

臻好印

无人自助打印系统 工程设计、部署与运维手册

从单台实测原型到多门店、多设备生产平台

文档版本	1.0
基准日期	2026-09-11
适用对象	产品负责人、研发、门店运维、测试与供应商
固定服务域名	print-api.munvor.com（规划）
文档属性	内部工程资料；不包含任何 AppSecret、支付密钥或临时隧道地址

文档结论

当前原型已经完成真实手机上传到 Windows 打印队列的端到端验证，并由用户确认可正常使用。要扩展为商业化多打印机平台，核心工作不是复制小程序，而是把单机绑定、SQLite、本地文件、模拟支付和进程内互斥，升级为中心化多租户控制面、可靠任务调度、设备身份体系、真实支付与可运营体系。

目录

目录	2
1. 文档目的与系统结论	5
1.1 当前结论	5
1.2 成功标准	5
2. 已验证基线与边界	6
2.1 当前技术栈	6
2.2 当前功能限制	6
2.3 已有防重复边界	6
3. 目标架构：多门店、多打印机	7
3.1 组件职责	7
3.2 为什么不能一台打印机配一个临时隧道	7
4. 用户扫码到出纸的完整链路	8
4.1 标准流程	8
4.2 二维码设计	8
4.3 异常恢复体验	8
5. 状态机、幂等与恰好一次边界	9
5.1 建议状态	9
5.2 幂等键清单	9
5.3 物理打印提交协议	9
6. 数据模型与多租户边界	10
6.1 核心实体	10
6.2 数据一致性	10
6.3 索引建议	10
7. API 设计基线	11
7.1 小程序 API	11
7.2 代理 API	11
7.3 管理 API	11
8. 门店代理与打印机接入	12
8.1 从单打印机到多打印机必须改造的点	12
8.2 设备注册 SOP	12
8.3 Windows 运行要求	12
9. 文件处理与内容安全	13
9.1 处理管线	13
9.2 Office 文档	13

9.3 隐私与保留	13
10. 真实微信支付设计	14
10.1 资金链路	14
10.2 必须具备	14
10.3 密钥管理	14
11. 域名、DNS 与云基础设施	15
11.1 固定域名方案	15
11.2 当前 DNS 事实与变更原则	15
11.3 推荐基础设施	15
12. 安全架构与威胁模型	16
12.1 主要威胁	16
12.2 网络原则	16
12.3 安全验收	16
13. 可观测性、告警与运营后台	17
13.1 指标	17
13.2 日志与追踪	17
13.3 后台最小模块	17
14. 日常维护制度	18
14.1 备份与恢复	18
14.2 升级策略	18
15. 故障处置手册	19
15.1 严重级别	19
15.2 事故复盘	19
16. 容量规划与硬件策略	20
16.1 分阶段规模	20
16.2 性能估算方法	20
16.3 Epson L3250 的定位	20
17. 测试与验收矩阵	21
17.1 软件自动化	21
17.2 设备实测用例	21
17.3 当前基线证据	21
18. 实施路线图与工作量	22
18.1 最小团队	22
18.2 难度判断	22
19. 成本模型与经营指标	23
19.1 单台月度总成本	23

19.2 应持续跟踪 23

19.3 不建议过早投入 23

20. 上线检查清单 24

20.1 平台 24

20.2 门店与设备 24

20.3 放量判定 24

附录 A. 推荐配置模板 25

代理配置示例 25

附录 B. 关键决策记录 26

版本变更记录 26

附录 C. 官方参考资料 27

1. 文档目的与系统结论

本手册把已经完成的单台自助打印验证，沉淀为可复用、可扩展、可审计的系统工程基线。它既记录当前真实能力，也给出多台打印机、多个门店和后续商业运营所需要的目标架构、开发清单、验收标准与运维制度。

1.1 当前结论

- 可行性：微信小程序可以完成扫码进入、文件上传、打印参数配置、任务创建和结果查询。Windows 门店代理可以下载并校验文件，然后通过官方驱动和系统打印队列提交到 Epson L3250。
- 实测状态：已完成两次受控 Windows 队列级真实打印提交；随后完成手机在外网环境上传并打印，用户确认正常使用。后台记录显示订单和任务完成、单次尝试、队列清空且打印机状态正常。
- 生产判断：当前版本属于经过真实链路验证的原型，不等于可以直接无人值守商业运营。支付、云数据库、对象存储、稳定域名、设备身份、后台、告警和故障处置仍需生产化。

1.2 成功标准

层级	成功标准	证据
用户体验	扫码后自动定位设备，3 分钟内完成上传、配置和支付	真机录屏、埋点漏斗、支付单号
系统可靠性	不重印、不漏单；不确定结果必须进入人工确认	幂等键、状态机、审计日志、故障注入
门店运营	断网/缺纸/卡纸/重启可恢复，门店人员有明确 SOP	告警、操作记录、演练报告
规模化	新增门店和打印机无需改代码，只需注册、绑定和验收	设备注册流程、配置版本、资产台账

2. 已验证基线与边界

2.1 当前技术栈

组件	当前实现	生产化方向
微信小程序	JavaScript + WXML + WXSS	保留；补充扫码场景、支付、埋点、异常恢复
中心 API	Node.js + Fastify	保留框架或等价实现；无状态化、水平扩展
数据存储	SQLite + 本地上传目录	PostgreSQL + 对象存储；Redis/可靠队列用于调度信号
门店代理	Node.js + PowerShell	Windows Service；设备证书、自动升级、按打印机隔离并发
打印通道	SumatraPDF 3.6.1 + Epson 官方驱动 + Windows 队列	保留可控工具链；锁定版本并做机型验收
支付	模拟支付	微信支付真实下单、回调验签、退款与对账

