

D12 用户自助与门户域 · 设计文档

本域总览见《账号计费中心 · 结构大纲》。本文为该域完整设计：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：终端用户面对账号计费中心的唯一自助面与编排层。它把各能力域已落定的事实——现金余额、赠金额度、信用额度、用量与费用、订单与退款进度、站内信、组织与成员关系——装配成两套工作区视图（个人空间 / 企业空间），并把用户意图（充值、邀请、退出组织、重签协议、设置余额告警阈值）翻译为对能力域端点的调用。本域不产生新事实，只回答四件事：取谁的事实、在哪个工作区上下文取、以什么形态呈现、用户动作该调谁的端点。全文顺序即数据模型（事实结构来自上游）→ 核心流程（运行路径）→ 接口契约（对外投影）。

关键口径

口径	内容
事实来源	门户只读其他域的表与端点；本域不建表、不写钱、不实现资金与计量口径
金额传输	一律元、6 位小数、字符串；余额与订单类展示 2 位小数，流水与费用类展示 6 位小数
欠款判定	唯一未偿债务真相 = 现金余额为负（ <code>cash_balance</code> 小于 0）；不读欠费派生标记，不读实时可用额度
工作区上下文	企业工作区请求携带组织上下文请求头，空值由后端回退企业优先；同一组件在两套路径族下复用，凭据与余额互不可见
令牌	访问令牌与刷新令牌由账号与身份域签发（详见 D01），门户只使用与续签

边界

- 不管钱：现金余额、赠金、信用额度与流水的记账在钱包与账务域（D04），本域只读。
- 不管计量与计价：用量聚合与账单口径由计量与计费域（D05）实现，门户复用同一聚合函数。
- 不管订单状态机与退款：订单创建、回调验签、退款工单在订购与支付域（D03）、退款与对账域（D07）。
- 不管组织与成员语义：组织、成员关系、组与邀请的写语义在账号与身份域（D01）；本域只写入口与编排边界。
- 不管站内信生成与投递：落表与短信、邮件触达在通知与触达域（D10）；本域只读列表、已读与阈值设置。
- 不管协议版本与运营面：协议版本与重签判定在风控与合规域（D09）；平台侧页面与运营端点索引在 D11。

2. 角色与依赖

能力矩阵

能力	本域	钱包与账务域	计量与计费域	订购与支付域	通知与触达域	账号与身份域
余额 / 赠金 / 额度展示	✓	✓	✗	✗	✗	✗
用量 / 账单 / 费用构成展示	✓	✗	✓	✗	✗	✗
充值下单与支付回跳	✓	✗	✗	✓	✗	✗
订单列表 / 详情 / 退款入口	✓	✗	✗	✓	✗	✗
组织 / 成员 / 组 / 邀请入口	✓	✗	✗	✗	✗	✓
站内信读取与已读、告警阈值设置	✓	✓	✗	✗	✓	✗
协议重确认门禁	✓	✗	✗	✗	✗	✓
工作区上下文解析	✓	✗	✗	✗	✗	投影

门户角色的可见性与禁用口径

角色	工作台	费用中心与订单	组织与部门组	消息中心
个人用户	个人工作台	可见	仅创建或加入组织的入口	个人消息中心
所有者	企业工作台	可见	成员与邀请、部门组、企业信息全可见	企业消息中心
管理员	企业工作台	可见	同上	企业消息中心
成员	企业工作台	不出现	部门组与企业信息可见；成员与邀请不出现	企业消息中心

- 菜单可见性由工作区角色驱动：未声明角色的菜单对所有工作区可见，声明角色的菜单按当前工作区角色过滤；角色判定同时作用于菜单渲染与路由拦截，避免「菜单不显示但路径可达」。角色映射是纯函数（工作区形态 + 组织内角色 → 菜单角色），工作区落定即重算并双写内存与本地缓存，避免「菜单已换、判断仍用旧角色」。
- 操作级权限不止于菜单：邀请、改成员角色、移除成员只对所有者与管理员开放；角色变更另有「不得越权改同级别或更高角色」的判定，越权由服务端拒绝并回以角色不足的错误码。

上游依赖

上游域	依赖内容	语义
钱包与账务域	钱包端点、流水分页与导出口径	余额卡与流水表的事实源
计量与计费域	用量聚合、分页下推、组织透视维度	页面查询、导出、组织透视三处同源
订购与支付域	商品与价格、渠道可见性、下单与订单查询	充值入口与订单记录的取数面
账号与身份域	工作区列表与组织投影、资料、安全日志、邀请与组	上下文解析与账号设置的取数面
风控与合规域	协议版本与重签要求、实名状态	重确认门禁与实名入口的判定输入

本域被引用 / 被进入面（邀请链接接收者经入站页消费邀请码并调用接受邀请端点）

引用方	引用内容	语义
统一登录服务	登录后的深链回跳参数	回跳保留原查询参数，登录后落回原意图页面
支付渠道收银台	浏览器回跳与本域支付结果页	回跳参数只用于定位订单，支付结果以订单查询为准

3. 数据模型

本域无自有表。事实载体有两类：其他域的表（客户、流水、赠金、用量、订单、站内信、组织与成员、组、用户与凭证、操作留痕）与其他域的端点（自助读写所依赖的能力出口）。本域对前者一律只读，对后者只做调用与编排。

