no / client_request_id / product_code / amount / channel / status / channel_trade_no / channel_raw / meta / paid_at / expires_at / order_poll_attempt_at / order_last_polled_at
customer_subscriptions	订阅套餐账本：每客户每商品一个在营订阅	customer_id / product_code / cycle_days / quota_tokens / price_cents / status / current_cycle_start / current_cycle_end / cancel_reason
pay_channel_configs	渠道配置：每渠道每模式一行、每渠道至多一行启用	channel / is_active / mode / rollout_stage / probe_ok_at / last_probe_error / credentials_encrypted / gateway_url / notify_url / return_url / bank_account_name / bank_account_no / bank_name
account_api_keys	账户访问密钥台账（明文仅创建时一次）	organization_id / user_id / group_id / name / key_prefix / key_hash / quotas / ip_allowlist / expires_at / status / deleted_at

3.4 设计约束

- 商品与售价分离：商品 `code` 唯一、`kind` 只取 `recharge`；售价只在 `product_prices` 上版本化。
- 售价区间快照：当前价恒为 `effective_to` 为空那条；调价先关旧价再落新价，新价生效时点不得早于当前价生效时点（不得抹掉价格历史）。
- 价目版本只增：按整版本发布、版本号自增、不提供单行改写。
- 订单双重唯一：`order_no` 全局唯一；`(客户, client_request_id)` 唯一（部分索引，空值互不相等，未携带该键的下单不受约束）。
- 订单状态集合固定：`pending` / `paid` / `failed` / `cancelled` / `refunding` / `refund_processing` / `refunded` / `refund_failed` / `refund_unknown`；`expires_at` 非空，金额为元 6 位小数。
- 订阅在营唯一：`(客户, 商品)` 至多一行在营订阅（部分唯一索引）。
- 渠道配置双唯一：`(渠道, 模式)` 唯一；每渠道至多一行启用（部分唯一索引，不同渠道可同时启用）。
- 凭据整体加密：凭据序列化后整体加密落单列，加密密钥经环境注入；对公收款账户面向付款用户公开，明文落库。
- 密钥不可逆取回：`key_hash` 唯一、明文不落库；软删（`deleted_at` 非空即视为不存在）保流水追溯。
- 密钥额度多周期：`quotas` 承载 `day` / `week` / `month` / `total`，缺省即不限；单值上界与请求口径同源（`QUOTA_VALUE_MAX`）。
- 来源白名单有上限：逐项须为地址或网段，去重保序，上限 20 条。