2.2 当前功能限制

- 支持 PDF、JPG、JPEG、PNG；单文件默认不超过 50 MB。PDF 使用真实页数；图片检查尺寸，默认上限 6000 万像素。
- 默认最多 100 页、100 个打印面、10 份；每台打印机最多 5 个活跃任务；每位用户 24 小时最多 200 个打印面。
- Epson L3250 当前按 A4、黑白/彩色、单面能力建模；不支持 A3 和自动双面。Office 文档当前禁用。
- 代理下载后再次核对文件长度和 SHA-256；扩展名、文件魔数和 PDF 结构均需校验。

2.3 已有防重复边界

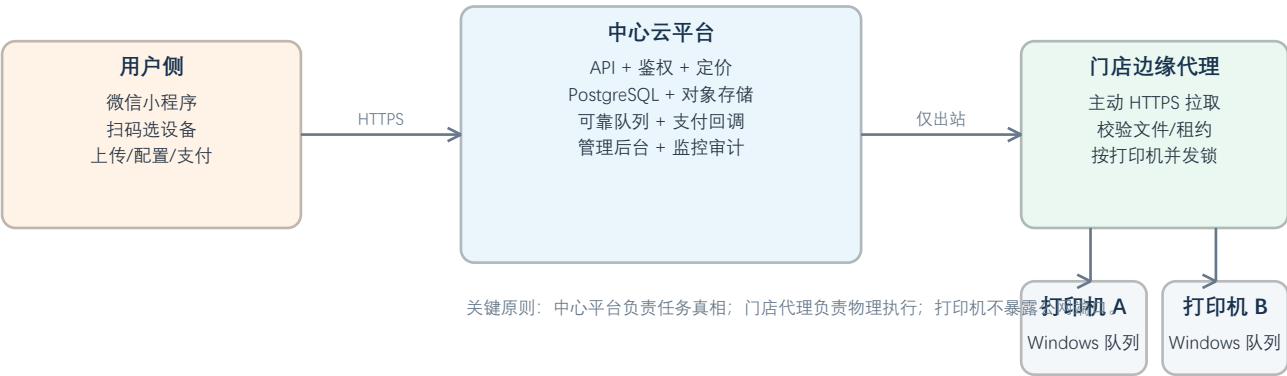
当前系统已经具有用户请求幂等键、打印尝试次数、处理租约、打印租约和 attention_required 人工确认状态。物理打印提交后，如果代理无法确定结果，不得自动重试，因为 Windows 队列清空只能证明任务离开队列，不能证明纸张已完整输出。

必须坚持的原则

支付可以重试、下载可以重试、状态回报可以重试；一旦可能已经提交给物理打印机，自动重试必须停止。任何‘可能已打但无法确认’的情况进入人工确认，避免给用户重复出纸。

3. 目标架构：多门店、多打印机

推荐采用中心云平台加门店边缘代理的架构。小程序、支付回调、数据库、文件存储和调度集中部署；每个门店只运行一个或少量代理，代理主动通过 HTTPS 访问中心平台，再把任务分发到本地 Windows 打印队列。这样无需给打印机或门店电脑开放公网入站端口。



3.1 组件职责

组件	职责	不得承担
小程序	登录、扫码识别设备、上传、参数、报价展示、支付、订单状态	不得自行计算最终应付金额；不得持有服务端密钥
中心 API	用户鉴权、设备解析、服务器定价、订单状态机、支付编排	不得直接访问门店局域网打印机
对象存储	保存源文件、派生文件、短期下载签名	不得公开永久 URL
PostgreSQL	订单、支付、打印任务和审计的唯一事实源	队列消息不得替代最终业务状态
可靠队列	削峰、唤醒调度、重试可重试步骤、死信隔离	不得用至少一次投递作为重复物理打印依据
门店代理	领取任务、下载验真、调用本地队列、上报心跳和结果	不得信任用户传入价格或跳过租约
管理后台	资产、门店、定价、订单、告警、退款、审计、版本管理	不得允许无审计地修改已支付订单

3.2 为什么不能一台打印机配一个临时隧道

临时隧道适合开发验证，不适合作为生产入口。规模化时应只保留一个固定 API 域名，所有代理采用出站长轮询或 WebSocket。即使使用命名隧道，也应部署在中心服务入口并配置冗余连接，而不是给每台打印机分配随机 URL。

4. 用户扫码到出纸的完整链路

4.1 标准流程

步骤	系统动作	关键控制
1. 扫码	二维码携带短场景值，例如设备别名或签名令牌	不可直接暴露数据库主键；支持吊销和换码
2. 登录	小程序 code 换取用户会话，绑定 openid/unionid	AppSecret 仅服务端保存；日志脱敏
3. 设备解析	中心平台把场景值解析为门店和打印机	校验设备启用、在线、能力与营业状态
4. 上传	获取短期上传凭证，文件直传对象存储	扩展名、魔数、大小、哈希、恶意文件扫描
5. 预检	解析页数、尺寸和色彩配置，生成标准化清单	Office 先沙箱转 PDF；失败不给报价
6. 报价	服务端根据设备、纸张、单双面、彩色、份数计价	客户端只展示；报价有版本和过期时间
7. 支付	服务端创建微信支付订单，小程序拉起支付	回调验签、金额复核、幂等入账、主动查单
8. 入队	已支付订单生成唯一打印任务并进入待领取	订单、任务和支付事务一致；一单一任务
9. 打印	代理持租约领取，下载验真，提交指定本地打印队列	每台打印机串行；提交前最后一次栅栏检查
10. 完成	代理持久化回执并幂等上报；用户看到结果	不确定结果进入人工确认，不自动重印
11. 清理	到期删除源文件和派生文件，保留必要审计元数据	默认短保留；支持用户主动删除

