

产品需求文档（PRD）模板

文件编号：PRD-TPL-001

版本号：V3.2

生效日期：2024 年 6 月 1 日

制定部门：产品管理中心

审批人：产品总监 刘敏

保密等级：▲▲ 内部公开（INTERNAL）- 产品、研发、测试团队全员可见

修订历史

版本号	修订日期	修订内容摘要	修订人
V3.2	2024-05-20	新增“AI 功能伦理审查”章节；强化非功能性需求中“数据安全合规”条款	产品经理 张恒
V3.1	2023-12-08	优化用户故事模板（增加“业务价值”字段）；统一交互原型标注规范	产品经理 李雯
V3.0	2023-07-15	重构文档结构，将“运营需求”独立成章节；增加“灰度发布策略”模板	产品总监 刘敏

目录

- 文档基础信息
- 业务背景与目标

- 3. 用户画像与场景分析
- 4. 功能需求详述
- 5. 非功能性需求
- 6. 交互设计与原型
- 7. 数据指标与验收标准
- 8. 项目排期与资源规划
- 9. 运营与推广需求
- 10. 风险与依赖
- 11. 附录

1. 文档基础信息

项目名称	(例：企业知识库智能问答系统 V2.0 - 扫码登录功能)
需求提出人	姓名 / 部门 (例：产研部 - 需求分析师 王浩)
产品负责人	姓名 / 岗位 (例：产品经理 张恒)
需求版本	V1.0 (首次提交) / V1.1 (迭代更新)
需求状态	<input type="checkbox"/> 草稿 <input type="checkbox"/> 评审中 <input type="checkbox"/> 已通过 <input type="checkbox"/> 已冻结 <input type="checkbox"/> 已废弃
关联文档	(可多选) <input type="checkbox"/> 《市场调研报告 - 2024Q2》 <input type="checkbox"/> 《技术架构设计方案 V1.5》 <input type="checkbox"/> 《用户反馈汇总 - 202405》
预计上线日期	YYYY 年 MM 月 DD 日
核心关键词	(最多 5 个, 例：扫码登录、安全验证、用户体验)

2. 业务背景与目标

2.1 背景描述

- 市场环境：（例：根据 2024 年 Q2 行业报告，85% 的 B 端产品已支持扫码登录，用户对操作便捷性的需求提升 37%）
- 现有问题：（例：当前系统仅支持账号密码登录，用户反馈 “频繁输入密码影响效率”，客服每月收到相关投诉 120 + 次）
- 业务驱动：（例：配合公司 “移动优先” 战略，提升移动端用户活跃度；降低账号密码泄露风险）

2.2 产品目标

- 核心目标：（例：上线后 3 个月内，扫码登录使用率达到 60%，用户登录耗时减少 50%）
- 辅助目标：（例：账号异常登录率下降 20%；移动端 DAU 提升 15%）
- 衡量指标：（需量化，例：登录成功率 \geq 99.9%、平均登录耗时 \leq 3 秒）

2.3 范围界定

- 包含功能：（例：Web 端生成二维码、移动端 APP 扫码确认、登录状态同步）
- 不包含功能：（例：第三方 APP 扫码（如微信 / 支付宝）、离线扫码登录）

3. 用户画像与场景分析

3.1 核心用户画像

用户角色	典型特征	使用频次	核心诉求
企业高管	年龄 35-50 岁，注重效率与安全，常用移动端	每日 2-3 次	登录流程简单，避免繁琐操作；确保账号安全
一线员工	年龄 25-35 岁，熟悉移动设备，对体验敏感	每日 5-8 次	快速完成登录，支持多端同步状态
系统管理员	关注稳定性与可维护性，需处理异常登录	每周 3-5 次	可追溯登录日志，支持紧急冻结账号

3.2 典型用户场景

场景 1：高管快速登录系统

- **用户：**CEO 李总
- **场景：**参加临时会议时，需通过笔记本电脑紧急登录系统查看数据报告，但未记住复杂密码。
- **操作路径：**打开 Web 端 → 点击 “扫码登录” → 手机 APP 扫描二维码 → 点击 “确认登录” → 电脑端自动跳转至首页。
- **痛点：**时间紧张时，密码输入错误会导致延误；担心在公共场合输入密码被窥视。