4. 核心流程

4.1 下单：意图幂等、撞号重试与快照定格

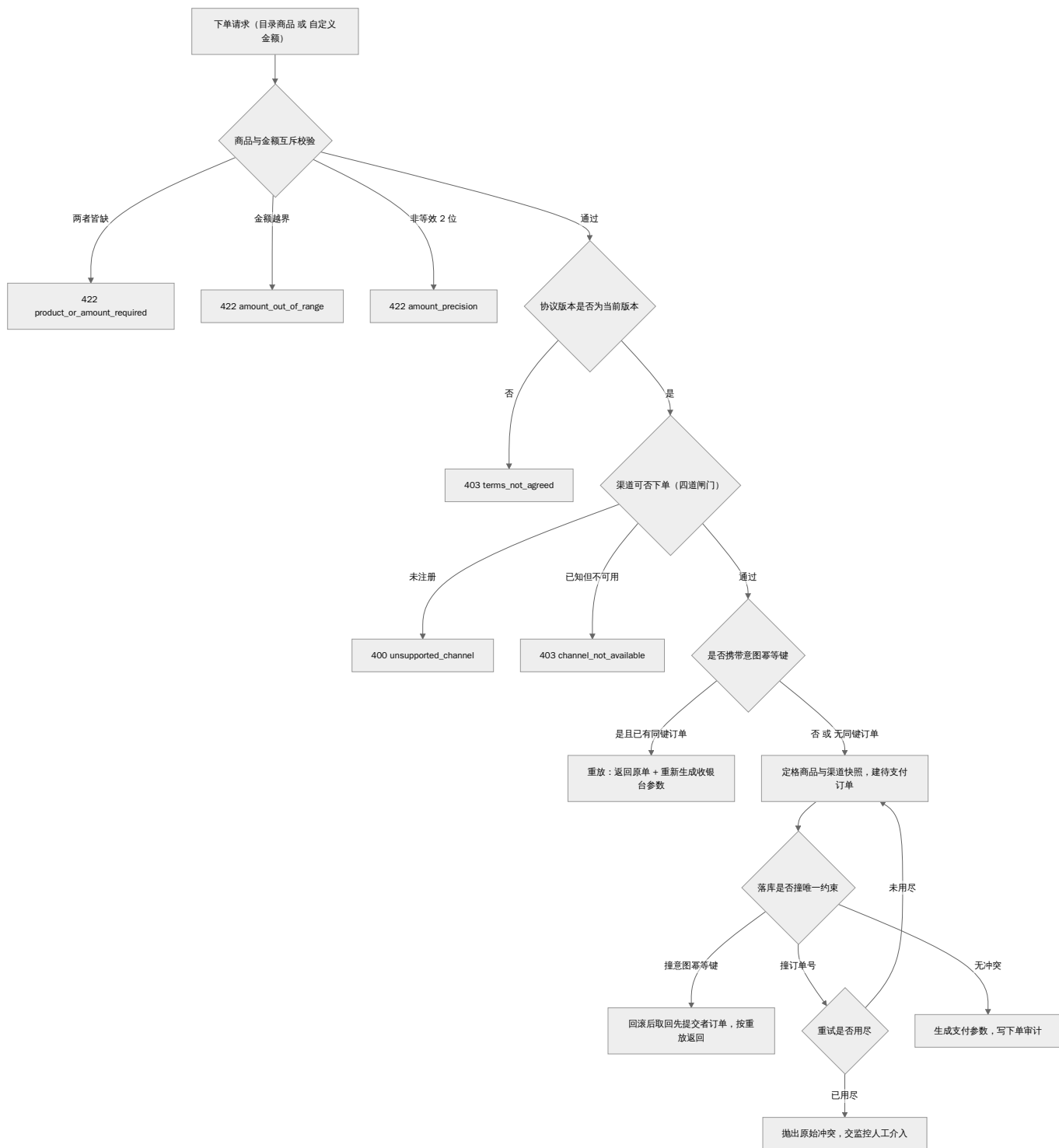


图 3

- 订单号 = 时间戳 + 16 位十六进制随机段（64 bit），同秒撞号概率约 $1/2^{64}$ ；重试有限次（上限 3 次）且只对唯一约束冲突生效，外键与校验类冲突原样抛出。
- 重试期间的会话状态：冲突后整事务回滚会使会话内对象过期，重试、日志与审计一律使用回滚前定格的客户与用户标识，不得再访问会话内对象属性，否则懒加载失败会把「自动重试」变成 500。
- 对公渠道收款账户从订单快照读：运营改账号后历史订单的收款信息不跟着变（用户可能已按旧账号转账）。

- 幂等重放的余额读已提交真值（显式加行锁）：并发双充值下，后到者若读本事务未提交视角，会返回未含本笔的旧值。

4.2 渠道支付回调：验签优先与幂等入账

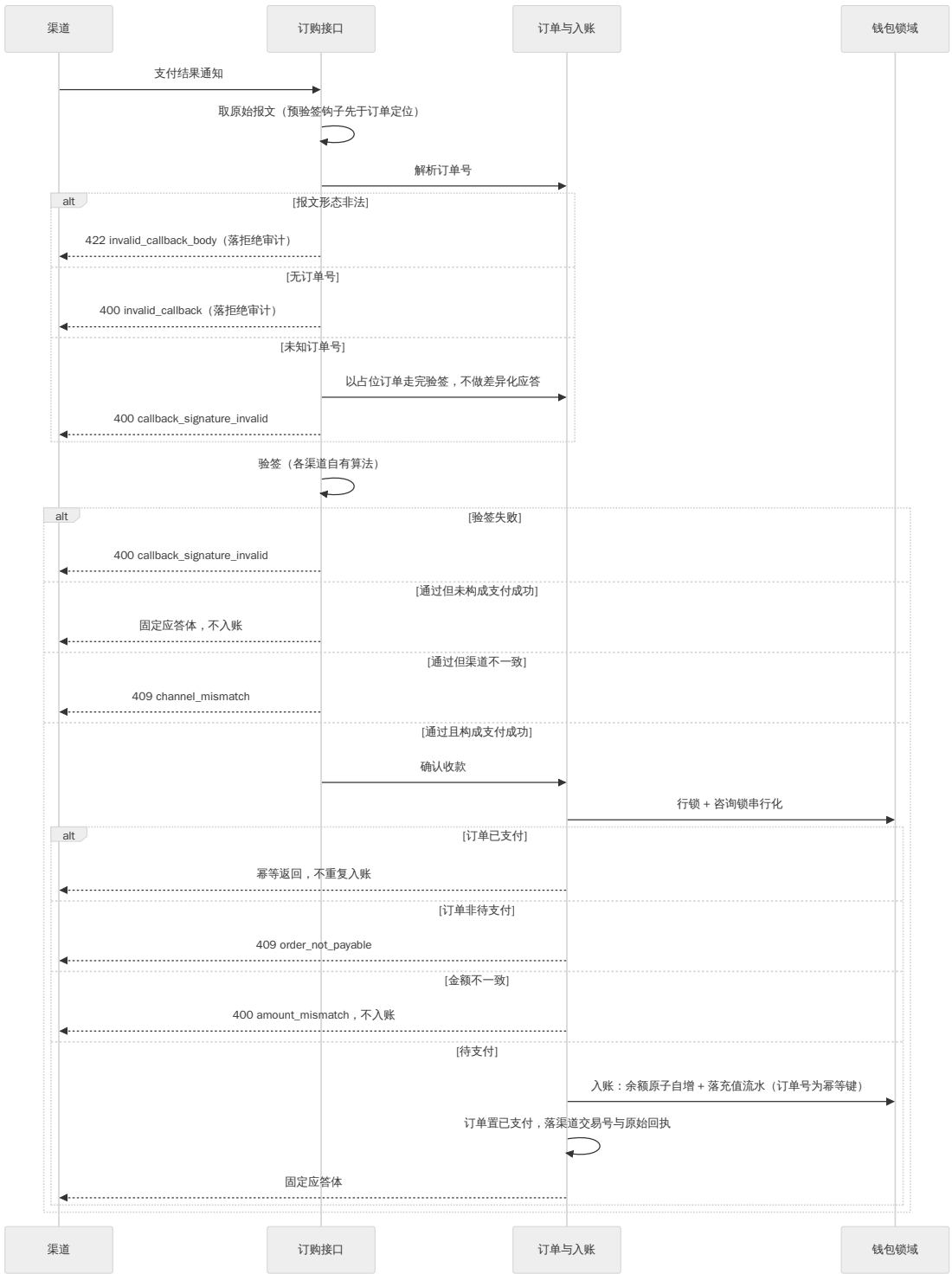


图 4

- 验签先于任何基于订单号的差异化应答：未知订单号与验签失败统一姿态，枚举订单号无法区分「订单是否存在」与「属哪个渠道」。
- 渠道一致性校验放在验签之后：验签已过说明报文确由该渠道签发，此时不匹配属配置或路由错误，用 409 而非探测语义。

- 入账的 DB 兜底：唯一索引使并发双入账在落库时显式冲突并收敛为幂等返回（非 500），本事务加款与流水整块回滚。
- 入账成功后同一请求内同步发布一次准入状态（充值是最主要解封路径），不另调异步发布以免重复事件。
- 拒绝姿态一律留痕（验签失败 / 报文非法 / 未知订单号探测），但审计写入失败绝不阻断拒绝应答。