4.2 二维码设计

每台物理设备使用独立二维码。推荐二维码场景值只包含可轮换的短别名，例如 p_x7K9m2，并由服务端解析。若需要防止截图长期滥用，可加入门店范围、过期时间和签名；但打印机机身上的静态码仍应可长期使用，因此重点是可吊销、可替换和服务端风控，而不是把敏感信息塞进二维码。

4.3 异常恢复体验

- 上传中断：续传或重新获取短期凭证，原订单不进入支付。
- 支付已扣款但前端未收到成功：客户端轮询订单；服务端以支付回调和主动查单为准。
- 打印机离线：支付前明确提示；已支付后进入可等待、改派或退款流程。
- 结果不确定：页面显示‘正在人工核实’，禁止用户点击重打；后台核对后完成或退款。

5. 状态机、幂等与恰好一次边界



5.1 建议状态

对象	主状态	说明
订单	draft / quoted / pending_payment / paid / printing / completed / cancelled / refunded / attention_required	业务和资金视角
支付	created / processing / succeeded / closed / refunding / refunded / failed	以微信支付结果为准
打印任务	queued / leased / downloading / validated / submitted / completed / failed / attention_required	物理执行视角
打印机	online / busy / offline / degraded / disabled / maintenance	调度和用户可用性视角

5.2 幂等键清单

操作	幂等键	重复请求处理
创建订单	user_id + client_request_id	返回原订单，不重复生成
支付回调	平台交易号 + 事件类型	验签后仅首次推进状态
创建打印任务	order_id 唯一约束	保证一单一任务
代理领取	job_id + attempt + lease_token	过期令牌拒绝提交或上报
完成回执	job_id + attempt + receipt_id	重复上报返回已确认结果
退款	order_id + refund_reason_version	重复操作查询已有退款单

5.3 物理打印提交协议

- 代理在本地先写入‘准备提交’记录并 fsync，包含任务、尝试号、文件哈希、目标队列和参数。
- 提交前向中心平台做一次租约栅栏检查，确认任务仍属于当前代理和当前尝试。
- 调用打印工具后记录 Windows Spooler 作业标识和时间。能够确认队列接受时进入 submitted。
- 代理重启后读取本地回执；若上次处于可能已提交状态，一律上报 attention_required，不再次执行打印命令。

工程现实
分布式系统无法仅凭网络重试获得物理世界的严格恰好一次。正确目标是：数字状态强幂等，物理提交使用持久回执和栅栏，所有不确定性可见、可审计、可人工处理。

6. 数据模型与多租户边界

6.1 核心实体

实体	关键字段	关键约束
tenant	id, name, status	所有业务表携带 tenant_id
store	id, tenant_id, name, address, timezone	门店和设备归属稳定
printer	id, store_id, alias, queue_name, capabilities, status	alias 全局唯一；能力版本化
agent	id, store_id, cert_fingerprint, version, last_seen	凭证可轮换、可吊销
user	id, tenant_id, openid_hash, status	openid 加密或哈希索引
file_asset	id, owner_id, object_key, sha256, size, mime, expires_at	对象私有、到期清理
quote	id, pricing_version, amount, currency, expires_at	支付金额必须等于有效报价
order	id, user_id, printer_id, client_request_id, status	user_id + client_request_id 唯一
payment	id, order_id, out_trade_no, transaction_id, status	商户单号和平台交易号唯一
print_job	id, order_id, attempt, lease_token, state	order_id 唯一；乐观版本号
job_receipt	job_id, attempt, spooler_id, submitted_at, result	job_id + attempt 唯一
audit_event	actor, action, resource, before, after, trace_id	追加写，不覆盖

6.2 数据一致性

PostgreSQL 是订单和任务状态的唯一事实源。队列只传递‘某任务可能可执行’的信号；消费者必须重新读取数据库、检查状态和租约。订单支付成功、创建打印任务和写入 outbox 事件应在同一数据库事务完成，再由 outbox worker 投递到队列。这样即使进程崩溃，也不会出现已付款但永远没有任务的静默丢失。

6.3 索引建议

至少建立：printer(alias)、agent(last_seen)、order(user_id, created_at)、order(status, created_at)、payment(out_trade_no)、print_job(printer_id, state, created_at)、print_job(lease_expires_at)、file_asset(expires_at) 和 audit_event(resource_type, resource_id, created_at)。所有多租户查询把 tenant_id 放在联合索引前部。

7. API 设计基线

7.1 小程序 API

方法与路径	用途	安全与幂等
POST /v1/auth/wechat	微信登录换取业务会话	限速；服务端换取 openid；不返回平台密钥
GET /v1/scenes/{code}	解析二维码并返回设备能力	只返回公开门店和设备信息
POST /v1/uploads	创建上传会话	限制大小、格式、次数；返回短期签名
POST /v1/files/{id}/finalize	声明上传完成并触发预检	校验实际对象大小和哈希
POST /v1/quotes	服务端报价	参数白名单；报价版本和过期时间
POST /v1/orders	创建订单	Idempotency-Key 或 client_request_id
POST /v1/orders/{id}/pay	创建微信支付单	校验所有权、报价和金额
GET /v1/orders/{id}	查询订单和打印状态	只允许订单所有者或授权人员
POST /v1/orders/{id}/cancel	未支付取消或申请售后	基于状态机校验