3.1 域内关联总览

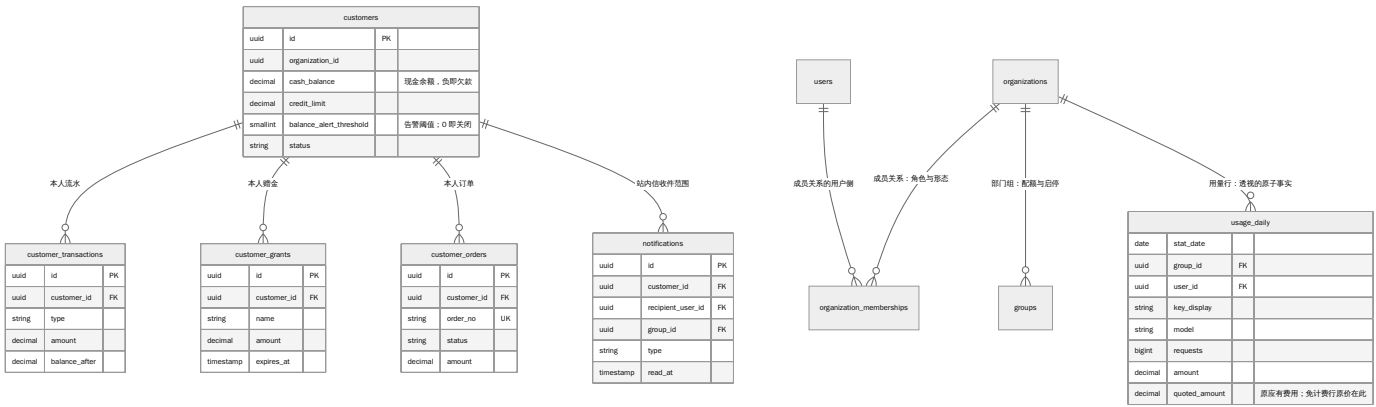


图 1

3.2 域间引用

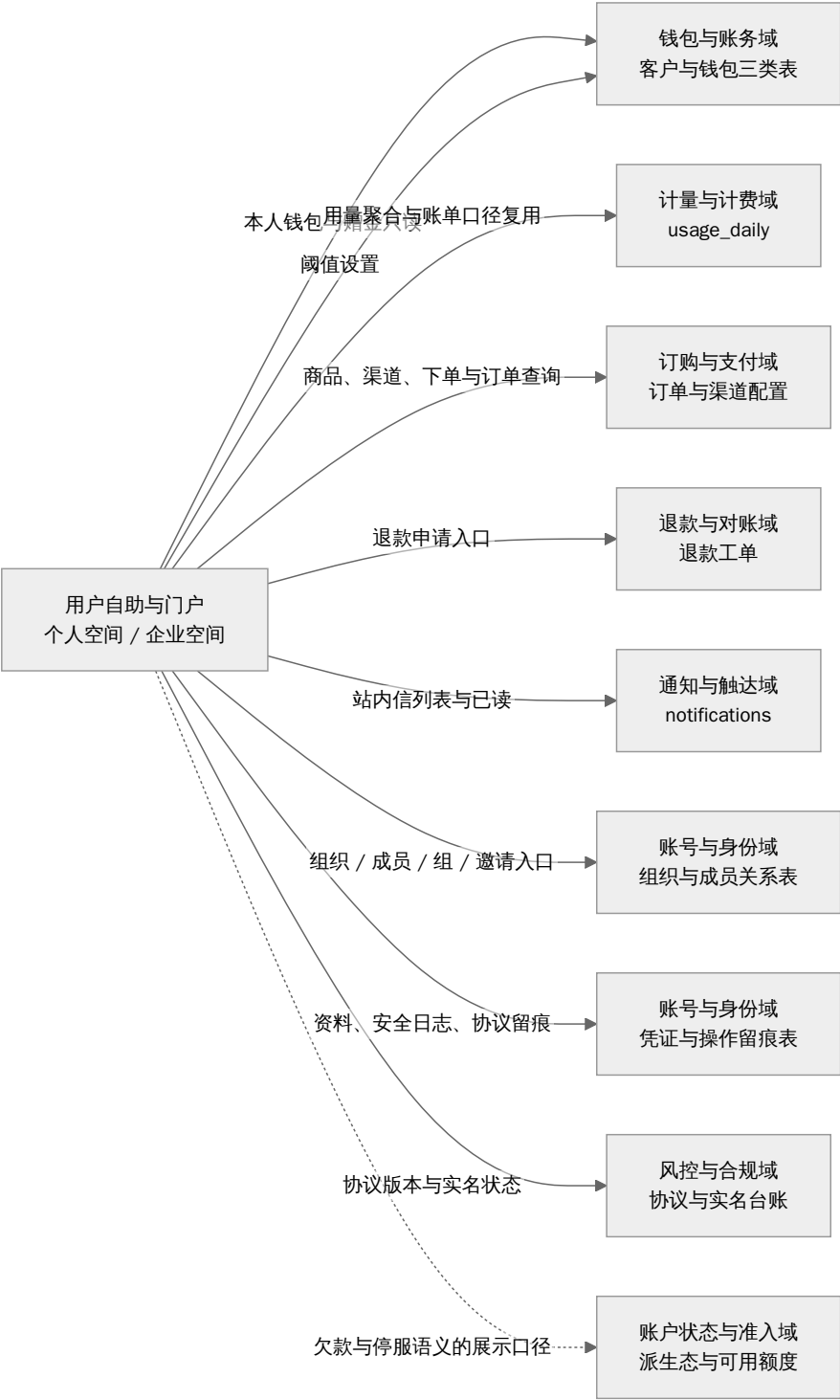


图 2

- 门户与上游是单一方向：读事实、调动作，没有一条上游依赖门户的数据。
- 欠款只看现金余额符号，派生态与可用额度只用于展示与文案（宽限中不得报停服）。

3.3 表清单（本域无自有表，只读下列 12 表）

表	归属域	本域读取的关键列
customers	钱包与账务域	cash_balance / credit_limit / balance_alert_threshold / organization_id / status
customer_transactions	钱包与账务域	type / amount / balance_after / ref_order / detail / created_at
customer_grants	钱包与账务域	name / amount / expires_at
usage_daily	计量与计费域	stat_date / model / key_display / group_id / user_id / requests / amount / quoted_amount
customer_orders	订购与支付域	order_no / status / amount / created_at
notifications	通知与触达域	type / title / content / read_at / recipient_user_id / created_at
organizations	账号与身份域	name / status / real_name_status
organization_memberships	账号与身份域	organization_id / user_id / role / org_kind
groups	账号与身份域	name / status / is_default
users	账号与身份域	display_name / avatar_url
user_credentials	账号与身份域	credential_value / is_primary
operation_logs	账号与身份域	action / created_at

3.4 设计约束

1. 本域零写入：不建表、不建列、不落派生缓存；展示值一律来自上游端点返回。
 2. 金额一律字符串：端点返回与前端传递均为元字符串、最多 6 位小数；前端不得先转浮点再比较，欠款判定按原始值符号进行。
 3. 窗口收敛与分页下推：用量与流水默认窗为最近 30 天、结束日不早于开始日，违规由服务端以日期序错误码拒绝；分页先计数再取页，不得把全量聚合拉入内存后切片。
 4. 字段白名单：流水不下发内部账务键，只出时间、类型、金额、交易后余额、订单号、备注与模型；备注中的内部原因编码必须翻译为可读文案后才下发。
 5. 收件范围两分：可见集合 = 当前工作区组织级（收件人为空） $\cup$ 本人个人收件；个人收件已读按收件人隔离，组织级已读成员共享。
 6. 工作区选择按账号隔离持久化：选择键携带账号标识，退出登录保留、账号之间不交叉；旧版无账号归属的键不再读取并一次性清理。
 7. 可用额度不参与欠款判定：可用额度 = 现金 + 赠金 + 信用额度，是准入额度；耗尽不构成未偿债务。
 8. 协议门禁以服务端留痕为准：重确认要求来自服务端下发的标记，本地标记仅用于弹窗展示与关闭。
-