4.3 订单超时自动关单

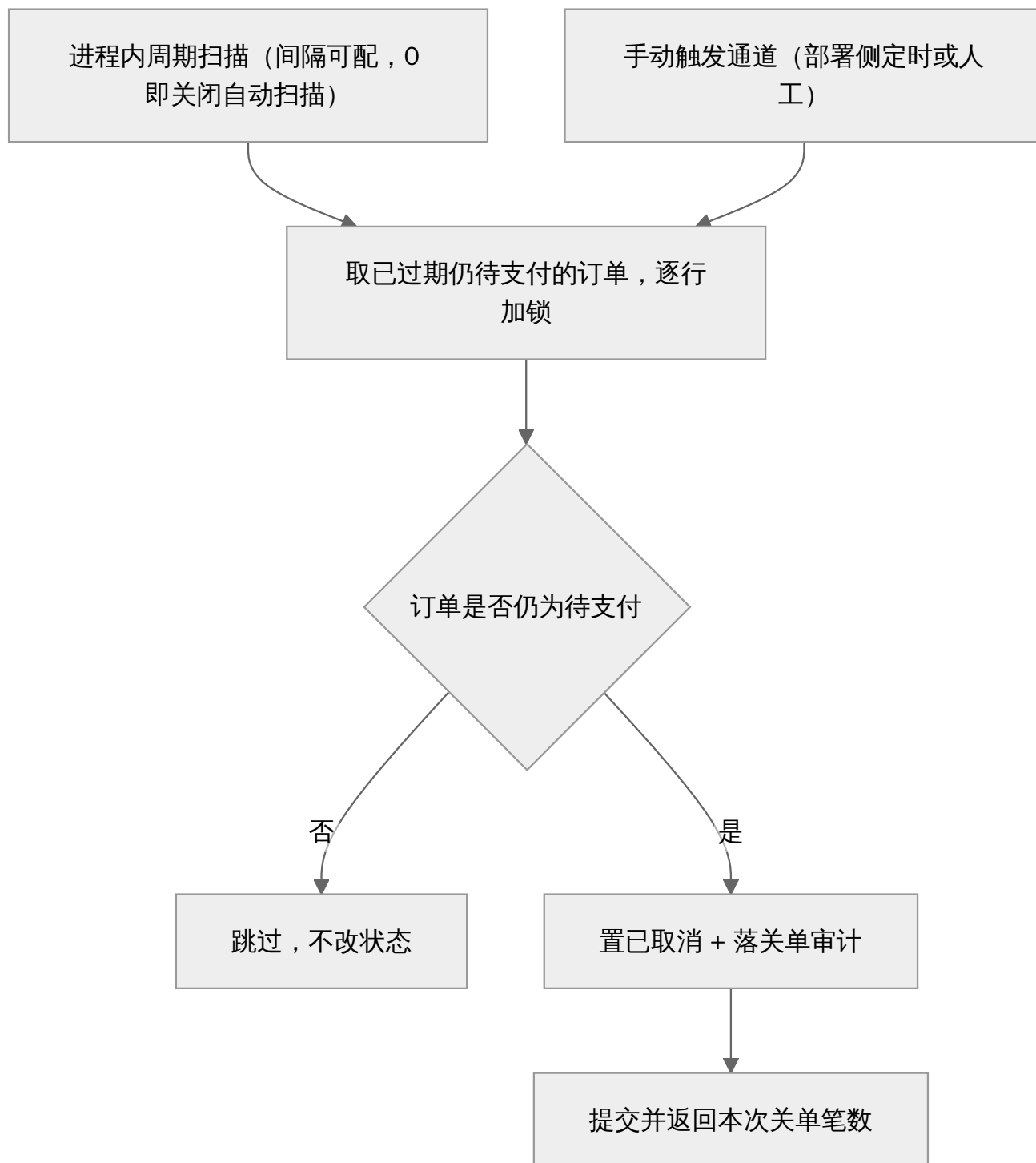


图 5

- 关单幂等：只改「待支付且已过期」的行，多副本并发触发安全；扫描用独立短会话与独立连接池，不随调用方事务回滚丢失，也不占业务请求的连接预算；单轮失败只记日志。

- 关单不是终局：渠道侧已完成收款的订单可由主动查单路径复活（见 4.4）。

4.4 主动查单自愈与已关单复活

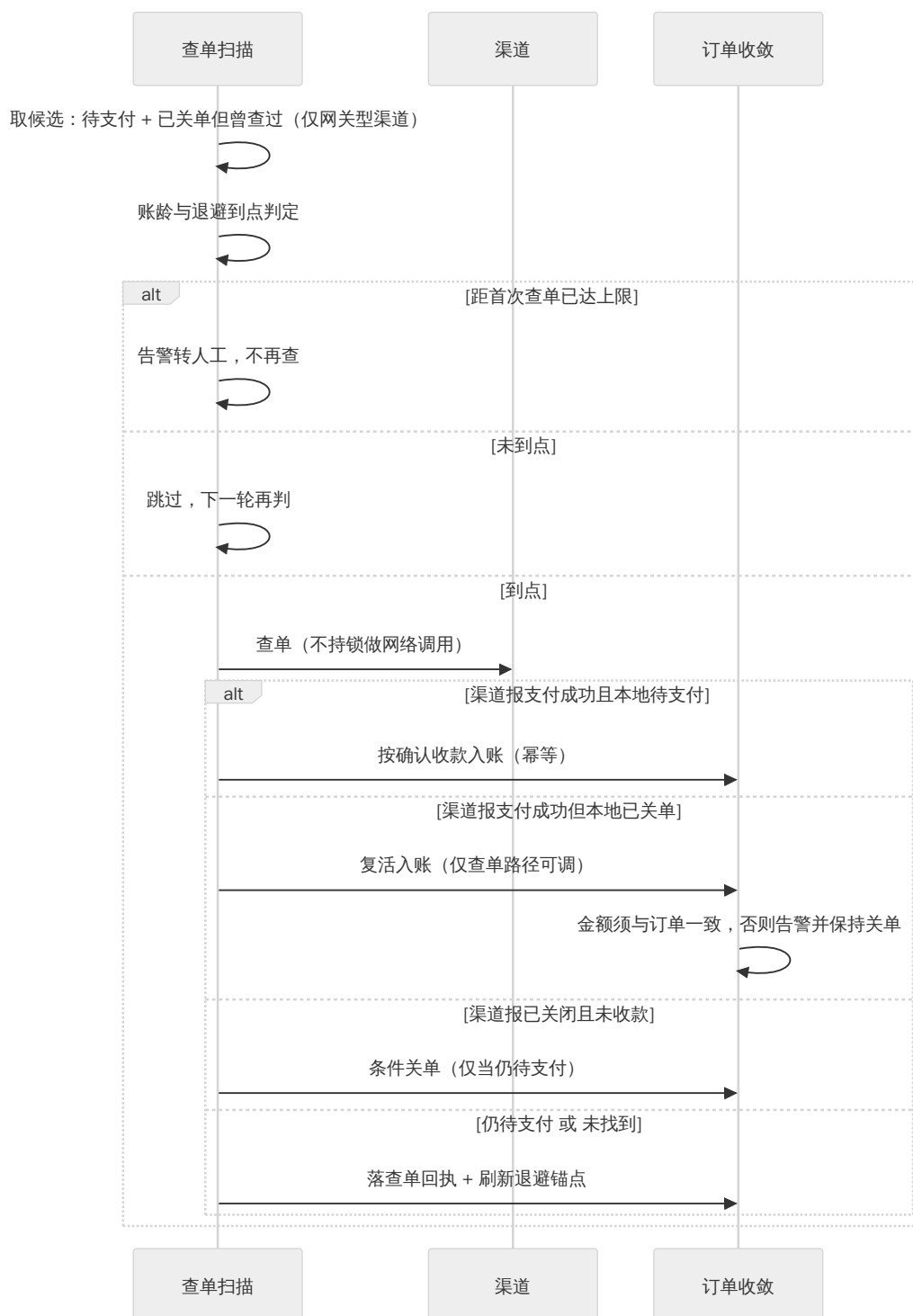


图 6

- 退避档位按账龄推进：前 60 分钟密查，之后 60 分钟一查，覆盖关单后的补偿窗口；自首次查单起 24 小时仍无法确认即告警转人工。
- 执行范式：无锁快照 → 锁外网络调用 → 收敛入口自行加锁；单笔异常不拖垮整轮，下轮重试。