7.2 代理 API

方法与路径	用途	关键字段
POST /v1/agent/session	设备证书换取短时令牌	agent_id, nonce, signature
POST /v1/agent/heartbeat	批量上报代理和打印机状态	版本、磁盘、队列、错误、耗材提示
POST /v1/agent/jobs/lease	按打印机能力领取任务	printer_ids, lease_seconds, agent_version
GET /v1/agent/jobs/{id}/file	获取一次性文件下载地址	lease_token；短期签名
POST /v1/agent/jobs/{id}/submitted	上报已提交队列	attempt, lease_token, spooler_id, receipt_id
POST /v1/agent/jobs/{id}/complete	幂等确认完成	receipt_id, result, diagnostics
POST /v1/agent/jobs/{id}/attention	结果不确定或需人工处理	reason_code, diagnostics

7.3 管理 API

管理端必须有独立身份体系、角色权限和强审计。典型角色包括平台管理员、运营、财务、门店经理、门店维护员和只读审计员。退款、设备吊销、定价发布和手工结单属于高风险动作，建议二次确认，并记录操作前后值、操作者、IP、设备和 trace_id。

8. 门店代理与打印机接入

8.1 从单打印机到多打印机必须改造的点

当前单机假设	风险	目标改造
API 默认取第一家门店、第一台打印机	扫码或报价可能落到错误设备	所有接口显式携带 scene/printer_id，并校验租户归属
代理只有一个 printerName	同门店无法独立控制多队列	配置 printerId 到 Windows queueName 的映射表
代理使用进程级全局 busy	一台设备繁忙会阻塞其他设备	每台打印机独立串行锁；代理可并行驱动不同队列
多个 printerIds 上报同一状态	后台看不到真实单机故障	逐队列采集在线、错误、作业数和能力
SQLite 和本地上传目录	多实例不一致、磁盘故障丢数据	PostgreSQL、对象存储、集中备份
硬编码默认打印机	新增设备要改代码	注册、绑定、验收和配置版本全部数据化

8.2 设备注册 SOP

- 资产建档：门店、设备编号、品牌型号、序列号、网络方式、纸张能力、彩色能力、单双面、安装位置。
- Windows 准备：安装官方驱动；设置固定且唯一的队列名；关闭会改变输出的驱动默认优化；打印测试页。
- 代理注册：由后台生成一次性注册码，在门店电脑兑换设备证书；注册码使用后作废。
- 映射绑定：把平台 printer_id 映射到本机队列名；运行能力测试并上传结果。
- 二维码安装：生成设备场景码，打印并贴在对应机器上；双人核对二维码和物理设备一致。
- 验收开通：完成黑白、彩色、多页、异常、断网和重启测试后，后台把设备从 maintenance 改为 online。

8.3 Windows 运行要求

生产环境建议将代理包装为 Windows Service，使用最小权限专用账户运行。服务应具备自动启动、崩溃重启、结构化日志轮转、磁盘空间保护、本地回执数据库、时间同步检查和签名升级。当前‘用户登录后计划任务启动’可用于试点，但无人值守门店更适合无需交互登录的系统服务。

9. 文件处理与内容安全

9.1 处理管线

阶段	处理	失败策略
上传前	扩展名白名单、声明大小、用户限额	直接拒绝并说明支持格式
上传完成	对象大小、MIME、文件魔数、SHA-256	隔离对象，不进入报价
预检	PDF 结构与真实页数；图片尺寸；加密/损坏检测	要求用户修复或重新上传
安全扫描	恶意文件扫描、压缩炸弹限制、解析超时	隔离并记录规则，不执行主动内容
规范化	图片转标准 PDF；未来 Office 在隔离沙箱转 PDF	转换输出再次校验哈希和页数
代理下载	校验 Content-Length、实际字节数和 SHA-256	不提交打印；可安全重试下载
打印后	按策略删除源文件和派生文件	删除任务可重试并告警

9.2 Office 文档

不要直接在门店代理上调用 Office 打开用户文件。Office 格式可能包含宏、外链和复杂对象，且页面排版受字体和版本影响。生产做法是在中心侧隔离沙箱中禁用网络和宏，限制 CPU、内存、磁盘与运行时间，转换为 PDF 后重新计算页数和报价，并让用户预览确认。第一期继续只收 PDF 和图片是合理的风险控制。

9.3 隐私与保留

- 对象存储默认私有；上传和下载 URL 短期有效，只允许指定动作。
- 文件正文不得进入普通应用日志、错误追踪或客服截图。
- 建议默认在打印完成后 24 小时内自动删除，可按业务和法规进一步缩短；元数据按财务和纠纷需要单独保留。
- 提供用户主动删除入口，并记录删除完成时间，不记录文件正文。
- 正式上线前完成微信小程序隐私保护指引、个人信息处理规则和必要备案；具体合规文本由专业法务确认。

10. 真实微信支付设计

10.1 资金链路

服务端根据有效报价创建商户订单，再调用微信支付小程序/JSAPI 下单接口。小程序只接收拉起支付所需的临时参数。支付成功不能依赖前端回调，而应以微信支付服务器通知为主、主动查单为补偿。回调需要验签、解密、校验商户号、AppID、金额、币种和订单号，然后幂等推进订单。

10.2 必须具备

能力	工程要求	运营要求
下单	服务端价格；商户单号唯一；描述不泄露文件名	支付失败可重新拉起
回调	平台证书验签；去重；事务更新；快速应答	异常进入支付告警
查单	回调丢失或超时后主动查询	用户页面自动恢复
关单	超时未支付关闭并释放文件/资源	展示明确失效状态
退款	全额/部分退款状态机；幂等；回调确认	退款原因、操作者和凭证留档
对账	按日下载账单，与订单、退款和手续费核对	差异当日处理并形成记录