4. 核心流程

4.1 门户信息架构与工作区落点解析

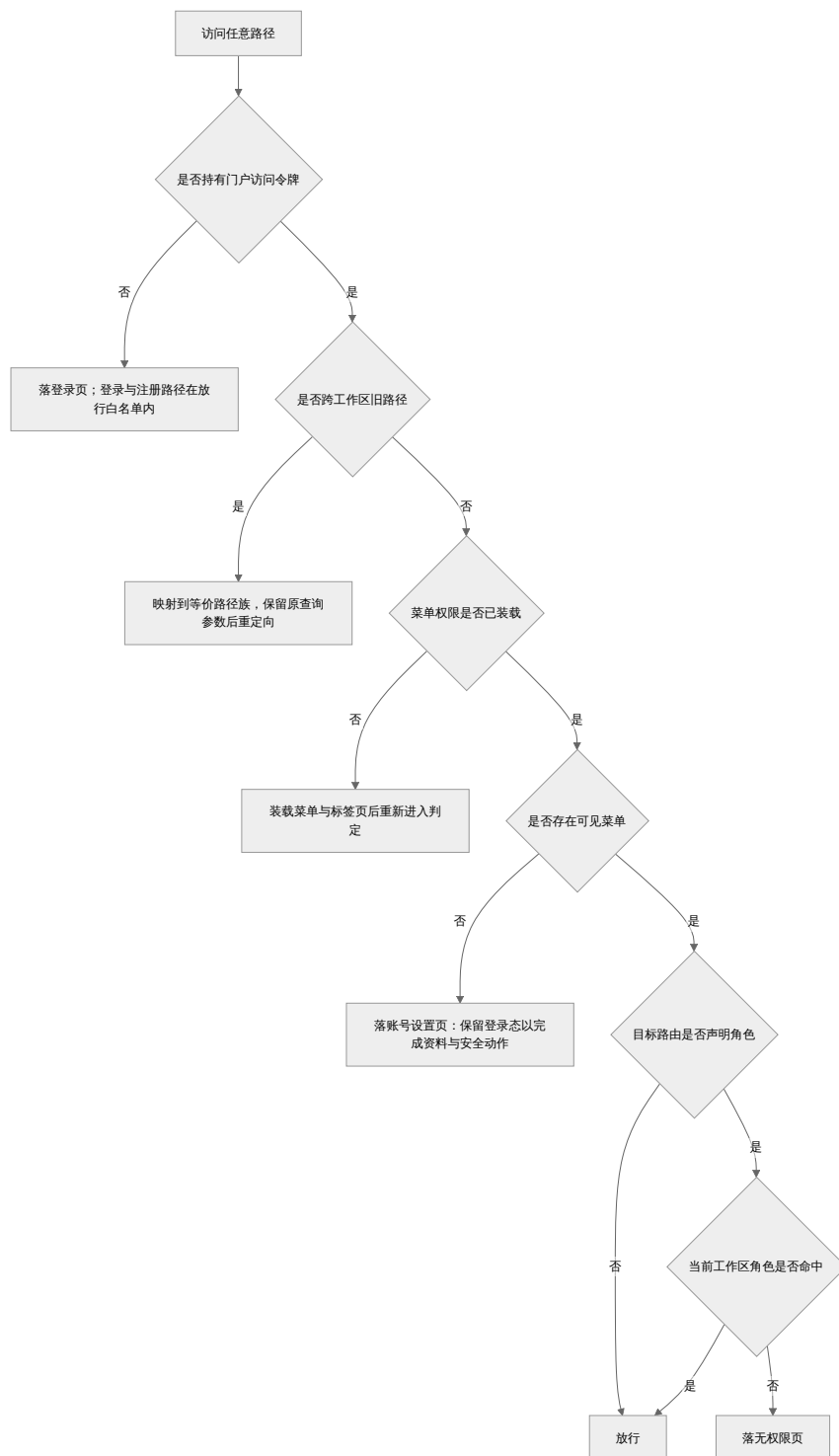


图 3

- 落点规则即四种情形的唯一答案：未登录落登录页（白名单路径除外）；无可见工作区落账号设置页且不清令牌；单工作区按后端回退口径直接落其首页；多工作区默认选最近使用、无活跃记录时回退最近加入的企业，仍无企业则落个人空间。
- 跨工作区旧路径的映射是纯函数：输入目标路径与查询参数、输出等价路径与查询参数（或空表示无需重定向），不依赖组件实例，可直接单测；映射先于角色拦截执行，避免旧链接被无权限页接收。

- 组织专属页（成员、部门组、企业信息）无个人等价物，反向映射一律回落个人工作台，避免死链。

4.2 工作区切换与菜单重建

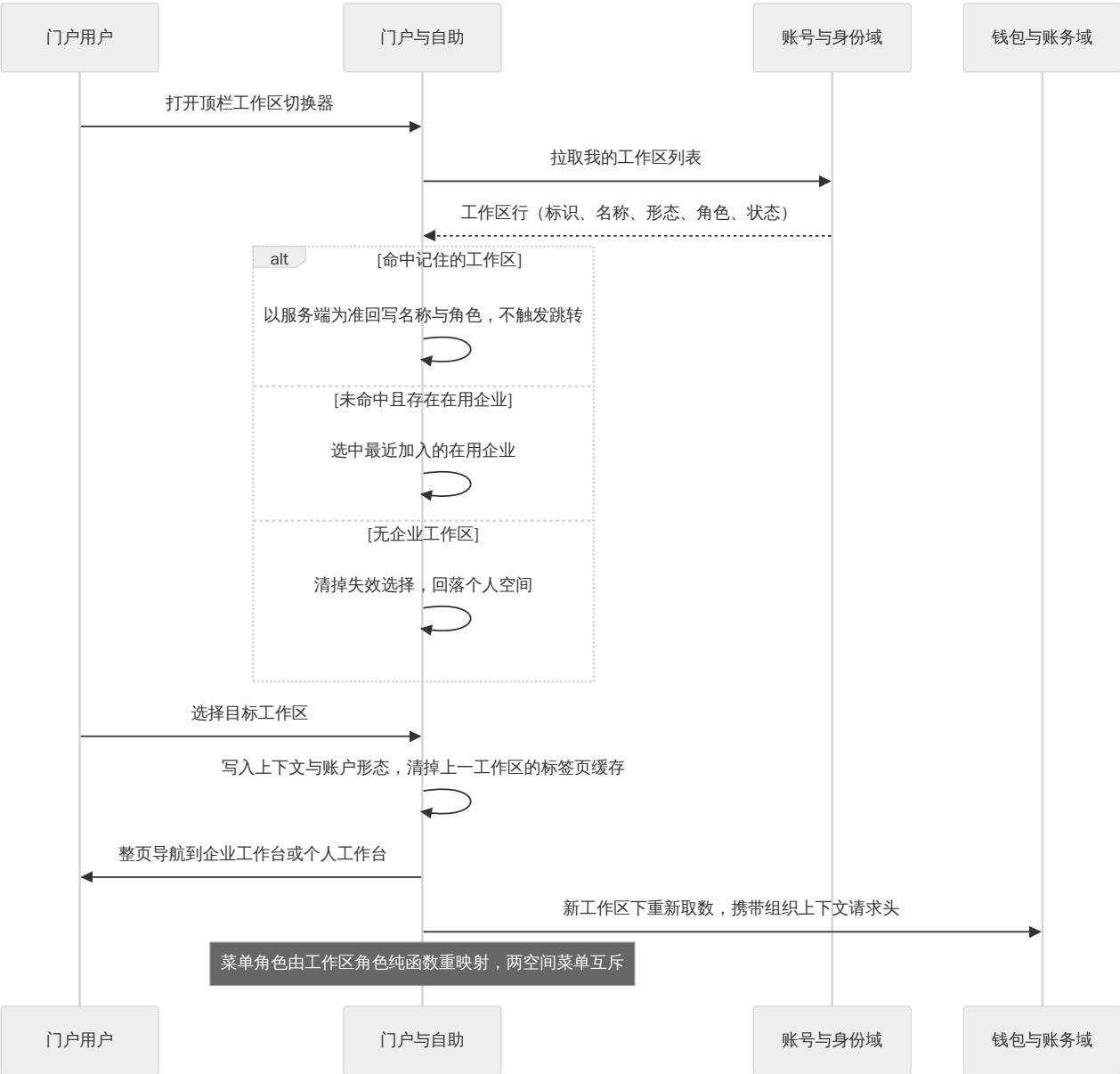


图 4

- 切换后整页导航：菜单树与标签栏都必须按新工作区重建，上一工作区的标签在此工作区即死链，故先清缓存再导航。
- 个人与企业首次切换时给出一次性告知：两个空间的余额、凭据与用量相互独立，个人资产不会丢失（按账号每设备仅首次弹出）。