- 条件关单只用「条件更新 + 状态判定在同一语句内完成」，不用「取锁后复检」：查单路径对象来自锁外快照，行锁不会刷新会话内陈旧对象，复检形同虚设。

- 复活只接受已关单态（超时关单），禁止从回调路径调用——回调可伪造；复活审计与「回调入账」「人工确认」三源可辨。运营可对单笔强制查一次（跳过退避）。

4.5 对公转账人工确认

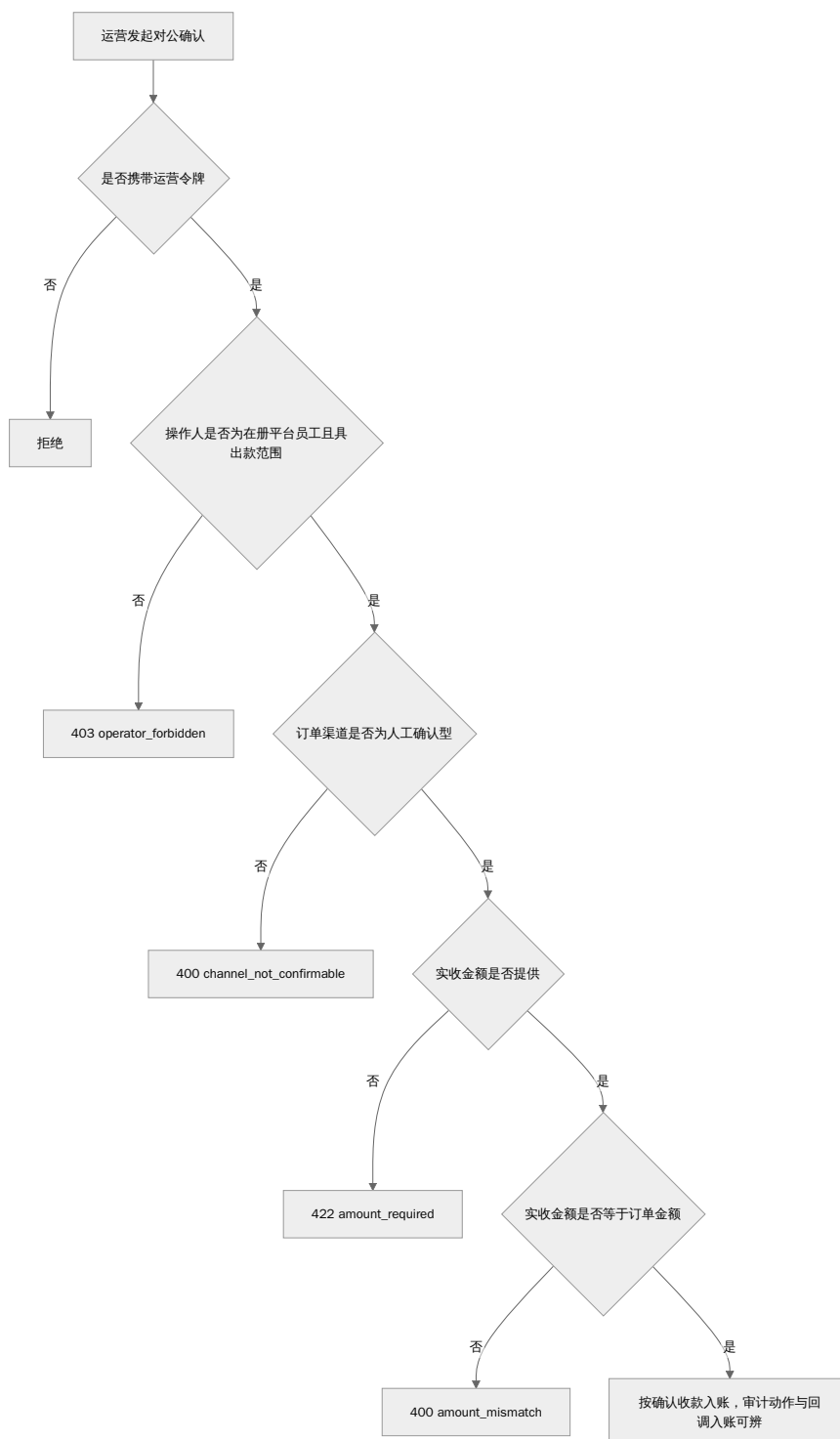


图 7

- 对公渠道无网关无回调，收款靠人工核对；确认端点与渠道回调共用同一条入账链路与同一幂等键。
- 两道门禁不可省：只允许人工确认型渠道（否则等于未收款先入账）；实收金额必填（否则比对被跳过而按订单金额直接入账）。