场景 2：员工多设备切换

- **用户：**市场专员 陈雪
- **场景：**在办公室用电脑编辑文档，临时外出时需用手机查看进度，希望保持登录状态。
- **操作路径：**电脑端已登录 → 手机 APP 打开 → 自动识别账号 → 一键确认同步登录状态。
- **痛点：**频繁切换设备时需重复登录，影响工作连续性。

4. 功能需求详述

4.1 功能架构图



- └— 确认弹窗（显示登录设备信息）
- └— 异常提醒（异地登录时增加二次验证）

4.2 用户故事与验收标准

（按优先级排序，P0 为最高）

优先级	用户故事	验收标准（必须可验证）	关联需求
P0	作为 Web 端用户，我希望点击“扫码登录”后生成二维码，以便通过手机快速登录	1. 点击按钮后 1 秒内生成二维码2. 二维码包含唯一标识（与当前设备绑定）3. 显示倒计时（默认 120 秒）	4.1 - 前端模块
P0	作为移动端用户，我希望扫码后看到设备信息，确认后完成登录	1. 扫码后弹窗显示“登录设备：- Windows 10 / Chrome 112.0”“- 登录 IP：xxx.xxx.xxx.xxx”2. 点击“确认”后 3 秒内完成登录同步3. 点击“取消”后，Web 端显示“登录已取消”	4.1 - 移动端模块
P1	作为系统管理员，我希望记录扫码登录日志，以便追溯异常操作	1. 日志包含“扫码时间、设备信息、登录结果、IP 地址”2. 支持按用户 ID / 时间筛选查询3. 日志保存期限≥180 天	4.1 - 后端模块
P2	作为用户，我希望二维码过期后可一键刷新，无需重新点击按钮	1. 倒计时结束后显示“已过期”，并提供“刷新”按钮2. 点击刷新后 1 秒内生成新二维码3. 新二维码与旧码不重复	4.1 - 前端模块

4.3 业务规则与限制

- 二维码有效期：默认 120 秒（可在后台配置，范围 30-300 秒）
- 设备绑定：同一账号最多绑定 5 台常用设备，新设备首次扫码需输入短信验证码
- 频率限制：单用户 1 分钟内最多生成 3 次二维码，避免恶意请求
- 异常处理：连续 3 次扫码失败后，触发账号临时锁定（10 分钟）

5. 非功能性需求

5.1 性能要求

- 响应时间：（例：二维码生成 $\leq 100\text{ms}$ ，扫码确认后状态同步 $\leq 500\text{ms}$ ）
- 并发支持：（例：峰值时段支持 1000 用户同时生成二维码，无延迟）
- 稳定性：（例：服务可用性 $\geq 99.95\%$ ，全年故障时间 ≤ 4.38 小时）

5.2 安全要求

- 数据加密：（例：二维码包含的用户信息需经 AES-256 加密；传输过程采用 TLS 1.3）
- 权限控制：（例：仅登录状态的移动端 APP 可扫码；管理员需双因素认证才能查看登录日志）
- 合规性：（需符合，例：《安全开发规范 V3.0》第 5.3 节扫码登录安全要求；GDPR 数据存储标准）

5.3 兼容性要求

- 浏览器支持：（例：Chrome 90+、Firefox 88+、Edge 90+、Safari 14+）
- 移动端支持：（例：iOS 13.0+、Android 8.0+，适配屏幕尺寸 4.7-6.7 英寸）
- 网络环境：（例：支持弱网环境（网速 $\geq 100\text{kbps}$ ），断网后可缓存 3 分钟内的二维码状态）

5.4 可访问性要求

- 视觉适配：（例：二维码大小支持放大 200%；色盲模式下状态提示色对比度 $\geq 4.5:1$ ）
- 辅助功能：（例：支持屏幕阅读器读取“二维码已过期”等提示；键盘快捷键可触发“刷新二维码”）

6. 交互设计与原型

6.1 核心流程图

```
graph TD
  A[用户点击"扫码登录"] --> B[后端生成带时效的二维码]
  B --> C[Web端显示二维码+倒计时]
  C --> D{用户是否扫码?}
  D -->|是| E[移动端APP解析二维码]
  E --> F[APP显示登录设备信息]
  F --> G{用户确认登录?}
  G -->|是| H[后端验证并生成登录令牌]
  H --> I[Web端与移动端同步登录状态]
  G -->|否| J[Web端显示"登录已取消"]
  D -->|否且超时| K[Web端显示"二维码已过期"+刷新按钮]
```