4.3 工作台取数与两形态差异

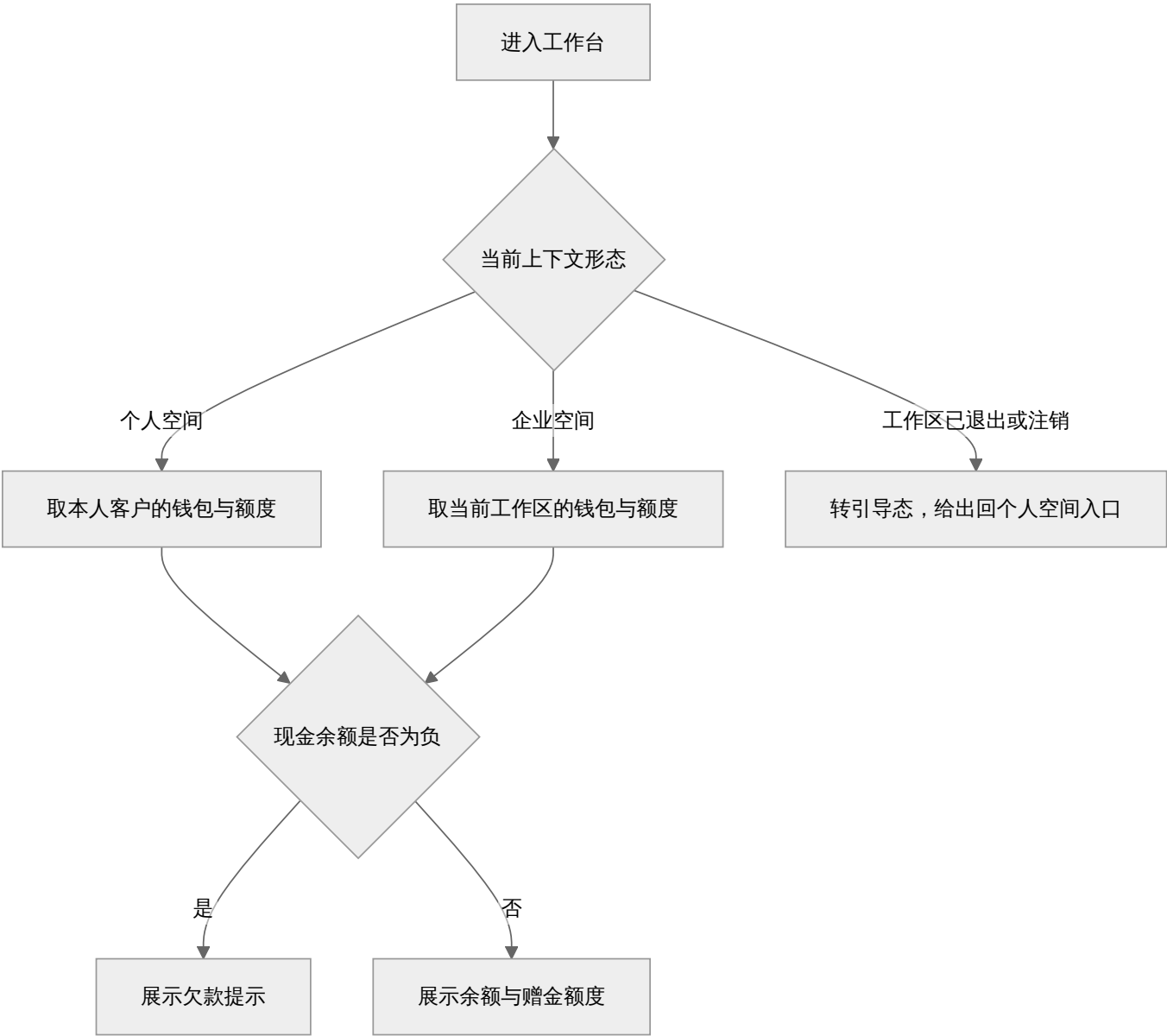


图 5

- 两张工作台共用同一个钱包端点，差异只在上下文：个人工作台取本人客户的钱包，企业工作台取当前组织的钱包，两者金额互不叠加。
- 欠款口径统一为现金余额为负；工作区不存在（被退出或注销）时页面转为引导态而非报错，并给出回个人空间的路径。

4.4 费用中心的四类面板取数

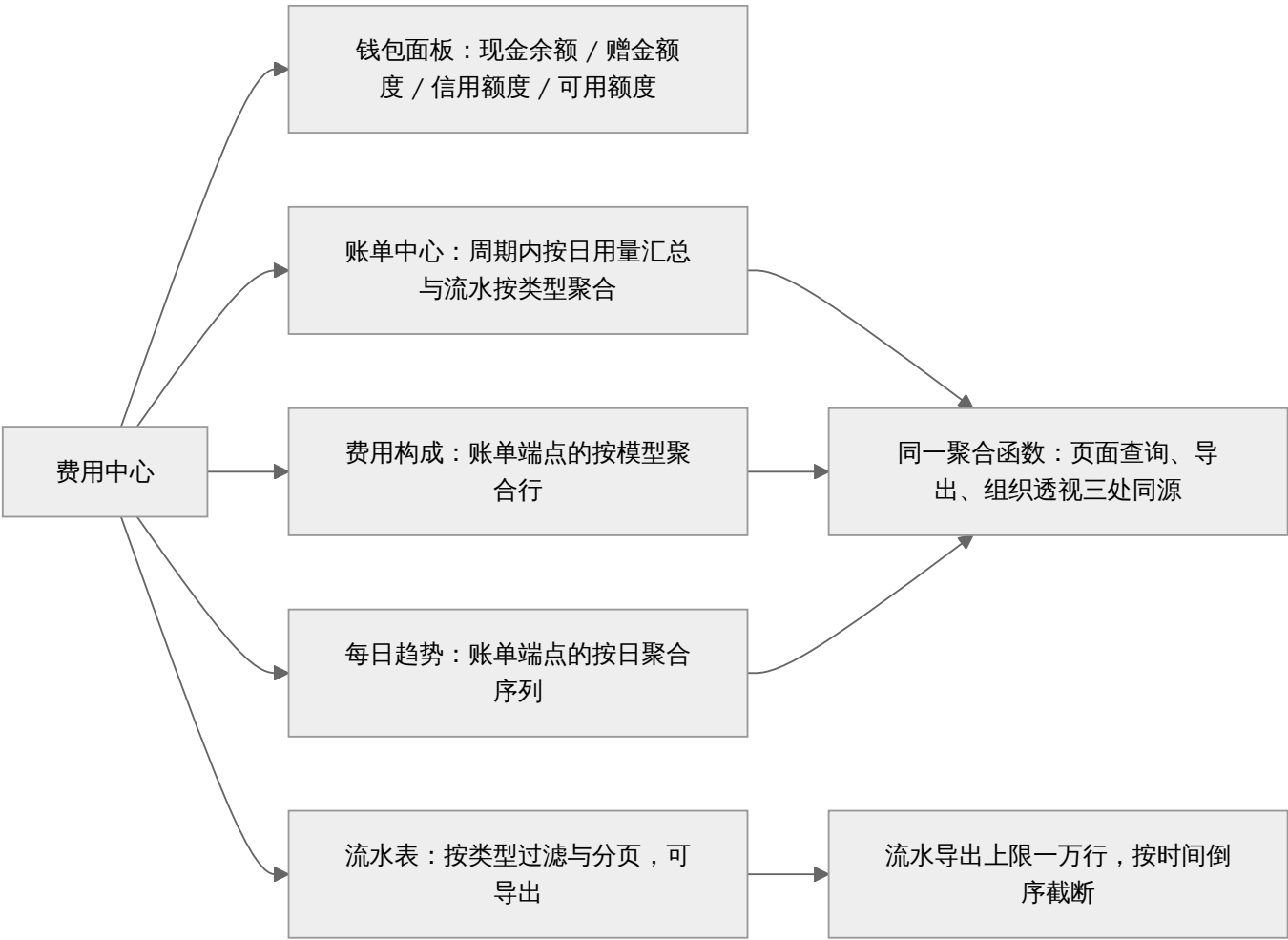


图 6

- 账单端点是一次请求三类结果：按日用量汇总（量对得上）、流水按类型聚合（钱对得上）、按模型聚合（费用构成）；每日趋势与费用构成复用同一过滤口径。
- 用量行带两个金额：实收费用与原应有费用（免计费行为零，原价另列），据此区分「用了多少」与「本该付多少」。
- 组织透视按维度组合（日期、组、成员、凭据展示名、模型）分组并支持导出，导出按用户可读名称列出行。

