

智能标书工作台

普通用户使用说明

从接入大模型、上传招标材料，到生成 Word / PDF 交付文件

适用于 Codex · Claude Code · Hermes · OpenClaw · WorkBuddy 等主流
Agent

版本：通用交付版

阅读导航

第一次使用建议按顺序阅读；熟悉后可直接查看对应步骤。

- 01 使用前必须知道
- 02 第一步：安装 Skill
- 03 第二步：启动前接入大模型
- 04 第三步：启动本地网页
- 05 可选准备：建立“我的标书素材库”
- 06 第四步：填写并保存项目信息
- 07 第五步：上传图片和文档材料
- 08 第六步：点击“开始提取”
- 09 第七步：点击“开始解标”
- 10 第八步：填写人工确认意见
- 11 第九步：点击“大模型逐章撰写”
- 12 第十步：点击“运行校验”
- 13 第十一步：生成 Word 和 PDF
- 14 第十二步：页面质检和人工签发
- 15 怎样判断它确实用了大模型
- 16 中断后继续

这是一套在本机运行的“大模型标书工作台”。普通使用者主要在网页里填写信息、上传材料和点击下一步，不需要理解 Python 命令。

它不是固定模板生成器：大模型负责阅读招标文件、理解评分办法、核对公司证据、规划目录并逐章写作；本地程序负责保存项目、提取文件、检查漏项、生成 Word/PDF 和页面质检。

使用前必须知道

- 标书内容必须经过大模型，未接入模型时网页不会允许创建项目。
- 可以填写任意服务商提供的模型 API，也可以使用 Codex、Claude Code、Hermes、OpenClaw、WorkBuddy 等当前 Agent 已经连接的大模型。网页中的厂商列表只是自动填 URL 的快捷入口，不是限制名单。
- API Key
属于敏感信息。不要在普通聊天消息里明文发送；请在网页密码框或终端隐藏输入中填写。
- 所有项目材料和配置都保存在本机。网页只监听 127.0.0.1，不会作为公网网站开放。
- Skill 不会编造资质、业绩、人员、证书、参数、报价、签章或承诺。

第一步：安装 Skill

把完整的 **biaoshu-skill** 文件夹交给当前 Agent，然后发送：

请安装 **biaoshu-skill**。不要直接覆盖已有同名版本；如已存在，先备份。安装依赖、检查运行环境，然后启动“老诸的Ai朋友圈 · 智能标书工作台”本地网页。模型未配置时先停在模型接入页，不要开始生成标书。

也可以在 Skill 文件夹中自己执行：

```
python -m pip install -r requirements.txt
python scripts/install_skill.py --target codex
python scripts/install_skill.py --target claude-code
python scripts/install_skill.py --target hermes
python scripts/install_skill.py --target openclaw
python scripts/install_skill.py --target workbuddy
```

只需选择当前使用的平台执行一条安装命令。其他平台可以使用：

```
python scripts/install_skill.py --dest "平台的技能根目录"
```

本步逻辑：把同一套通用 Skill 安装到当前 Agent 能识别的位置。

本步产物：平台技能目录中的 **biaoshu-skill/** 完整副本。

第二步：启动前接入大模型

运行标书工作台之前，必须确定模型从哪里来。

方式 A：在网页填写模型 API

普通用户只需准备三项信息：

1. 完整调用 URL：必须是实际接收 POST 请求的完整地址，不是服务商首页或控制台地址。
2. API Key。
3. 模型名称：填写服务商提供的准确模型 ID。

网页可一键选择 DeepSeek、Kimi、智谱

GLM、通义千问、豆包、腾讯混元、硅基流动、OpenAI 或 Claude，并自动填写官方调用 URL。列表中没有的模型选择“其他 / 自定义”，照样可以填写自己的 URL、Key 和模型名。大多数国内模型保持默认协议即可；只有服务商文档明确要求时才展开“高级设置”选择 OpenAI Responses 或 Anthropic Messages。常见地址和填写示例见 [references/model-api.md](#) (references/model-api.md)。

网页会先发送一条极小的测试请求。只有测试成功，项目功能才会解锁。

默认只在本次网页进程内使用 Key。勾选“保存到本机”后，Key 才会保存到当前用户的 `.biaoshu-skill/.secrets/`；页面状态和日志不会回显完整 Key。

方式 B：使用当前 Agent 的大模型

如果当前已经在 Codex、Claude Code、OpenClaw 等 Agent 中，可以选择“由当前 Agent 托管”。网页遇到“大模型解标”或“大模型撰写”时，会生成一条任务指令，使用者把指令交给当前 Agent 执行。

也可以让 Agent 配置模型：

请为 `biaoshu-skill` 配置大模型连接。先询问我使用 API 还是当前 Agent 托管。若使用 API，请让我通过网页密码框或 `configure_model.py --api-key-stdin` 隐藏输入 Key，不要让我在聊天里明文发送。配置后必须测试调用 URL 和模型名，成功后再启动项目。