- 操作人门禁与退款审批同口径：必须是在册且具出款范围的平台员工，缺标识 / 标识非法 / 无绑定 / 已停用同一拒绝语义，不泄露绑定状态。

4.6 支付渠道生命周期：四道闸门与灰度

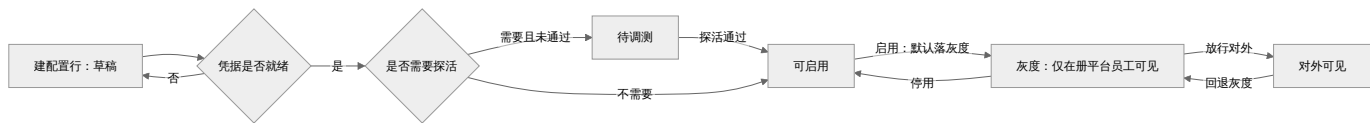


图 8

- 四道闸门：凭据就绪、调测完成（真实模式必过）、人工开关、灰度放行；四者齐备才对客户可见，判定只实现一次并在配置面、下单门禁、门户列表三处共用。
- 启用默认落灰度（fail-closed）：启用与对外是两次独立动作；放行对外需重验凭据与探活证据，回退灰度无条件允许。
- 派生生命周期状态只用于运营面徽标展示，不作门禁判定：判定走原始字段，避免派生状态与外部事实漂移。
- 每渠道至多一行启用（部分唯一索引）：启用某行时同渠道其他行在同事务内清零；删除启用行被拒绝，须先停用。

4.7 渠道凭据托管与探活证据

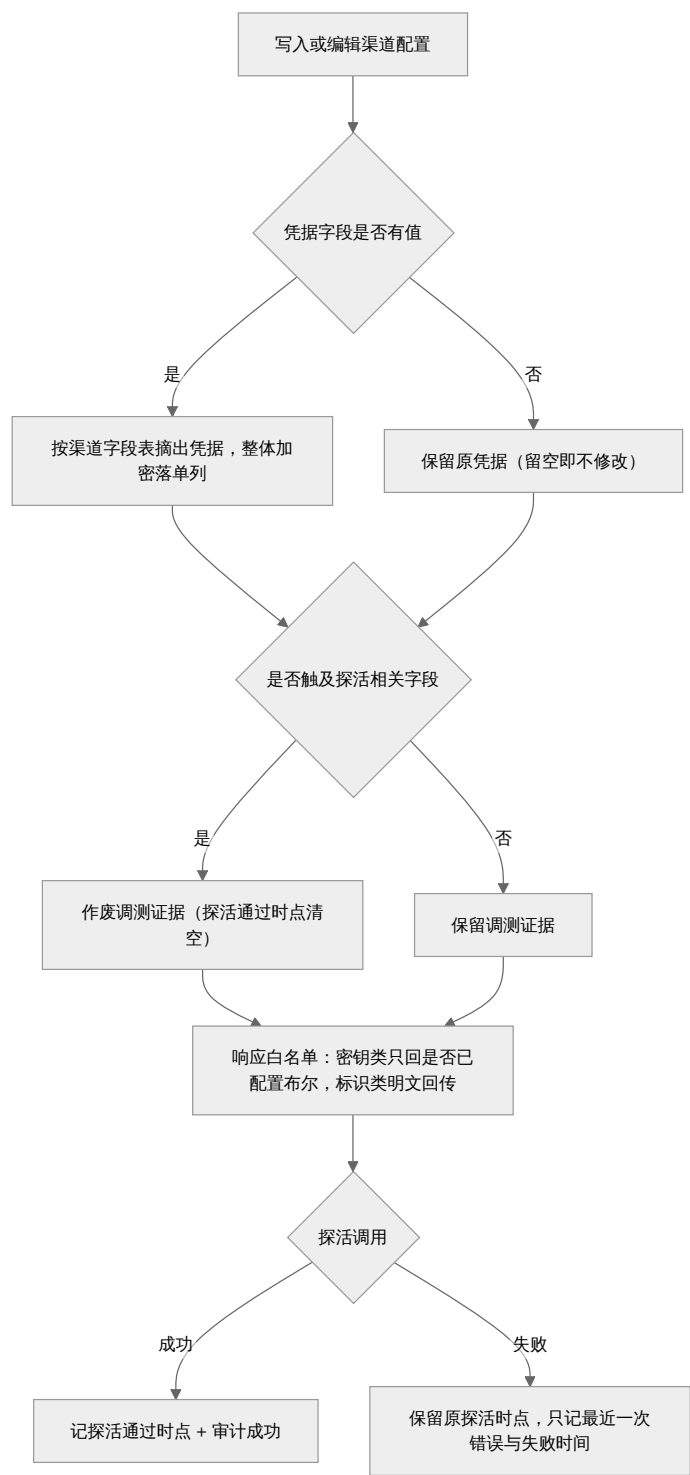


图 9

- 凭据读取只有一个入口：解密失败按「未就绪」处理（fail-closed），不上真实渠道；历史键名在该入口归一为规范名；写入字段表创建与编辑共用一份，防字段被静默丢弃。
- 探活相关字段集合是常量（模式、凭据、网关地址、通知与回跳地址、对公账户四要素）；触及任一即作废探活证据，防「改了密钥仍凭旧证据上线」。
- 探活失败不清空已有探活通过时点（网络抖动不应让已上线渠道被降级），但失败同样留痕（谁在何时试过、报了什么）。