10.3 密钥管理

AppSecret、API v3 密钥、商户私钥和平台证书不得写入小程序、Git、PDF、截图或普通配置文件。生产使用云密钥管理或受控环境变量，区分开发、预发和生产，建立轮换、吊销和访问审计。由于密钥曾在沟通环境中明文出现，正式上线前应在微信公众平台重新生成并更新部署。

支付上线闸门
在真实支付、退款和对账全部通过前，只能标记为‘受控试用’，不得面向公众长期无人值守收费。

11. 域名、DNS 与云基础设施

11.1 固定域名方案

推荐固定 API 域名为 print-api.munvor.com。小程序后台将它配置为 request 和 uploadFile/downloadFile 合法域名，必须使用有效 HTTPS 证书。接口、对象存储上传域名和下载域名如不同，也要分别加入对应合法域名列表。开发工具的‘不校验合法域名’开关不能作为真机生产方案。

11.2 当前 DNS 事实与变更原则

- munvor.com 当前使用阿里云/万网 DNS 服务器。主站与 www 已有网站解析，企业邮箱使用阿里企业邮箱 MX，并有 SPF、mail、smtp、imap 等记录。
- print-api 子域名当前可独立新增 A 或 CNAME 记录，不需要迁移整个根域名的 DNS。
- 最稳妥方案：先在云平台获得固定公网入口，再只在现有阿里云 DNS 新增 print-api 记录。
- 若未来切换 Cloudflare 权威 DNS，必须先完整导出并核对网站、MX、SPF、DKIM、DMARC 等记录，灰度验证后再改 NS。盲目迁移可能造成网站或企业邮箱中断。

11.3 推荐基础设施

层	推荐形态	高可用要点
入口	HTTPS 负载均衡或边缘代理	两实例以上；健康检查；限速；WAF
API	容器或无状态云服务	跨故障域；滚动发布；自动扩缩
数据库	托管 PostgreSQL	自动备份、时间点恢复、主备、连接池
对象存储	私有 Bucket	生命周期删除、服务端加密、跨区策略按预算
队列	可靠托管队列	至少一次投递；重试上限；死信队列；消费者幂等
缓存	Redis 或等价服务	仅缓存、限流和短租约；不得替代订单事实
监控	指标、日志、追踪和告警平台	trace_id 贯穿小程序、API、代理和支付

12. 安全架构与威胁模型

12.1 主要威胁

威胁	可能后果	控制措施
伪造二维码或篡改 printer_id	任务发往错误设备、欺诈	短别名解析、服务端归属校验、二维码可吊销
伪造价格或页数	少付款多打印	服务端解析和报价；支付金额与报价严格比较
恶意文件	解析器攻击、门店电脑感染	白名单、魔数、扫描、沙箱、资源限制
代理凭证泄露	领取或伪造任务	每代理独立证书、短令牌、轮换、吊销、异常设备告警
请求重放	重复订单或重复动作	nonce、时间窗、幂等键、签名和租约 token
后台越权	退款、改价、查看隐私文件	RBAC、MFA、最小权限、审计、敏感动作复核
日志泄密	文件名、openid、支付信息外泄	字段白名单、脱敏、分级访问、保留期限
供应链篡改	代理升级包被植入	签名发布、哈希校验、固定依赖、回滚和 SBOM

12.2 网络原则

- 门店代理仅主动访问中心 HTTPS 443；不开放打印机 9100、Windows 共享或远程桌面到公网。
- 管理后台与用户 API 分离权限和速率限制；管理员启用 MFA。
- 数据库和对象存储使用私网或严格服务身份访问；生产环境禁止共享开发凭证。
- 所有服务器启用时间同步，支付验签、令牌过期和审计时间依赖准确时钟。

12.3 安全验收

上线前至少完成依赖漏洞扫描、密钥扫描、API 越权测试、上传绕过测试、支付回调伪造测试、重放攻击测试、代理证书吊销测试、对象存储公开性检查和管理后台权限矩阵验证。

13. 可观测性、告警与运营后台

13.1 指标

维度	核心指标	建议告警
业务	扫码、上传、报价、支付、完成转化率	任一步骤成功率显著低于基线
订单	待支付、待打印、处理中、人工确认数量	最老待打印超过 3 分钟；人工确认有新增
设备	心跳年龄、队列长度、错误、代理版本、磁盘	心跳超过 90 秒；磁盘低于 2 GB；打印机错误
支付	下单成功率、回调延迟、查单补偿、对账差异	金额不一致或对账差异立即 P1
文件	上传失败、扫描失败、解析耗时、删除积压	删除任务积压或存储异常增长
平台	API 延迟、5xx、数据库连接、队列年龄、死信	错误率、延迟或死信超过阈值

13.2 日志与追踪

统一结构化 JSON 日志。每次扫码会话、订单、支付、任务和代理领取都携带 trace_id。日志只记录文件 id、哈希前缀、页数和大小，不记录原始文件名或内容。代理日志需要包含 Windows 队列名、Spooler 作业号、尝试号、租约号、工具退出码和持续时间。

13.3 后台最小模块

- 实时总览：在线门店/打印机、排队任务、成功率、收入、退款和告警。
- 资产管理：门店、代理、打印机、能力、二维码、固件/代理版本。
- 订单中心：状态时间线、支付流水、打印回执、退款和客服备注。
- 运维中心：心跳、队列、错误码、远程采集诊断包、维护模式和版本发布。
- 配置中心：定价版本、限制、文件保留、营业时间和灰度策略。
- 审计中心：管理员操作、密钥轮换、设备吊销、配置发布和数据导出。