高级命令：

```
python scripts/configure_model.py --mode agent
python scripts/configure_model.py --mode api --provider openai-chat --endpoint "完整调用URL"
--model "模型名" --api-key-stdin --test
```

本步逻辑：保证后续解标和写作真的由大模型完成，而不是退回固定模板。

本步产物：本机模型配置和连接测试结果；API Key 不会写进标书项目。

第三步：启动本地网页

Windows 普通用户推荐直接双击 Skill 根目录的：

```
启动标书工作台.cmd
```

首次启动会在 Skill 内建立独立 **.venv** 并安装依赖，不会把依赖混进标书项目。macOS/Linux 可运行 **sh start-web.sh**。

也可以让 Agent 启动，或者在 Skill 文件夹运行：

```
python scripts/start_web.py
```

浏览器会自动打开：

```
http://127.0.0.1:8765
```

网页标题应显示：

```
老诸的Ai朋友圈 · 智能标书工作台
```

如果 8765 端口被占用：

```
python scripts/start_web.py --port 8766
```

如需改变项目保存目录：

```
python scripts/start_web.py --data-dir "D:\标书项目"
```

本步逻辑：网页只是本地操作面板，文件仍保存在自己的电脑上。

本步产物：打开的本地网页；默认项目目录为用户目录下的 **BiaoShuProjects/**。

可选准备：建立“我的标书素材库”

如果有以前的标书、资质、案例或技术方案，建议先在网页的“我的标书素材库”中入库。素材库保存在本机用户目录下的

BiaoShuKnowledge/，以后创建的新标书都可以检索使用，不需要重复上传。

操作方法：

1. 选择材料类型：历史标书、资质证书、项目案例、技术方案、企业标准资料或其他材料。
2. 选择使用规则：
 - “仅作参考”：适合历史标书和技术方案，只参考结构、方法和表达。
 - “候选证据，使用前核验”：适合资质、合同、验收材料和人员证书。

- “保存但禁止调用”：材料留在本机，但任何新标书都不会检索它。
- 3. 填写标题和标签，例如“数据治理、政务、中标、运维”。
- 4. 选择 PDF、Word、Excel、图片或文本文件，点击“提取并加入素材库”。
- 5. 使用搜索框输入“数据治理实施方案”等关键词，可以检查是否能检索到目标内容。

本功能不要求额外配置向量模型。系统先使用本地中文关键词、标签和项目类型检索，再由当前大模型判断如何参考。历史标书不会直接整本塞进提示词，也不会自动复制到新标书。

每个新项目默认勾选“自动参考我的标书素材库”。如某个项目涉及严格隔离或不允许使用历史资料，可以在项目信息中取消勾选。

本步逻辑：把“可复用写法”“候选事实证据”和“禁止使用资料”分开管理，避免照抄旧项目或误用过期证书、历史报价和人员承诺。

本步产物：本机 `BiaoShuKnowledge/knowledge.db`、入库文件副本和可检索片段。

第四步：填写并保存项目信息

在网页第一栏填写：

- 项目名称。
- 招标编号。
- 采购人和投标人。
- 投标截止时间。
- 采购类型。
- 完整标书、技术标、商务标或报价标。
- 输出 **Word**、**PDF** 或 **Word + PDF**。
- 页数、字体、装订要求和其他说明。
- 是否自动参考“我的标书素材库”。

点击“保存项目信息并进入下一步”。以后再次打开网页，可从左侧项目列表继续，不需要重新填写。

本步逻辑：固定全书共用的项目事实，避免后续章节名称、日期和主体不一致。

本步产物：独立项目目录和 `project.json`。

第五步：上传图片 and 文档材料

先选择材料类别，再一次或多次上传：

- 招标文件、澄清、补遗、评分办法和官方格式表。
- 营业执照、资质证书、人员资料、业绩合同、验收材料、产品参数和检测报告。
- 报价、工期、质保期和本次项目决策。

- 图片、PDF、Word、Excel、CSV、TXT、Markdown 等。

网页拒绝 .exe 等可执行文件。单个文件默认不超过 100MB。

图片会交给支持视觉理解的模型；如果所选模型不能看图，需要补充 OCR 文本或人工说明。扫描版 PDF 如果提取不到文字，也必须先 OCR，不能让模型猜测。

本步逻辑：招标文件定义“必须回答什么”，公司材料定义“可以真实证明什么”。

本步产物：

- incoming/：网页上传的原始材料。
- sources/：带来源编号和哈希的项目材料副本。
- project.json：材料登记记录。

第六步：点击“开始提取”

系统读取 PDF、Word、Excel、图片和文本，建立大模型可阅读的材料包。

重点查看页面提示中的提取错误、扫描页、乱码和低文字页。关键材料不可读时，先补文件，不要继续解标。

本步逻辑：不同格式先转换为带文件名、页码、表格和来源编号的统一材料包。

本步产物：

- extracted/source-pack.md：大模型材料包。
- extracted/extraction-report.json：可读性和错误报告。

第七步：点击“开始解标”