- 人工确认型渠道无网关可探，「调测」等价于账户信息完整；模拟模式无真实网关可测。响应只出标识类字段与「是否已配置」布尔，密钥类明文永不回传。

4.8 售价版本与计价规则版本发布

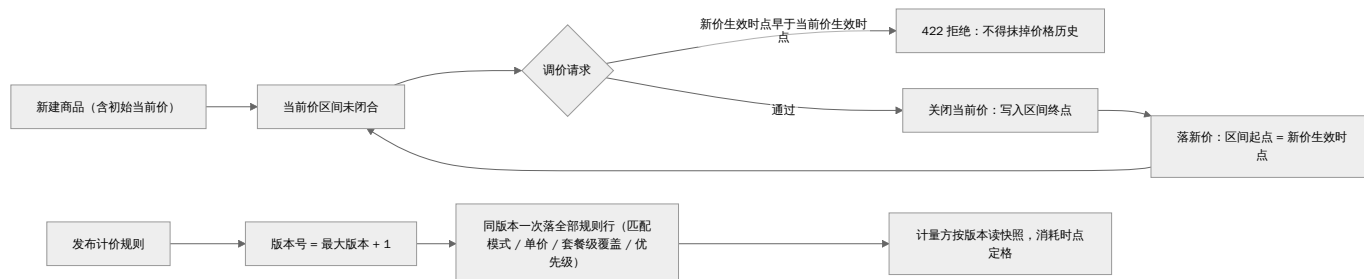


图 10

- 目录只展示当前价；历史售价经内部接口按区间回查，用于对账与公示。商品无当前价时下单拒绝（409），无价即不上架。
- 计价规则只按整版本发布，同版本内重叠命中取优先级高者；无匹配即未定价，计量方不产生费用。
- 本域只出单价规则、不参与扣费核算：扣费金额由计量方即算即传，账务扣减在钱包与账务域。

4.9 账户访问密钥生命周期与联动失效

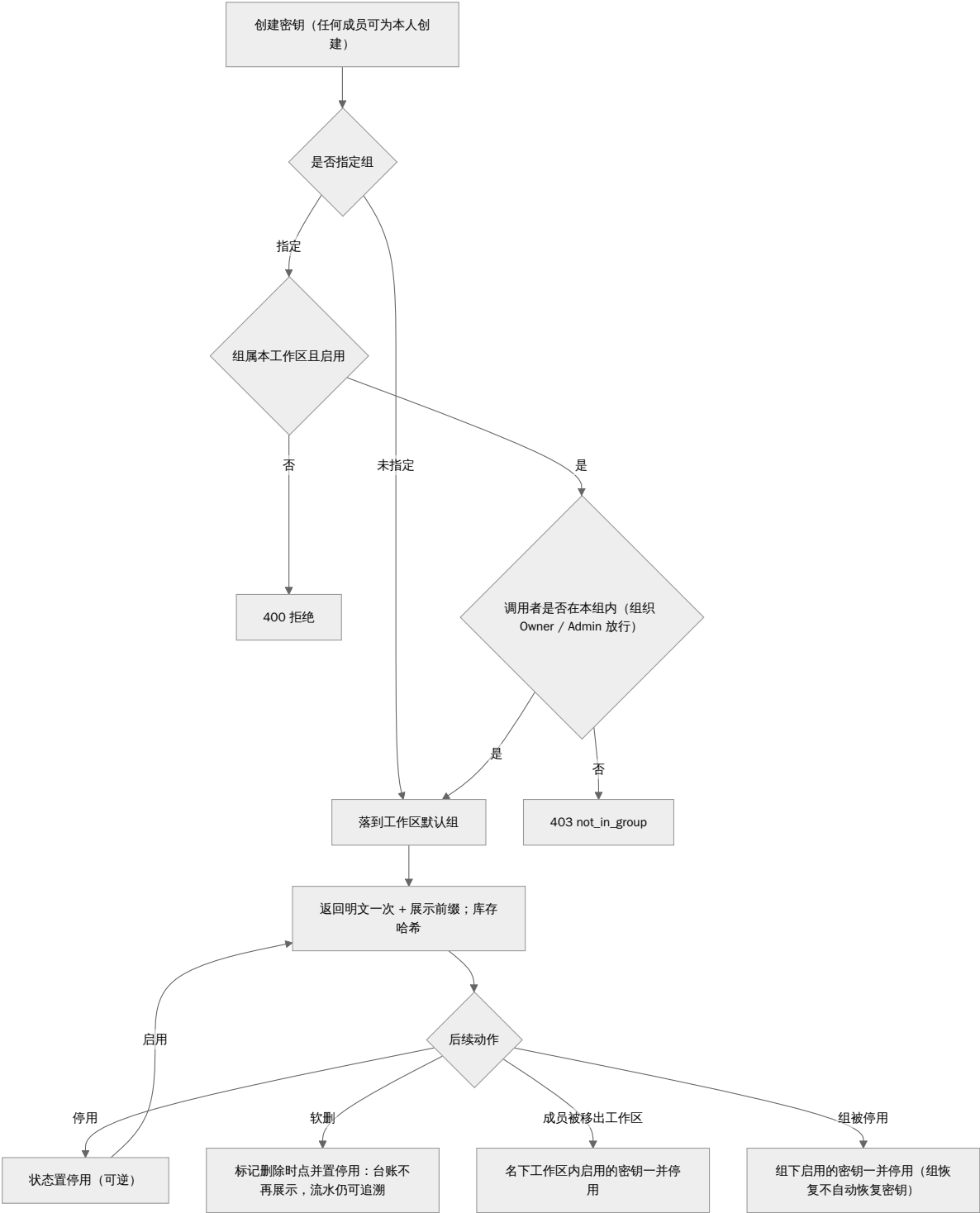


图 11

- 明文只出现在创建响应里一次，库内只存哈希与展示前缀；软删行视为不存在（明文现取校验返回未找到）。
- 额度多周期（`day` / `week` / `month` / `total`），缺省即不限，清空即回到不限；来源白名单逐项须为地址或网段、去重保序、上限 20 条，空列表即不限制来源。
- 临时密钥靠过期时点约束，过期即不可用；清空过期时点即转长期密钥。
- 联动失效是单向的：成员移出与组停用只做停用，组恢复启用不自动恢复密钥（避免「密钥显示可用却用不了」）；软删保流水追溯，不做物理删除。