4.5 充值下单与支付回跳

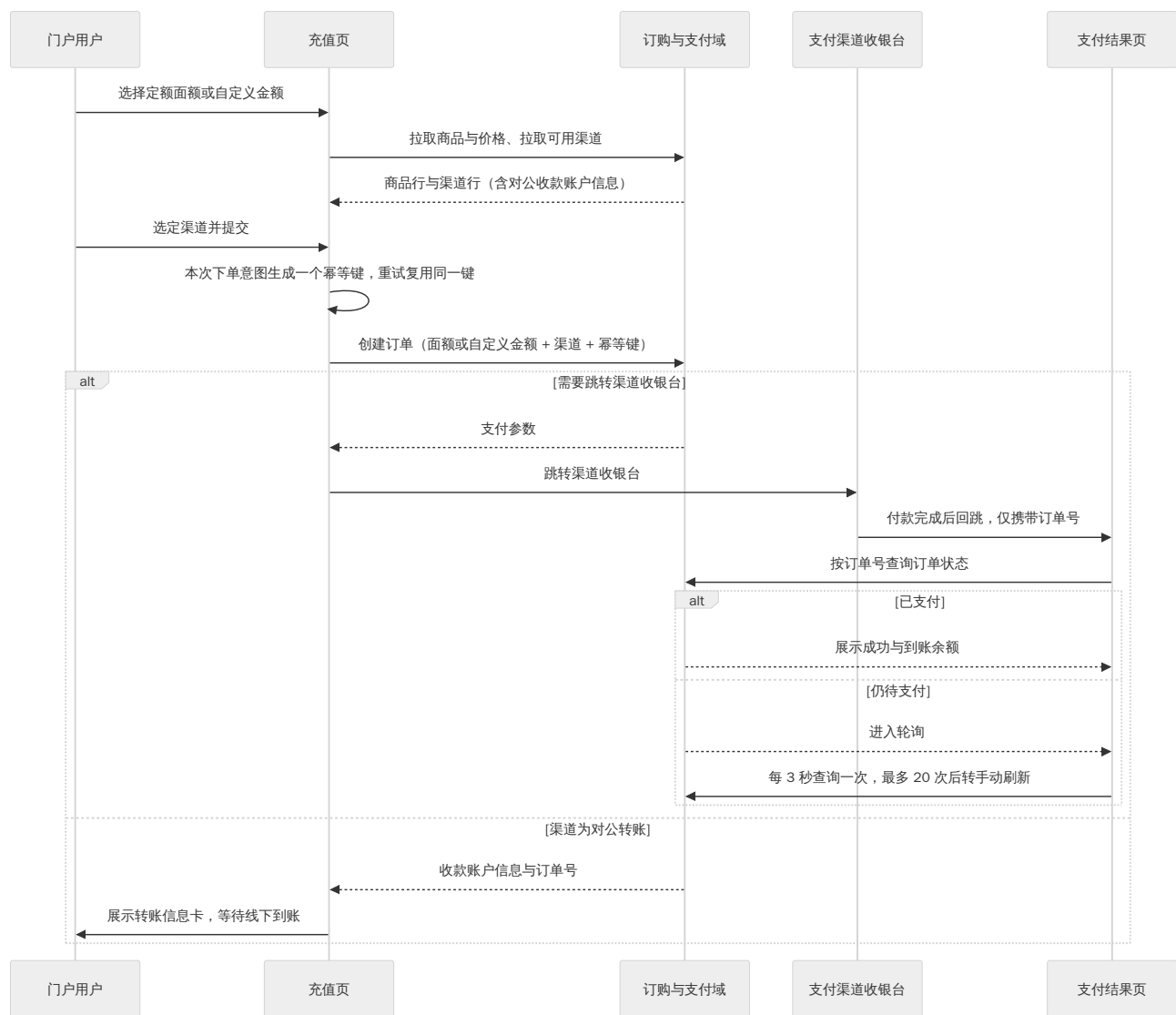


图 7

- 自定义金额与定额面额共用一次下单意图；意图变更（换渠道、换面额、改金额）即作废幂等键，防止「改了金额却拿到旧单」。
- 支付结果页不信任任何回跳参数：回跳只取订单号用于定位，入账一律由服务端渠道回调验签完成；页面状态完全由订单查询结果决定，查询失败单独成态并给重试；结果页四态为已支付、待支付、失败、订单不存在。
- 渠道列表由后端按四道闸门（凭据齐备、探活通过、已启用、灰度放行）下发，门户不硬编码渠道，杜绝「点了才被拒」。