14. 日常维护制度

周期	平台侧	门店侧	输出物
每日	查支付对账、死信、人工确认、文件删除积压	检查纸张、墨量、喷嘴、卡纸和现场整洁	日检记录、异常工单
每周	复盘成功率和延迟；核对离线设备；抽查审计日志	打印黑白/彩色测试页；清洁进纸区域	周报、设备健康榜
每月	恢复演练、权限复核、成本分析、容量预测	检查驱动/系统更新影响；盘点耗材和备件	恢复报告、月度运营报告
每季度	密钥轮换演练、灾备演练、渗透/漏洞复测	全面保养，高故障设备评估替换	季度风险清单
每次发布	预发验证、灰度、指标观察、回滚准备	试点门店先升级，确认打印参数不变	发布记录和验收报告

14.1 备份与恢复

- 数据库：每日全量加持续日志，明确 RPO/RTO；每月至少一次从备份恢复到隔离环境并验证订单关联。
- 对象存储：文件短期保留，重点保证生命周期策略、删除审计和误删保护配置正确。
- 配置：定价、设备能力、二维码映射和代理版本配置均版本化，可回滚。
- 门店代理：本地只保留必要回执和短期缓存；重装后可通过注册流程恢复，不依赖人工复制密钥。

14.2 升级策略

代理采用分批灰度：内部设备、1 家试点门店、10% 门店、50% 门店、全量。升级包必须签名，代理校验签名后安装；发现打印参数或驱动兼容异常立即暂停并回滚。Windows 和打印驱动更新也应纳入变更管理，不能由门店电脑随意自动更新。

15. 故障处置手册

场景	自动动作	人工步骤	禁止事项
打印机离线	停止分配新任务；支付前标记不可用	查电源、USB/网络、驱动、队列；恢复后打一张测试页	不要反复重启所有服务
缺纸/缺墨/卡纸	任务保持或进入 degraded；提示用户	补纸/墨、清除卡纸、核对是否已出部分页面	未核对前不要重打
队列卡住	超时上报；停止该打印机领取	记录 Spooler ID；检查队列和驱动；必要时进入人工确认	不要直接清空后自动重试
代理重启	读取本地回执并恢复安全步骤	检查上次任务是否可能已提交	submitted 未确认任务不得重新执行
门店断网	代理保留状态；云端显示离线	恢复网络后让代理回报；已支付任务按状态继续或退款	不要开放公网打印端口救急
中心 API 故障	健康检查摘除；客户端重试查询	切换实例/回滚；核对支付回调积压	不要丢弃未处理回调
支付扣款未出纸	进入售后/人工确认流程	核对支付、任务、回执和现场；确认未打印后退款或授权重打	不得让用户重复支付
疑似重复打印	冻结该打印机自动任务	保全日志、回执、Spooler 记录和现场证据；定位幂等边界	不要删除证据
对象存储异常	暂停新上传和任务领取	核对象完整性；切换服务；恢复后哈希复验	不要打印校验失败文件

15.1 严重级别

- P1：资金金额错误、批量重复打印、数据泄露、全平台不可用。立即停止相关功能并通知负责人。
- P2：单门店全部不可用、支付成功任务大量积压、数据库或队列严重退化。30 分钟内响应。
- P3：单打印机故障、少量文件兼容问题、非关键后台功能异常。进入工单并按营业影响处理。

15.2 事故复盘

每次 P1/P2 事故保留时间线、影响订单、用户补偿、根因、临时措施和永久修复。复盘重点是系统控制为何未能提前发现或阻断，而不是追责个人。修复项必须有负责人、截止日期和验证证据。

16. 容量规划与硬件策略

16.1 分阶段规模

阶段	规模	架构重点	放量闸门
试点	3-5 台，1-2 家门店	固定域名、真实支付、PostgreSQL/对象存储、基础后台	连续 2 周无重复打印；成功率 和售后可控
小规模	10-50 台	可靠队列、自动告警、代理灰度升级、门店 SOP	故障恢复演练通过；可独立新增设备
规模化	50-300 台	分区调度、容量自动扩展、财务对账、备件和 SLA	月度稳定性、支付差异和人工 率达标
大规模	300 台以上	多区域、数据分区、运营自动化、供应链和 NOC	灾备、合规、成本和供应商体 系成熟

16.2 性能估算方法

打印吞吐通常受物理设备限制而非 API。按每台设备平均每单打印面数 S、黑白/彩色混合实测速率 V（面/分钟）和换单开销 T（分钟），单机理论订单吞吐约为 $60 / (S/V + T)$ 单/小时，再乘以 0.6-0.75 的运营系数，给缺纸、清洁、网络和复杂文档留余量。容量规划必须以目标机型真实打印样本测量。

16.3 Epson L3250 的定位

L3250 适合作为低成本试点和轻负载彩色 A4 设备。官方同系列 L3253 资料显示其为 A4 墨仓式一体机，后部进纸器约 100 张 A4 普通纸、出纸容量约 30 张，标准模式打印速度约黑白 10 页/分钟、彩色 5 页/分钟，并支持 USB、IPv4/IPv6、LPD/9100/WSD 和 Wi-Fi Direct。具体 L3250 地区版本仍应以本机驱动和实测为准。

