REUPPlus 如何与 ChatGPT 接口规范吻合

REUP+ 要与 ChatGPT 接口规范吻合，关键是在现有网站和业务后台之间，增加一个符合 MCP 标准的服务接口。 这个接口把您的“需求审核、服务商配对、招投标和项目跟进”转换成 ChatGPT 能理解、能调用、能验证结果的工具。

网站可以继续承担品牌展示和客户入口；接口负责实际业务操作。以下可作为交给建站和开发团队的实施要求。

1. 先明确接入方向

两种建设容易混淆：

建设方向	用途	与您的目标关系
REUP+ 网站调用 OpenAI API	网站内提供 AI 咨询、需求整理	提升站内服务
ChatGPT 调用 REUP+ 接口	ChatGPT 用户直接查询、提交需求、跟进项目	承接 ChatGPT 用户需求

您本次要实现的是第二种。

建议架构为：ChatGPT 通过 REUP+ 的 MCP 接口，调用同一个业务后台；网站也使用这个后台。这样客户在两个入口看到的项目、报价和进度保持一致。

2. 技术接口需要满足哪些要求

官方文档要求 MCP 服务支持 **Streamable HTTP**，部署到稳定的接口地址，通常使用 `/mcp` 路径。公开提交需要可访问的 HTTPS 服务。每项工具都应有明确名称、说明、输入结构、适用的输出结构和真实的行为标注。OpenAI Developers

可以规划类似这样的地址：

```
https://api.reupplus.com/mcp
```

这是建议地址，尚未代表已经部署。

接口要求	REUP+ 如何落实
工具名称清晰	“查询服务覆盖”“保存需求草稿”，分别提供
输入字段明确	地区、项目类型、预算、时间等有固定格式
输出结构固定	返回需求编号、状态、候选和下一步
数据有稳定编号	同一项目始终使用同一个 project_id
操作行为如实标注	查询、修改、发布和外部联系分别标注
错误可理解	明确区分未登录、资料不足、无匹配和系统故障

3. 将运营流程拆成几个独立工具

以下工具名称是针对 REUPPlus 的建议，并非 OpenAI 指定名称。

建议工具	对应业务	权限及控制
check_service_coverage	查询地区和业务覆盖	可匿名查询公开信息
save_request_draft	保存客户需求草稿	登录，限定本人账户
get_provider_matches	查询符合条件的服务商	只返回有权查看的资料
publish_tender	正式发布招标、邀请供应商	验证确认、权限与共享范围
get_project_status	查询项目阶段和待办	仅项目授权人员可查
request_human_support	创建人工协助工单	登录，返回工单编号

第一版建议先实现覆盖查询、需求草稿、候选配对和项目状态。 正式招标发布等对外操作，等前四项稳定后再开放。

需求草稿至少应包含：

- 项目类别、城市或邮编、工作范围。
- 预算区间、币种、期望时间。
- 已提供的信息与仍待确认的信息。
- 客户是否同意向候选服务商共享资料。

预算没有提供，就记录为“待确认”；不能让 AI 自动填成客户承诺的预算。

4. 返回结果要让 ChatGPT 能继续办事

官方支持通过 `structuredContent` 返回结构化数据，通过 `content` 提供可读说明。稳定编号能让后续工具继续操作同一条记录。OpenAI Developers

例如，保存草稿后可以返回：

```
{
  "structuredContent": {
    "request_id": "req_001",
    "status": "draft",
    "missing_fields": ["budget", "target_start_date"],
    "next_action": "complete_missing_fields"
  },
  "content": [
    {
      "type": "text",
      "text": "需求草稿已保存，还需确认预算与开工时间。"
    }
  ]
}
```

这是示意结果。实际开发时，必须与工具声明的输出结构一致。

候选结果还应包含**匹配理由、审核状态、资料更新时间**。报价必须区分估算与正式报价，档期必须区分参考信息与已确认安排。

5. 登录和操作确认必须由后台落实

查询公开服务可以不登录；查看私人项目或执行写入操作，应采用符合 MCP 授权规范的 **OAuth 2.1**。服务器需要逐次验证令牌及权限，不能仅凭 ChatGPT 传来的用户编号判断身份。OpenAI Developers

对 REUPPlus，重点落实三个控制：

- **项目访问权限：** 屋主、施工方、平台人员只能查看被授权的资料。
- **正式发布确认：** 草稿确认后，才允许共享客户资料或邀请供应商。
- **重复请求保护：** 网络重试不能造成重复招标、重复邀请或重复收费。

官方的 `readOnlyHint`、`destructiveHint`、`openWorldHint` 等标注帮助 ChatGPT 判断操作行为，但不能替代服务器自己的授权和确认检查。OpenAI Developers

6. 界面可以后加，先把业务调用做好

第一版即使没有定制界面，也能通过工具返回结果。后续再增加：

- 服务商比较卡片。
- 需求确认表。
- 报价对比表。
- 项目进度和待办。

ChatGPT 当前支持通过 **MCP Apps** 标准展示接口返回的交互界面。OpenAI Developers

7. 验收不能只看“接口连接成功”

开发团队至少应证明：

验收场景	合格结果
客户需求不完整	生成草稿，指出缺失信息
服务地区不覆盖	如实返回，不虚构候选
客户查询他人项目	后台拒绝访问
同一请求重复提交	不重复创建业务记录
客户要求发布招标	按权限和确认规则执行
客户继续追问项目	使用原项目编号，返回最新状态

官方建议先用 MCP Inspector 检查工具，再在 ChatGPT 开发者模式测试直接请求、间接表达、后续追问、写入操作和不支持的请求。OpenAI Developers

您可以直接向开发团队提出这条要求：

> **为 REUP+ 建设符合 MCP 标准的 ChatGPT 接口，共用网站业务后台，先实现服务覆盖查询、需求草稿、服务商配对和项目状态查询；落实 OAuth 登录、项目权限、结构化结果、重复请求保护和操作日志，并完成 ChatGPT 端到端验收。**

另外，**MCP 接口接通本身不等于主动商业已经实现**。长期目标记录、变化检测和提醒调度仍需由 REUP+ 后台建设；接入 ChatGPT 也不代表可以任意主动联系用户。