4.6 订单记录与退款入口

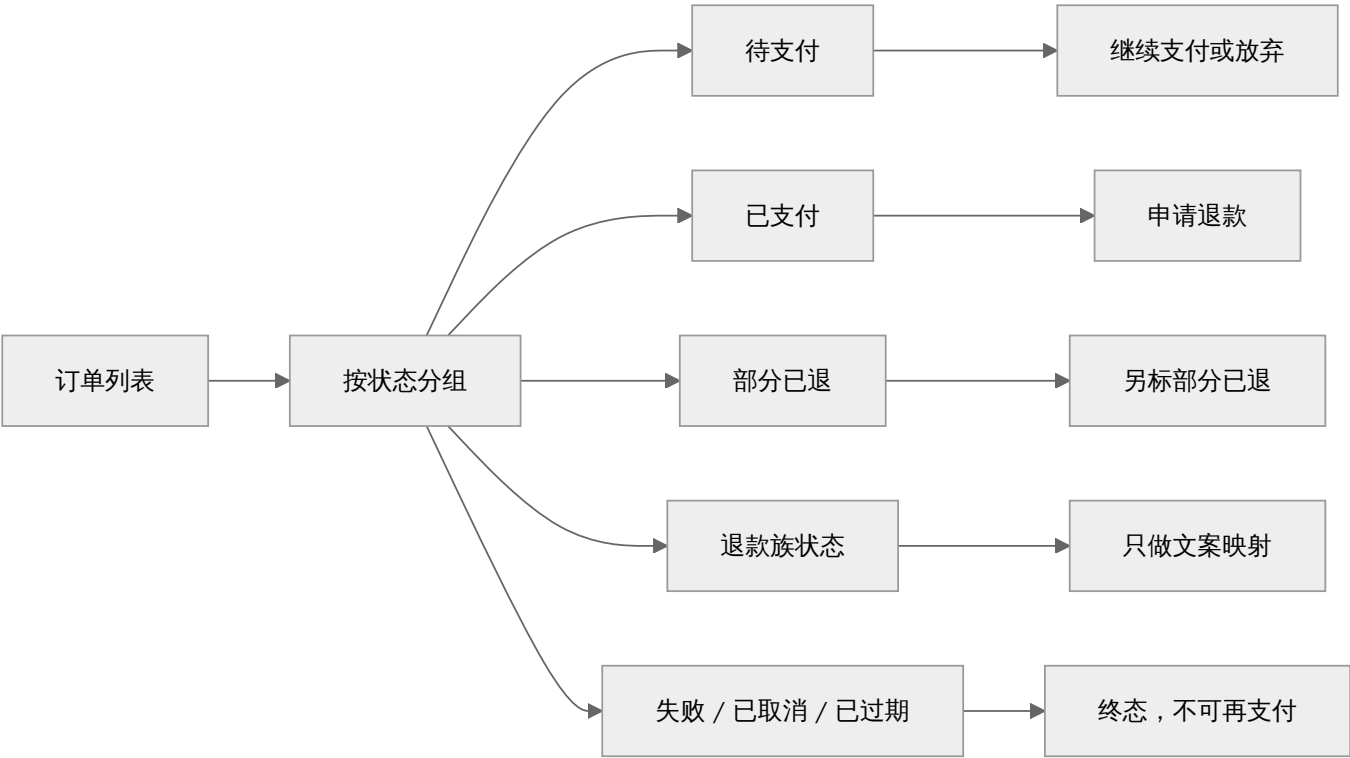


图 8

- 订单号是页面与端点的唯一索引：详情按订单号取单条，列表由服务端返回后在前端按状态分组——待支付可继续支付或放弃，已支付可申请退款并按部分退款另标「部分已退」，失败、已取消与已过期为终态且不可再支付，退款中、退款处理中、已退款、退款失败与退款未知分别展示。
- 退款族状态复用订单状态字段回传，门户只做文案映射；限流与冷静期由服务端判定，门户按错误码提示，不做本地倒计时。

4.7 组织与部门组的门户编排

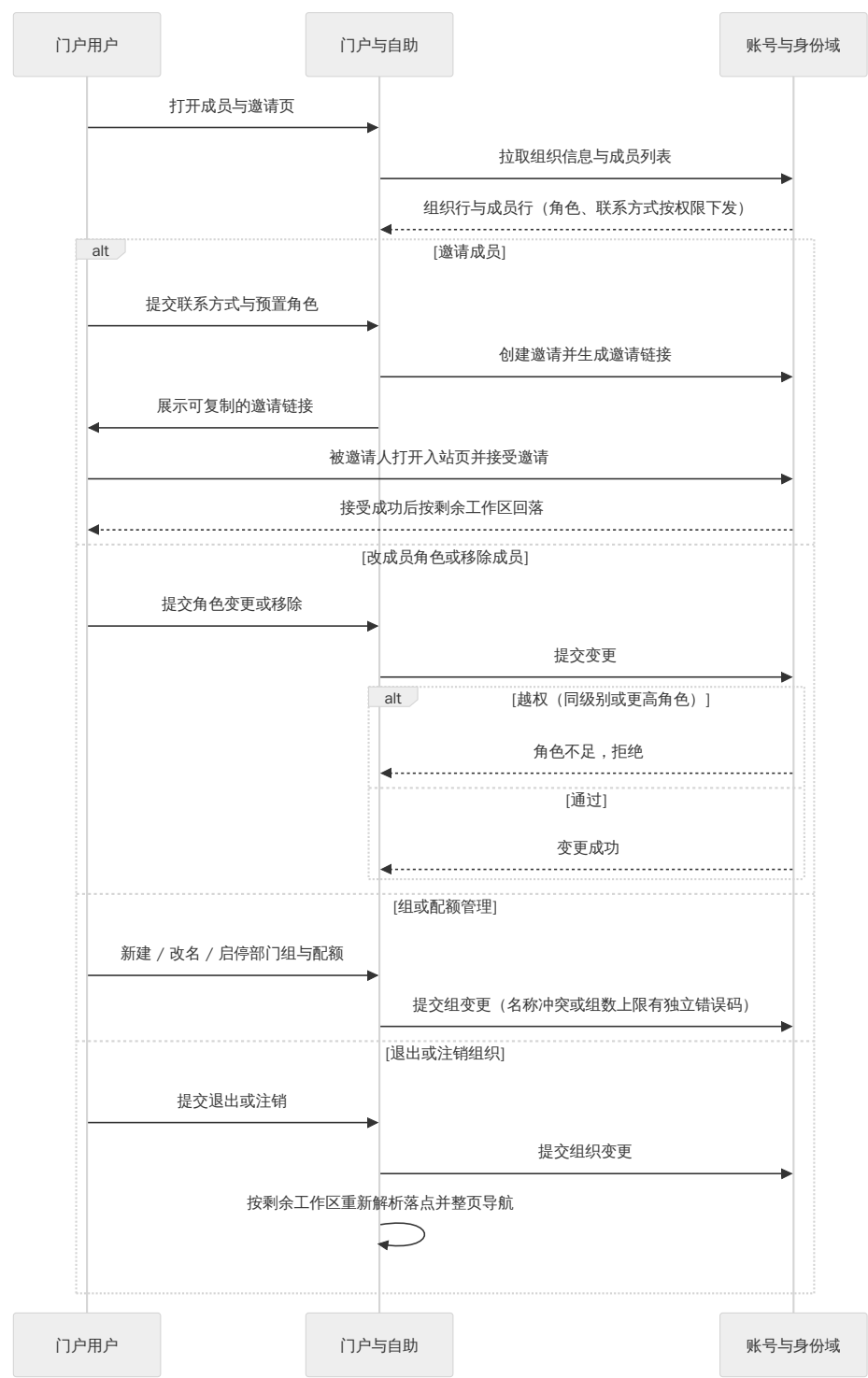


图 9

- 本域只提供入口与编排：成员、邀请、组、配额的语义与写入都在账号与身份域，门户不复制校验规则，只把服务端错误码映射为提示。
- 组织变更（创建、加入、退出、注销）之后统一走回落流程：按剩余工作区重算上下文与账户形态再整页导航，避免「组织已退出但页面仍停在企业上下文」。