4.10 订阅套餐账本与周期滚动

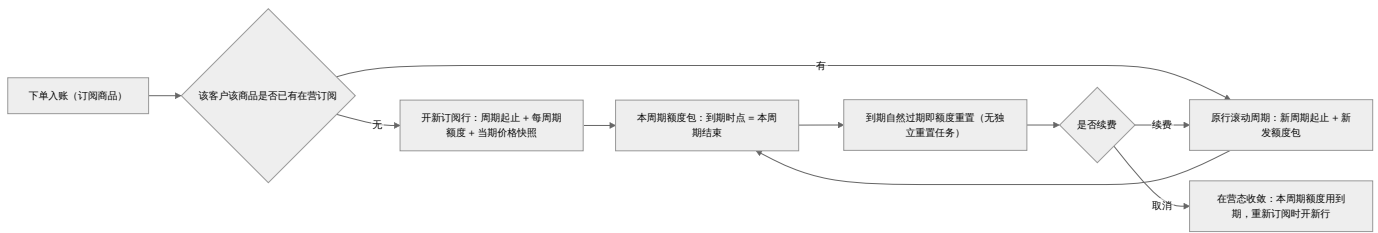


图 12

- 在营唯一性：每客户每商品至多一行在营订阅（部分唯一索引兜底）；取消让位后重新订阅开新行。
- 周期额度不做余额计数器：每周期新发一个额度包，剩余量由流水聚合得出；到期即过期，天然实现按周期重置。
- 周期天数、每周期额度、当期价格都在订阅行上快照，后续改价不回改已开订阅；取消后本周期额度用到期为止，取消原因留痕。

5. 接口契约

5.1 门户目录与渠道 (/api/account)

方法	路径	语义
GET	/api/account/products	公开目录：仅已上架商品，可按类型过滤
GET	/api/account/products/{code}	商品详情：未上架与不存在一律 404
GET	/api/account/price-rules	计费公示：仅当前有效版本；未发布返回空
GET	/api/account/pay-channels	当前用户可见渠道（含对公收款账户明文）

5.2 门户订购 (/api/account)

方法	路径	语义
POST	/api/account/orders	下单 → 待支付订单 + 支付参数；带意图幂等键时重复提交返回原单
GET	/api/account/orders	我的订单（时间倒序，最多 50 条）
GET	/api/account/orders/{order_no}	订单详情（字段白名单，不透渠道原始回执）
POST	/api/account/orders/{order_no}/refund-apply	申请退款（审批与出款详见 D07）
POST	/api/account/payments/callback/{channel}	渠道支付回调：验签优先 → 订单定位 → 渠道一致性 → 金额一致性 → 幂等入账

5.3 内部商品与定价 (/internal)

方法	路径	语义
POST	/internal/products	新建商品 + 初始当前价（充值面额须等于售价）
PUT	/internal/products/{code}	改规格与上架状态（编码与类型不可改）
POST	/internal/products/{code}/prices	新价格版本：关旧价区间 + 落新价
POST	/internal/price-rules	发布计价规则整版本
GET	/internal/products	管理列表（含未上架）：当前价
GET	/internal/products/{code}/prices	价格历史（区间回查）
GET	/internal/price-rules	计价规则版本快照（可按版本号读）

5.4 内部支付渠道（前缀 /internal/pay，下表为前缀内相对路径）

方法	路径	语义
GET	/status	当前生效支付模式与来源（配置行优先，部署配置兜底）
GET	/channels	配置列表（启用行在前；密钥类只回是否已配置）
POST	/channels	新建配置（不自动启用；同渠道同模式只能一条）
PATCH	/channels/{config_id}	部分更新：凭据留空不改；触及探活相关字段即作废调测证据
POST	/channels/{config_id}/activate	启用（同事务清零同渠道其他行；默认落灰度）
POST	/channels/{config_id}/rollout	灰度与对外切换
POST	/channels/{config_id}/deactivate	停用（幂等）
DELETE	/channels/{config_id}	删除配置（启用行拒绝，须先停用）
POST	/channels/{config_id}/probe	探活：只读查询验签，落库为调测证据

5.5 内部订单 (/internal)

方法	路径	语义
POST	/internal/orders/{order_no}/confirm	对公人工确认 → 已支付 + 入账
POST	/internal/orders/expire	超时关单（幂等，可重复触发）
POST	/internal/orders/poll	主动查单（幂等、自愈、多副本安全）
GET	/internal/orders	运营订单列表（可按状态筛选，含工作区名）
GET	/internal/orders/{order_no}	订单详情（含渠道原始回执）

- 同一前缀下的退款申请、审批、驳回、轮询与渠道对账端点属退款与对账域，详见 D07。

5.6 内部密钥现取校验 (/internal)

方法	路径	语义
POST	/internal/api-keys/lookup	哈希命中且未软删 → 台账（归属组与工作区、状态、额度、过期），不返回明文

- 鉴权为内部服务令牌的计量范围；状态与过期由调用方（数据面网关鉴权）决策，本端点只回答「是不是一把未软删的账户密钥」。封禁与解封属风控处置语义，详见 D09。

5.7 运营面 (/api/account/ops)

方法	路径	语义
GET	/api/account/ops/payments/status	生效支付模式与来源
GET	/api/account/ops/payments/channels	渠道配置列表
POST	/api/account/ops/payments/channels	新建配置
PATCH	/api/account/ops/payments/channels/{config_id}	编辑配置（凭据留空不改）
POST	/api/account/ops/payments/channels/{config_id}/activate	启用渠道
POST	/api/account/ops/payments/channels/{config_id}/rollout	灰度与对外切换
POST	/api/account/ops/payments/channels/{config_id}/deactivate	停用渠道
POST	/api/account/ops/payments/channels/{config_id}/probe	渠道探活
DELETE	/api/account/ops/payments/channels/{config_id}	删除渠道配置
GET	/api/account/ops/orders	运营订单列表
GET	/api/account/ops/orders/{order_no}	运营订单详情
POST	/api/account/ops/orders/{order_no}/confirm	对公人工确认（运营令牌路径）
POST	/api/account/ops/orders/{order_no}/query	单笔强制查单（跳过退避）
POST	/api/account/ops/orders/poll	整轮主动查单
GET	/api/account/ops/orders/refunds/offline-pending	待线下打款核对清单（详见 D07）
GET	/api/account/ops/orders/{order_no}/refund-risk	退款审批画像（详见 D07 与 D09）