API 模式下，网页直接调用已测试的大模型；Agent

托管模式下，网页会显示一条任务指令，把它交给当前 Agent。

大模型会逐条分析强制条款、评分项、技术要求、商务要求、资格要求、格式要求和递交要求，并核对公司证据。

本步逻辑：先理解评分和废标规则，再决定怎么写，禁止一上来生成整本通用标书。

本步产物：

- analysis/requirements.json：招标要求清单。
- analysis/evidence.json：公司证据账本。
- analysis/compliance-matrix.md：要求、章节和证据对应关系。
- analysis/risk-register.md：废标、扣分、缺证和冲突风险。
- analysis/knowledge-reference.md：本项目检索到的历史素材摘录和使用规则。
- analysis/knowledge-retrieval.json：可追溯的素材编号、来源文件、匹配分和分类。
- plan/outline.json：建议目录和各章节写作任务。

第八步：填写人工确认意见

网页不会自动跳过这一关。至少确认：

1. 目录和任务范围。
2. 报价、工期、质保期、付款响应等数字。
3. 使用哪些项目人员和业绩。
4. 哪些缺失材料稍后补充。
5. 哪些内部资料不能写入投标文件。
6. 素材库中的候选证据是否仍然有效、属于本公司并适用于本项目。

示例：

目录确认。工期为 60 日历天，质保期 3 年；报价暂不写入；R012 的证书稍后补充，正文保留待补充标记；其他按建议执行。

本步逻辑：事实和商业承诺由人负责，大模型负责整理、推理和表达。

本步产物：[analysis/human-confirmation.md](#) 和确认后的项目状态。

第九步：点击“大模型逐章撰写”

模型按照确认目录逐章写作，并引用要求编号、证据编号和素材库参考编号。技术方案应说明做什么、怎么做、谁负责、何时完成、如何验收。

缺少证据的信息会写成 **[待补充：具体内容]**，不会自动编造。

历史标书和技术方案只用于借鉴结构、方法和表达，模型必须结合本次招标重新撰写；不得复用旧项目名称、客户、人员、金额、报价、工期和承诺。使用知识库候选证据时会保留 **[待核验：素材编号]** 和 **<!-- KB:KBREF-001 -->** 追踪标记。

本步逻辑：长标书拆成可单独检查和修改的章节，同时保持“招标要求—证据—正文”的追踪关系。

本步产物：

- [sections/NN-章节名.md](#)：逐章正文。
- [final/标书正文.md](#)：组装后的统一总稿。

第十步：点击“运行校验”

系统检查漏项、未知证据、缺失材料、未响应评分项、占位符和关键字段一致性。

- **BLOCKER**：必须修复，否则不能生成正式交付物。
- **WARNING**：需要补充、解释或明确接受风险。

本步逻辑：机械校验负责找漏项，大模型和人工负责判断内容是否合理，二者不能互相替代。

本步产物：

- [reports/validation.md](#)：人可阅读报告。
- [reports/validation.json](#)：结构化报告。
- 校验通过后的 [final/标书正文.md](#)。

第十一步：生成 Word 和 PDF

选择 [Word](#)、[PDF](#) 或 [Word + PDF](#)，点击“生成交付文件”。只有严格校验没有 [BLOCKER](#) 时才能生成。

PDF 转换会依次尝试：

1. LibreOffice。
2. Microsoft Word。
3. WPS Office。
4. ReportLab 兼容生成。

安装了 Microsoft Word、WPS Office 或 LibreOffice 时，复杂表格和分页通常更接近 Word 版式；使用 ReportLab 回退时必须重点检查分页和表格。

本步逻辑：Word 和 PDF 使用同一份最终正文生成，减少两个版本内容不一致。

本步产物：

- [deliverables/项目名称-投标文件.docx](#)
- [deliverables/项目名称-投标文件.pdf](#)
- [reports/build-report.json](#)

第十二步：页面质检和人工签发

系统会把 PDF 渲染成图片，检查疑似空白页；使用者还要重点检查封面、目录、密集表格、章节换页、页码、中文字体、图片清晰度和文字截断。

本步产物：

- [reports/rendered/](#)：逐页质检图片。
- [reports/render-report.json](#)：渲染报告。
- [deliverables/](#)：最终 Word/PDF。

正式递交前必须人工确认报价大小写、签字盖章、证书有效期、人员、业绩、投标保证金、文件命名、份数、密封、电子签章、上传平台和截止时间。

怎样判断它确实用了大模型

正确流程中，正文之前一定会先出现：要求清单、证据账本、响应矩阵、风险清单和建议目录。正文应明确对应本次招标的具体评分项与公司证据。

如果系统跳过分析直接生成大量通用段落，或者没有要求编号、证据编号和校验报告，就没有按本 Skill 的正确流程执行。

中断后继续

重新运行 `python scripts/start_web.py`，从左侧选择原项目即可。不要删除项目目录，也不要重新创建同名项目。

Agent 托管模式可发送：

请继续 biaoshu-skill 项目。项目目录是 “××”。先读取 project.json、已有 analysis、sections 和 reports，告诉我当前阶段、未解决 BLOCKER 和下一步，再从断点继续，不要覆盖已确认内容。