4.8 站内信与余额告警阈值

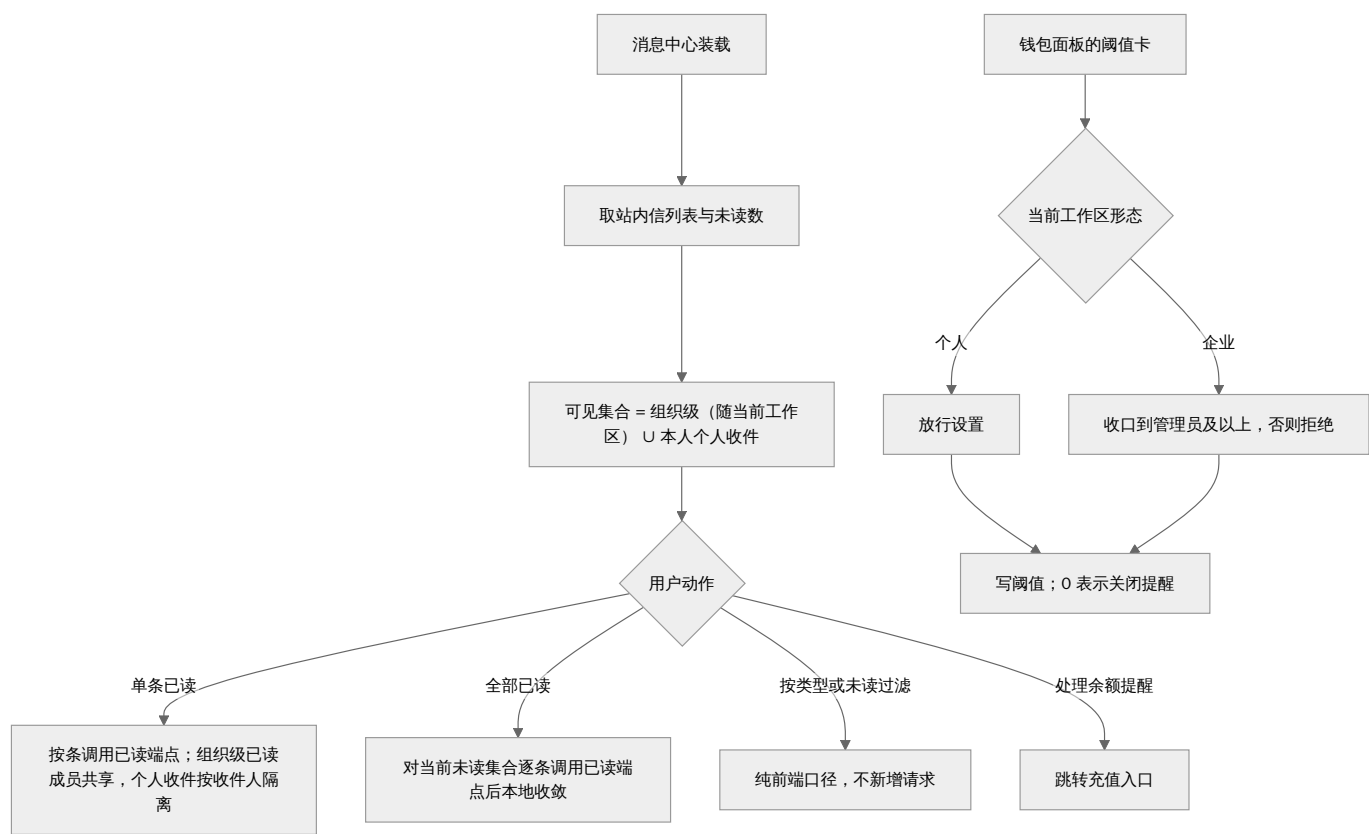


图 10

- 未读数来自同一可见集合的计数，与列表同源，不额外聚合。
- 阈值是门户侧唯一可持久化的通知偏好（单位为元，允许 0 表示关闭）；触发与投递在通知与触达域，门户只负责展示与设置。
- 告警状态回显包含阈值、当前现金余额与是否已触发；保存后必须重新拉取完整状态，因为写入响应只回阈值，触发态需按最新余额重算。

4.9 协议重确认门禁

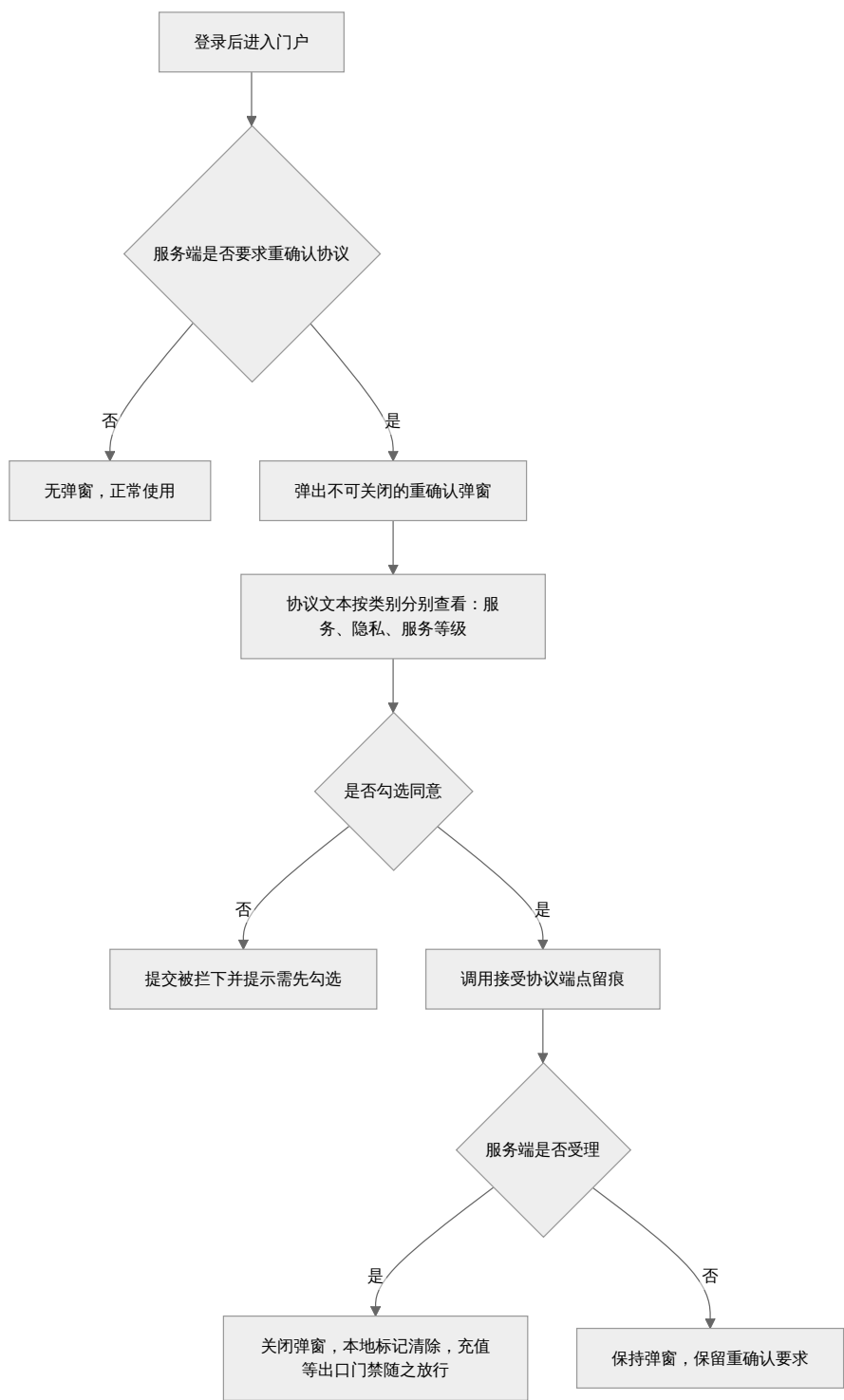


图 11

- 弹窗不可关闭（无关闭按钮、遮罩与键盘退出均无效），保证「未同意不得继续使用」由交互强制。
- 拦截时机在登录后首次进入门户，而非某个具体动作；出口侧仍有服务端门禁兜底（未同意即拒绝下单等动作），两层不互相替代。

5. 接口契约

5.1 本域自有自助端点（前缀 `/api/account`，门户访问令牌）

方法	路径	语义
GET	<code>/api/account/usage</code>	本人用量明细分页：按日期、凭据展示名、模型、组过滤，按日期倒序；返回总量与分页信息
GET	<code>/api/account/org/usage</code>	组织用量透视与分账：维度可组合，支持导出同源数据文件；返回汇总与分页行双份口径
GET	<code>/api/account/transactions</code>	本人流水：按类型与日期过滤、分页，支持导出
GET	<code>/api/account/bills</code>	账期账单：周期内按日用量汇总、按模型聚合的构成、按类型聚合的收支
GET	<code>/api/account/alerts</code>	余额告警设置与当前触发状态：阈值、现金余额、是否已触发
PUT	<code>/api/account/alerts</code>	更新余额告警阈值；企业工作区要求管理员及以上，个人工作区放行；0 表示关闭
GET	<code>/api/account/notifications</code>	站内信列表：组织级与本人在同一可见集合内按时间倒序取最近若干条，附未读数
POST	<code>/api/account/notifications/{nid}/read</code>	标记站内信已读：组织级共享已读态，个人收件按收件人隔离；重复标记幂等