- 运营面端点与内部端点共用同一组处理器（鉴权分别为门户令牌 + 运营配置范围、内部运营范围令牌）；出款类动作另加在册实人门禁。运营面端点索引表统一登记在 D11，本节只收主语义属本域的端点。

6. 关键约束与验收标准

6.1 约束

1. 单一幂等键入账：入账以 `order_no` 为幂等键、以 `recharge` 类型流水为唯一判据；重复回调、重复确认、查单收敛三源并发时净效果为恰好一次入账。
2. 验签优先且不泄露存在性：回调在任何基于订单号的差异化应答之前完成验签；未知订单号与验签失败同姿态；渠道一致性校验置于验签之后。
3. 非法迁移一律拒绝：只有待支付订单可转为已支付；已支付重复确认按幂等返回；其他状态一律拒绝，不产生状态回退。
4. 金额一致性硬门禁：回调与人工确认的金额必须与订单金额一致，不一致即拒绝且不入账；2 位小数口径由下单门的精度校验前置保证。
5. 关单与入账互斥：关单只在订单仍为待支付时生效，条件更新在单条语句内完成判定与写入，绝不覆盖在途入账结果。
6. 复活路径唯一：只有主动查单可复活已关单订单，且金额必须一致；回调路径不放开。
7. 渠道四闸门：凭据就绪、调测完成、人工开关、灰度放行四者齐备才可见可下单；启用与对外是两次动作；派生状态不作判定。
8. 凭据单向可写：凭据整体加密落单列，读取只有一个入口，解密失败按未就绪处理；响应只出标识类字段与「是否已配置」布尔，密钥类明文永不回传。
9. 探活证据随配置失效：触及探活相关字段即作废调测证据；探活失败不清空既有通过时点但必须留痕。
10. 密钥零明文与可逆停用：明文只在创建响应出现一次，库存哈希；停用与启用可逆；软删保留追溯；成员移出与组停用触发名下令牌一并停用，组恢复不自动恢复密钥。
11. 运营动作实人可追：入账与出款类动作必须带在册且有出款范围的操作人；申请与驳回类动作虽不设实人门禁，但操作人缺失必须显式落审计标记。
12. 价目只增不改：售价按区间追加、计价规则按整版本追加；任何路径都不得抹掉价格历史或改写已发布版本。

6.2 验收标准

#	验收口径
1	同一意图幂等键重复下单返回同一订单号，不产生新订单与新流水；并发同键提交仅落一行
2	不带意图幂等键的下单撞订单号时自动重试，多次撞号后仍失败才抛冲突，不出现以撞号为由的 500
3	同一订单重复回调仅首次入账，其后幂等返回当前余额；余额取已提交真值，并发双充值下响应余额含本笔
4	回调金额与订单金额不一致 → 拒绝且余额不变；对公确认实收金额不一致 → 拒绝且余额不变
5	未知订单号的回调与签名错误的回调应答姿态一致；渠道不一致的回调被明确拒绝
6	已支付订单再收回调 → 幂等返回；已取消订单收回调 → 拒绝（不复活），由查单路径处置
7	超时关单只改写已过期的待支付订单；关单后渠道确认收款的订单可被复活入账，金额不一致时保持关单并告警
8	关单扫描多副本并发不产生重复关单审计；关闭自动扫描后手动触发仍可用
9	渠道未启用 / 凭据不全 / 未探活 / 灰度未放行时，既不出现在门户列表也不可下单（同一份判定）

#	验收口径
10	启用渠道默认落灰度：非在册员工看不到；放行对外后普通用户可见；回退灰度后立即不可见
11	同渠道启用新行时旧行自动停用；不同渠道可同时启用；启用行删除被拒绝
12	修改密钥类凭据后调测证据被作废，渠道回到待调测态，无法直接放行对外
13	渠道配置响应中密钥类字段只出现「是否已配置」布尔，不出现明文；对公收款账户为明文
14	密钥创建响应含明文一次，此后任何查询都不返回明文；软删后现取校验返回未找到，流水仍可追溯
15	密钥额度按多周期生效，缺省即不限；来源白名单超过 20 条或含非法项 → 拒绝
16	成员移出工作区后其名下工作区内启用的密钥全部停用；组停用后组下启用的密钥全部停用，组恢复后密钥仍为停用
17	调价后新下单按下单时当前价定格；历史价格可按区间回查；新价生效时点早于当前价生效时点被拒绝
18	计价规则按整版本发布，同版本重叠命中取优先级高者；未发布时公开公示返回空
19	同客户同商品的并发订阅开通至多一行在营订阅；取消后可重新订阅开新行
20	运营令牌缺失或操作人非在册平台员工时对公确认被拒；非人工确认型渠道被拒；实收金额缺失被拒

6.3 待后续设计细化的开放项

- 1. 订阅的开通与续费入口编排：周期滚动、取消与重新订阅的行级约束已定，门户侧入口与文案编排待与其他页面统一。
- 2. 渠道对账的订单侧视图：本域只出订单与渠道配置，账单比对在退款与对账域；跨域差异处置口径需两侧联合定稿。
- 3. 密钥额度在执行侧的落点：额度字段与口径在本域，扣减时的额度判定归属待与计量与计费域对齐（当前扣费只按金额扣钱包）。
- 4. 计价规则的套餐级覆盖：字段已就位，套餐级单价的生效范围与切换时机待与计量与计费域共同细化。
- 5. 渠道凭据轮换：密钥经环境注入、凭据整体加密；轮换期双写与历史密文重加密策略待定。