6.2 原型链接与标注

- 高保真原型：[Figma 链接](#)（需包含所有页面，标注交互逻辑）
- 关键页面标注：
 - 二维码生成页：（例：二维码尺寸 200×200px，倒计时文字颜色 #FF5722，过期后显示红色边框）
 - 扫码确认页：（例：设备信息字体 16px，“确认”按钮点击后有 0.3s 反馈动画）

6.3 文案规范

- 成功提示：（例：“登录成功！正在跳转...”）
- 失败提示：（例：“二维码已过期，请点击刷新” “该设备未绑定，需完成安全验证”）
- 按钮文案：（例：主按钮“确认登录”，次要按钮“取消”“刷新二维码”）

7. 数据指标与验收标准

7.1 功能验收标准

功能点	验收条件（必须可量化 / 可操作）	验收人
二维码生成	1. 点击按钮后 1 秒内显示二维码 2. 二维码包含唯一标识（通过后端接口可查询）	测试工程师
扫码确认流程	1. 扫码后 3 秒内显示设备信息 2. 点击“确认”后 5 秒内完成登录	产品经理
异常处理	1. 二维码过期后自动提示并提供刷新 2. 网络中断后重连可恢复状态	测试工程师

7.2 数据监控指标

指标名称	基准值（当前）	目标值（上线后）	监控工具
扫码登录成功率	-	≥99.9%	数据中台看板
平均登录耗时	8 秒（密码登录）	≤3 秒	前端性能监控
二维码过期率	-	≤5%	后端日志分析
用户投诉量	120 次 / 月	≤30 次 / 月	客服系统

8. 项目排期与资源规划

8.1 里程碑计划

阶段	时间节点	交付物	负责人
需求评审	YYYY-MM-DD	《PRD 终稿 V1.0》 、评审会议纪要	产品经理

技术开发	YYYY-MM-DD ~ YYYY-MM-DD	前端代码、后端接口、数据库脚本	开发负责人
测试验收	YYYY-MM-DD ~ YYYY-MM-DD	《测试用例 V1.0》、《缺陷报告》	测试工程师
灰度发布	YYYY-MM-DD	覆盖 20% 用户，收集反馈	运维工程师
全量上线	YYYY-MM-DD	生产环境部署完成，监控系统启动	项目经理

8.2 资源需求

- 研发资源：（例：前端开发 1 人 · 5 天，后端开发 1 人 · 7 天，测试 1 人 · 3 天）
- 设备资源：（例：测试服务器 2 台，移动端测试设备（iOS/Android 各 3 款））
- 其他支持：（例：UI 设计 1 人 · 2 天，安全团队评审 1 次）

9. 运营与推广需求

9.1 上线策略

- 灰度计划：（例：第 1 周向内部员工开放，第 2 周向 VIP 客户开放，第 3 周全量上线）
- 切换方案：（例：与原有密码登录并行 3 个月，后期逐步引导至扫码登录）

9.2 用户教育

- 帮助文档：（例：《扫码登录操作指南》（图文版 + 视频版））
- 引导设计：（例：首次登录时显示引导弹窗，标注 “新功能：扫码登录更快捷”）
- 客服支持：（例：更新 FAQ，培训客服团队解答常见问题（如 “扫码失败怎么办”））

9.3 效果追踪

- 数据看板：（需包含：日活 / 周活、转化率、用户反馈关键词云）
- 复盘计划：上线后第 15 天 / 30 天各召开 1 次复盘会，输出优化方案

10. 风险与依赖

10.1 风险评估

风险类型	描述	影响程度（1-5）	发生概率（1-5）	应对措施
技术风险	移动端与 Web 端时间同步偏差导致登录失败	4	2	采用服务器时间戳校准；增加重试机制
用户接受度风险	部分用户习惯密码登录，抵触新功能	3	3	上线初期保留双方案；通过弹窗强调“安全 + 便捷”优势
安全风险	二维码被劫持导致账号被盗	5	1	实现二维码动态加密；异常 IP 登录需二次验证

10.2 依赖关系

- 内部依赖：（例：需移动端团队配合开发扫码解析功能；依赖《安全开发规范》第 5.3 节的加密标准）
- 外部依赖：（例：需第三方提供 WebSocket 服务稳定性保障；iOS 端需通过 App Store 审核）

11. 附录

11.1 术语表

- 二维码 Token：（定义：后端生成的临时凭证，有效期 120 秒，关联用户 ID）
（注：文档部分内容可能由 AI 生成）