- 本人用量默认窗口为最近 30 天，页大小上限 100；组织透视页大小上限 200，维度缺省为「组 × 日期」，非法维度以参数错误拒绝。
- 透视导出取全量聚合行（行数受维度组约束，非原始流水全量）；流水导出行数上限一万行并按导出时间命名。
- 全部端点金额为元字符串；用量行同时给出实收费用与原应有费用；流水行不下发内部账务键；阈值取值 0 至 10000 元。

5.2 门户页面 → 被引用端点索引（语义详见对应域）

页面能力	方法	路径	语义归属
工作台、费用中心钱包面板、充值页余额	GET	<code>/api/account/wallet</code>	钱包与账务域 (D04)
充值订单记录、订单详情与结果页轮询	GET	<code>/api/account/orders/{order_no}</code>	订购与支付域 (D03)
充值下单	POST	<code>/api/account/orders</code>	订购与支付域 (D03)
订单退款申请入口	POST	<code>/api/account/orders/{order_no}/refund-apply</code>	退款与对账域 (D07)

页面能力	方法	路径	语义归属
支付渠道选择与对公转账信息	GET	/api/account/pay-channels	订购与支付域 (D03)
工作区列表与切换、企业工作台组织信息	GET	/api/account/organizations	账号与身份域 (D01)
企业信息读写、成员列表与移除	PUT	/api/account/organization	账号与身份域 (D01)
成员角色变更	PUT	/api/account/members/{membership_id}/role	账号与身份域 (D01)
部门组成员与配额	GET	/api/account/groups/{group_id}/members	账号与身份域 (D01)
部门组配额设置与启停	PUT	/api/account/groups/{group_id}/quota	账号与身份域 (D01)
邀请与邀请列表	POST	/api/account/invitations	账号与身份域 (D01)
邀请链接生成与撤销	POST	/api/account/invitations/link	账号与身份域 (D01)
凭邀请入站	POST	/api/account/invitations/accept	账号与身份域 (D01)
个人资料读写	PATCH	/api/account/profile	账号与身份域 (D01)
安全日志分页	GET	/api/account/security-logs	账号与身份域 (D01)
协议文本查看与重确认留痕	POST	/api/account/me/accept-terms	风控与合规域 (D09)
个人与企业注册	POST	/api/account/register	账号与身份域 (D01)
退出与注销组织、所有权移交	POST	/api/account/organization/ownership-transfer	账号与身份域 (D01)

- 本表只登记门户页面实际引用的端点，各行语义归属对应能力域，本域不重复展开；组织上下文相关请求携带组织上下文请求头，服务端按所选组织解析数据与权限。
- 订单回跳与渠道回调在订购与支付域完成，门户只做订单查询与展示，不参与验签入账；企业退出、注销、创建与加入之后的落点重算在本域，属组织变更的编排收口。

5.3 前端契约

契约	口径
金额	端点一律元字符串、最多 6 位小数；余额与订单类展示 2 位小数，流水与费用类展示 6 位小数；负债保留符号由页面渲染颜色与文案
令牌	访问令牌短时效、刷新令牌续签；路由切换遇令牌过期先单飞续签，失败才清理并落登录页，回跳保留原查询参数
分页与错误	列表类端点统一返回条目、总量、页码与页大小；工作区不存在、角色不足、渠道不可用等转成页面级提示或引导，不以空白渲染
渠道凭据	用户中心不接触任何渠道凭据；渠道与对公账户信息由服务端按闸门下发，门户只展示

6. 关键约束与验收标准

6.1 约束

- 1. 零自有事实：本域不建表、不写账、不缓存派生金额；所有金额与状态来自上游端点返回。
- 2. 欠款只看现金符号：欠款提示与还款入口以现金余额为负为唯一依据，不读欠费派生标记、不读可用额度。
- 3. 上下文单一实现：工作区判定与角色映射都是纯函数，请求头注入、菜单过滤、落点解析共用同一产出。
- 4. 无可见菜单不清令牌：落账号设置页保留登录态，保证用户仍能完成资料与安全动作。
- 5. 落点四分支封闭：未登录落登录页；无工作区落账号设置页；单工作区直接落其首页；多工作区按最近使用、最近加入、个人空间三级回退。
- 6. 切换即整页重建：工作区切换与组织变更后必须整页导航并清掉上一工作区的标签页缓存。
- 7. 两空间资产隔离：个人与企业工作区的余额、凭据与用量互不可见、互不叠加，首次进入企业工作区必须给出资产独立告知。
- 8. 金额字符串通道：从端点返回到前端渲染全程字符串，禁止先转浮点再比较或再格式化。
- 9. 支付结果不信任回跳：回跳参数仅用于定位订单，入账由服务端回调验签完成；结果页状态以订单查询为准。
- 10. 下单幂等键随意图：一次下单意图一个幂等键，重试复用；意图变更即作废。
- 11. 渠道由服务端下发：门户不硬编码渠道与账户信息，未通过闸门的渠道不得出现在充值页。
- 12. 企业工作区的资金与成员管理收口到所有者与管理员：成员仅可见部门组与企业信息；余额告警阈值同样收口。
- 13. 错误码只做映射：门户不复制上游校验规则，只把服务端错误码映射为提示与引导。

6.2 验收标准

#	验收口径
1	未登录访问受保护路径落登录页；访问注册与凭企业注册路径不被重定向到登录页
2	已登录但无任何可见菜单时落账号设置页，且令牌未被清理，改密码与联系方式仍可操作
3	多工作区账号默认落最近使用的企业工作台，无活跃记录回退最近加入者，无企业落个人工作台

#	验收口径
4	记住的工作区被退出或注销后，下一次拉取自动回退到仍可用的工作区，不出现不可用工作区的入口
5	企业上下文访问个人路径族旧链接被引导到企业等价路径且原查询参数保留，不被无权限页接收
6	现金余额为负时工作台与费用中心均展示欠款与充值入口；现金为正但赠金已过期时不得展示欠款
7	账单端点一次请求返回按日汇总、按模型构成与按类型收支三组结果，按日汇总与费用构成总量一致
8	流水行不含内部账务键；赠金行备注为可读文案而非内部编码；扣减行备注透出模型名
9	改金额后重试不返回旧订单；同一下单意图重复提交返回原订单而非产生第二单
10	未配置凭据、未探活、未启用或未放行的渠道不出现；对公转账渠道展示收款账户信息
11	邀请链接可复制且被邀请人可凭其入站并接受邀请；接受后按剩余工作区落到正确工作台
12	管理员变更同级或更高级角色成员时被拒绝；成员看不到成员与邀请菜单，直接访问该路径被拦到无权限页
13	站内信列表同时包含当前工作区组织级与本人个人收件；个人收件已读不影响同组织其他成员的未读数
14	余额告警阈值在企业工作区由非管理员提交时被拒绝，个人工作区提交成功；阈值 0 时告警状态为未触发
15	协议升级后登录首次进入门户弹出不可关闭弹窗；未勾选提交被拦；确认后下单等出口不再被协议门禁拒绝

6.3 待后续设计细化的开放项

1. 组织级站内信的细粒度个人已读：现为组织内共享已读态；拆分为每成员一份需先定存储与迁移口径。
2. 通知偏好的可订阅面：现仅余额告警阈值可持久化，用量突增、组织关闭等类型的订阅开关是否开放、粒度到人还是到工作区待定。
3. 工作区切换的免整页刷新：改为局部热切换需要菜单树与标签栏的上下文隔离方案。
4. 费用中心的跨工作区合并视图与门户侧分页服务端化：跨企业消费汇总是否需要、欠款与停服口径如何呈现待定；订单列表表现按全量返回前端分组，量级增长后需改为服务端过滤分页。