硬件建议

如果目标是长时间无人值守、高日印量、自动双面或更强故障检测，应尽早评估商用激光/喷墨设备、较大纸仓、自动双面、可读取耗材和错误状态的管理协议，以及明确的售后 SLA。不要把家用机型的低采购价等同于更低总成本。

17. 测试与验收矩阵

17.1 软件自动化

层	必测内容	通过标准
单元测试	计价、限制、状态转换、权限、哈希、签名	关键分支覆盖；错误输入有确定结果
API 集成	登录、上传、报价、订单、支付回调、代理领取	数据库约束、幂等和事务行为符合设计
代理测试	下载校验、队列映射、锁、租约、回执、重启恢复	同任务重复投递不造成重复提交
端到端	真机扫码、移动网络上传、支付、真实打印、结果反馈	全链路 trace 可查；用户看到最终状态
故障注入	断网、API 5xx、队列重复消息、进程崩溃、磁盘满	安全恢复；不重印；异常可告警
安全	越权、重放、恶意文件、密钥泄漏、签名 URL	无高危问题；修复项复测通过

17.2 设备实测用例

编号	用例	预期
P01	1 页黑白 PDF，单份	目标打印机仅输出 1 张，内容方向正确
P02	多页彩色 PDF，多份	页数、份数、色彩和顺序正确
P03	JPG/PNG 大小边界	合法图片正常；超限明确拒绝
P04	支付回调重复 5 次	只创建一个打印任务
P05	领取后下载中断	可重试下载，不重复物理提交
P06	提交打印命令后立即杀死代理	重启进入人工确认，不自动重打
P07	缺纸/卡纸后恢复	状态和用户提示正确；人工确认部分输出
P08	同门店两台打印机同时工作	各自串行、互不阻塞、任务不串机
P09	扫描 A 机二维码但篡改请求为 B 机	服务端拒绝或按有效场景重新解析
P10	门店电脑重启	服务自动启动、心跳恢复、无任务重复

17.3 当前基线证据

当前代码基线完成 API 自动测试 20 项、代理自动测试 18 项，共 38/38 通过；完成 JavaScript 语法检查和依赖审计。真实打印链路中，两个受控作业进入 Windows Spooler 并完成，后续用户在手机外网环境完成上传和打印并确认可正常使用。以上证据证明链路可行，但不能替代真实支付、规模并发、长稳和故障注入验收。

18. 实施路线图与工作量

阶段	建议周期	主要交付	退出条件
0. 基线固化	1 周	代码版本、配置清单、当前验收报告、密钥轮换	可重复部署并完成单机真测
1. 云端生产底座	2-4 周	固定域名、HTTPS、PostgreSQL、对象存储、CI/CD、监控	预发环境稳定，备份恢复通过
2. 真实支付	2-3 周	下单、回调、查单、退款、对账	沙箱/小额真实支付闭环
3. 多设备改造	3-5 周	设备注册、映射、每机锁、心跳、后台资产模块	两台并行和重启故障测试通过
4. 运营与安全	2-4 周	RBAC、审计、告警、工单、隐私和上传安全	安全验收和门店 SOP 演练通过
5. 试点运营	2-4 周	3-5 台真实营业、指标和售后闭环	连续稳定期达到放量门槛
6. 扩容	持续	自动升级、容量治理、财务和供应链	按季度稳定性与成本目标复评

18.1 最小团队

- 后端/架构 1-2 人：订单、支付、调度、数据和云基础设施。
- 小程序 1 人：扫码、上传、支付、订单状态和用户体验。
- Windows/设备 1 人：代理、驱动、打印参数、安装包和机型兼容。
- 测试 1 人：端到端、支付、故障注入、设备矩阵和回归。
- 运营/门店支持 1 人：设备台账、耗材、工单、退款和现场 SOP。

18.2 难度判断

做出‘一台可打印’的原型属于中等难度，当前已完成。做成‘几十台可收费无人值守’属于中高难度，难点集中在支付一致性、物理结果不确定、多机调度、远程运维和线下耗材故障。做成‘数百台跨区域平台’是持续工程，需要专门的可靠性、财务、安全和供应链能力。

19. 成本模型与经营指标

19.1 单台月度总成本

单台月度 TCO = 设备折旧 + 场地/分成 + 纸张 + 墨水/硒鼓 + 门店电脑与网络 + 云资源分摊 + 支付手续费 + 运维人工 + 售后退款 + 备件损耗。定价必须覆盖彩色高墨耗页面、低客单支付手续费、故障停机和人工处理成本。

19.2 应持续跟踪

指标	定义	用途
支付转化率	支付成功订单 / 有效报价	发现价格或支付体验问题
打印成功率	无需人工处理完成 / 已支付任务	衡量核心服务质量
人工确认率	attention_required / 已提交任务	衡量不确定性和代理质量
重复打印率	确认重复任务 / 已支付任务	核心安全红线
退款率	退款订单 / 已支付订单	综合体验和成本信号
单机利用率	实际打印时间 / 可营业时间	设备配置和选址依据
单面贡献毛利	收入减耗材、支付和分成后的单面贡献	定价和扩张决策
平均恢复时间	故障到恢复的平均时长	运维效率和 SLA

19.3 不建议过早投入

试点阶段优先验证真实需求、支付闭环、故障率和单位经济性。不要在尚未完成 3-5 台稳定运营前，投入复杂的跨区域多活、智能推荐或大量定制硬件。先把不重印、可退款、能远程定位故障和可重复装机做好。

