赛前熟悉资料包

Zettlab × 进迭时空 校园 Hackathon | 选手版

智能体电脑 / Agent Computer

一句话：在 K3 开发板上做一台面向家庭场景的 Agent Computer，让它能听、能看、能说、能办事、能留下可审计记录。

48h 目标：跑通 App 输入 -> K3 处理 -> App 展示结果，并沉淀成可复用的 feature 或 Skill。

现在先看什么	系统架构、三档递进路线、安全底线、K3/Spacemit 公开文档。
现在不用等什么	不用等待完整软件包合集。已有 agent 入口和 token 后，大多数软件接入可由队伍自行完成；私密 token 会另行发放，不应写进资料包。
还没正式发布什么	正式赛题与评分细则按筹备说明定于 7月15日发布；本文是赛前熟悉材料，不替代 7月15日正式文件。

现场硬件以组织方发放为准：K3 Pico-ITX / K3 CoM260 kit、摄像头、麦克风、音响等。

参赛作品应该长什么样

把它理解成一条完整闭环，而不是一个孤立模型 Demo。App 是中枢，K3 是本地处理大脑，选手把自己的功能入口和可复用 Skill 接进去。

1. 外设输入	智能眼镜、摄像头、麦克风、录音笔等先进入 App 或已封装外设 Skill。
2. App 中转	App 负责收输入、调 K3、展示聊天窗/学习卡片/操作结果。
3. K3 本地处理	ASR、TTS、VLM 等多模态能力优先在 K3 本地完成。
4. 最终交付	一个可演示的 feature，加一个可复用 Skill，并能在 App 里看到结果。

系统架构：App 是中枢，K3 负责处理

下面这张图用于让选手快速理解底座分工：外设接入 App，App 把语音/画面交给 K3，K3 返回结果给 App 展示。

关于云端与本地的边界

赛前熟悉阶段先按“本地优先”理解：语音、画面、家庭数据和可审计 trace 应留在 K3 或本地设备侧。

图中“云端重推理”是架构参考，不代表入门闭环可以依赖云端 LLM。正式允许范围以 7月15日赛题和评分细则为准。

三档递进：必须按顺序跑通

不要跳档。入门版没跑通，进阶和挑战即使功能看起来更炫，也无法证明作品闭环成立。

档位	能力目标	功能要求	安全要求
入门版 必须先完成	听 + 说 单轮闭环	K3 ASR 把语音转文本；hermes Agent 调至少 1 个本地工具；K3 TTS 回播；端到端不依赖云端 LLM。	S1 数据本地化；S2 最小权限 manifest；S3 副作用动作二次确认；S4 本地 trace 可审计。
进阶版 依赖入门	看 + 记 + 多轮	接入 K3 VLM 摄像头输入；多轮对话和轻量记忆；完成一个家庭场景 Demo，如冰箱菜谱、便签建提醒、看护异常推送。	S5 操作可逆/快照回滚：写文件先快照，>= 7 天回滚窗口，删除进回收站。
挑战版 依赖进阶	办 + 可上架 Skill	封装为符合 hermes Skill 规范的可发布 Skill；另一台 K3 扫码安装后 <= 60s 出声；给家庭用户一张“能干什么/不能干什么”报告卡。	S6 抗 prompt injection；S7 本地人脸/声纹差异化权限；S8 工作区沙箱 + Diff 预览。三项至少完成 2 项才进入第一档评分范围。

底线提示

入门版 S1-S4 任意一条缺失、数据上云被抓包、或越权注入测试失守，都属于高风险问题。赛前就把这些作为产品需求设计进去。

赛前资料清单：先熟悉，不等安装包

这份 7月6日资料包适合提前发给选手，用来建立共同语境。具体账号、token、仓库权限和现场环境由组织方另行开通。

类别	选手现在要知道什么	资料状态
硬件/平台	K3 Pico-ITX 或 K3 CoM260 kit，预装 Ubuntu / Bianbu，并接入 Spacemit AI SDK；每队现场以发放设备为准。	组织方提供
外设工具包	摄像头、麦克风、音响、智能门铃等外设及接入方式，用作“看、听、说”的输入输出。	筹办方提供
Zettlab 软件入口	zettlab-app、hermes-agent、Skill SDK、local-server、Skill Store 上架接口等能力，原则上通过 agent 入口和 token 接入；不需要把所有软件包提前打成资料包。	agent/token 开通后自助接入
token/API Key	由 Zettlab 发放给队伍或现场账号；不要放进公开 PDF，不要截图传播。	另行发放
赛题/评分	正式赛题和评分细则按筹备说明定于 7月15日发布。当前 PDF 只用于提前熟悉技术路线。	7月15日另发

建议提前打开的公开文档

Spacemit AI SDK：ASR / TTS / LLM / VLM
https://www.spacemit.com/community/document/info?lang=zh&nodepath=ai/application_tools/ai-sdk.md

AI Computer 解决方案
https://www.spacemit.com/community/document/info?lang=zh&nodepath=ai/solutions/aicomputer_solution

K3 Pico-ITX 开发板 Wiki
https://www.spacemit.com/community/development-kit/k3-pico-itx

K3 CoM260 开发板 Wiki
https://www.spacemit.com/community/development-kit/k3-com260

选手行动清单

7月15日正式赛题发布前，先把下面几件事想清楚。这样拿到 token 和现场设备后，能直接进入实现。

建议先做

选一个家庭场景：冰箱菜谱、便签/收据、老人/小孩看护，或自定义但同样清晰的家庭任务。

画出你的链路：外设输入 -> App -> K3 -> Agent/Skill -> App 展示。

列出 Skill 需要的权限：mic、camera、fs、network、profile 等，默认最小化。

设计 trace：记录输入摘要、工具调用、出参、时间戳和调用 profile。

准备一个本地优先方案：没有云端 LLM 时也能跑通入门闭环。

不要这样做

不要跳过入门闭环，直接做复杂挑战版。

不要把 token、API Key、家庭原始语音/图像写进代码仓库或展示材料。

不要默认上传家庭隐私数据到云端。

不要把安全当成最后一天补丁，权限、确认、审计和回滚要从第一版做进去。

不要等完整软件资料包才开始，先按本文理解架构和接口边界。

资料包来源

相关说明.txt：筹备进展、硬件/网络/token/评估分工、7月6日资料发布与7月15日赛题评分发布时间。
zettlab选题清单表.xlsx：赛事主题、赛道命题、三档递进、安全基线、参考资料。
赛题提报表.xlsx：与 zettlab选题清单表.xlsx 内容一致，作为交叉确认。
参赛作品的数据流.pic.jpg、参赛作品功能相关说明.jpg：作品闭环与系统架构图。
crop-pico板子.png：K3 Pico-ITX 开发板视觉材料。

可直接给选手看的版本说明

本文刻意不包含私密 token、账号、仓库权限和未定评分细则。发给选手后，组织方只需要再补充实际领取方式、群通知和7月15日正式赛题链接。