20. 上线检查清单

20.1 平台

检查项	验收证据	状态
固定域名与 HTTPS 正常，微信合法域名已配置	真机移动网络请求、证书检查	☐
生产密钥已轮换并进入密钥管理	密钥清单和访问审计	☐
PostgreSQL 备份与恢复演练通过	恢复报告	☐
对象存储私有、生命周期和删除任务有效	策略截图和抽检记录	☐
支付下单、回调、查单、退款、对账闭环	小额实测流水	☐
监控、P1/P2 告警和联系人有效	告警演练	☐
隐私保护指引、备案和用户协议完成	平台审核/法务记录	☐

20.2 门店与设备

检查项	验收证据	状态
打印机、队列名、平台设备和二维码一一对应	双人核对照片和资产台账	☐
Windows Service 开机自启并可自动恢复	重启测试	☐
黑白、彩色、多页、多份样本通过	验收打印件	☐
缺纸、卡纸、断网、代理重启演练通过	演练记录	☐
纸张、墨水、备件和联系人员到位	门店交接清单	☐
设备贴有用户提示、客服和隐私说明	现场照片	☐

20.3 放量判定

Go / No-Go

只有当真实支付可对账、真实打印无重复、故障可恢复、密钥已轮换、门店 SOP 已演练、告警能够触达、隐私和备案完成时，才进入公开无人值守运营。任何资金错误、重复打印或数据泄露风险均为 No-Go。

附录 A. 推荐配置模板

以下仅展示字段，不包含真实凭证。敏感值应由密钥管理系统注入。

环境变量示例
<pre>NODE_ENV=production PUBLIC_BASE_URL=https://print-api.munvor.com DATABASE_URL=<secret-reference> OBJECT_STORAGE_BUCKET=zhenhaoyin-files-prod WECHAT_APP_ID=<secret-reference> WECHAT_APP_SECRET=<secret-reference> WECHAT_PAY_MCH_ID=<secret-reference> WECHAT_PAY_API_V3_KEY=<secret-reference> FILE_RETENTION_HOURS=24 MAX_FILE_BYTES=52428800 MAX_PAGES=100 MAX_COPIES=10</pre>

代理配置示例

agent.yaml
<pre>agentId: store-sz-001-agent-01 apiBaseUrl: https://print-api.munvor.com credentialRef: windows-cert-store://zhenhaoyin-agent printers: - printerId: printer-sz-001-a queueName: EPSON L3250 Series maxConcurrent: 1 heartbeatSeconds: 30 leaseSeconds: 90 receiptDb: C:/ProgramData/Zhenhaoyin/receipts.db</pre>

附录 B. 关键决策记录

决策	选择	原因
生产入口	固定域名 print-api.munvor.com	满足微信合法域名和长期运维；不依赖随机测试 URL
门店连接	代理主动出站 HTTPS	无需开放打印机或门店电脑公网端口
订单事实源	PostgreSQL	支持事务、约束、备份恢复和水平 API 实例
文件	私有对象存储	适合大文件直传、短签名和生命周期删除
任务队列	至少一次投递 + 消费者幂等 + 死信	可靠削峰，但不把消息投递等同物理打印
多机并发	每台打印机串行，不同打印机可并行	兼顾物理安全和门店吞吐
不确定结果	人工确认，禁止自动重试	避免物理重复出纸
Office	后续中心沙箱转换	降低门店执行风险并确保报价页数一致
DNS	优先在现有阿里云 DNS 新增子域记录	保护现有网站和企业邮箱，变更范围最小

版本变更记录

版本	日期	内容
1.0	2026-09-11	首次系统化沉淀：现状、目标架构、支付、多机、运维、测试与路线图

附录 C. 官方参考资料

下列链接用于生产实现时复核最新平台规则。微信、支付、云服务和合规要求可能更新，上线前应以官方实时文档为准。

- 1. 微信小程序网络能力与服务器域名
<https://developers.weixin.qq.com/miniprogram/dev/framework/ability/network.html>
- 2. 微信小程序获取不限制数量二维码
<https://developers.weixin.qq.com/miniprogram/dev/OpenApiDoc/qrcode-link/qr-code/getUnlimitedQRCode.html>
- 3. 微信支付商户接入指引
<https://pay.weixin.qq.com/doc/v3/merchant/4015459512>
- 4. 微信支付小程序/JSAPI 下单
<https://pay.weixin.qq.com/doc/v3/merchant/4012791897>
- 5. Cloudflare Queues 投递保证：至少一次与幂等
<https://developers.cloudflare.com/queues/reference/delivery-guarantees/>
- 6. Cloudflare Queues 死信队列
<https://developers.cloudflare.com/queues/configuration/dead-letter-queues/>
- 7. Cloudflare Tunnel 可用性与副本
<https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/configure-tunnels/tunnel-availability/>
- 8. Cloudflare Tunnel DNS 路由
<https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/routing-to-tunnel/dns/>
- 9. Cloudflare 部分 DNS 设置说明
<https://developers.cloudflare.com/dns/zone-setups/partial-setup/setup/>
- 10. 工业和信息化部 ICP/IP 地址/域名信息备案管理系统
<https://beian.miit.gov.cn/>
- 11. Epson L3250 官方支持检索
<https://www.epson.com.cn/services/search.html?key=L3250>
- 12. Epson L3253 官方产品规格（同系列能力参考）
<https://www.epson.com.cn/products/l-all-in-ones/l3253/>
- 13. Epson L325x 用户指南
<https://www.epson.com.cn/drive/97282e24cba04135b331e36a0095a760.html?productId=03f00e0df281466ea6390a9e8465e28c>

文档维护

每次生产架构、支付接口、支持格式、设备型号、限制值或运维流程发生变化，都应更新本手册版本、变更记录和验收证据。建议至少每季度复审一次。