

基础设施架构：从一部手机到更广阔的真实世界

C0-013-PART-III-6L · 19 aligned sections · English canonical master · AI-assisted translation · independent professional review pending

GENAI PHYSICAL · INFRASTRUCTURE PROPOSITION

从 App 控制的智能产品，迈向人类治理的物理能力

百亿手机激活并非已经拥有百亿台在线设备，而是一场让全球现有个人和共享硬件参与真实 Work 的开放邀请。传统 App 智能家居只展示了物理能力冰山的一角：灯光、开关和传感器原本就有可用的物理功能，却往往围绕各厂商界面组织。更大的机会是把设备、场地、物料、技能、制造及无障碍服务组合起来，而不要求所有参与者属于同一品牌或云平台。

架构变化的关键，是将 Human Authority 明确放在受控本地边界。云端模型可以建议计划，MCP Client 可以调用声明过的工具，但涉及实际效果的动作仍须经过权利主体授权的本地策略、真实设备权限、独立物理安全保护及具名的人类验收。云端可以继续参与；把最终执行控制点靠近人，并不等于绕过合法配对、产品安全或商业权利。

CHAPTER 7 / HSIMC BLUEPRINT

7. 手机是第一个节点，而不是系统的边界

合格手机是进入受人控制的 Reality 的入口，并非控制一切的资格

PROPOSITION

旧手机能够同时提供感知、显示、无障碍交互、数据及连接，但价值来自与合格设备、服务和人类能力安全组合，而不是把手机简单宣布为 AI 可以任意接管的机器。

7.1 手机原生能力：感知、显示、存储、连接与运算

退出主力使用的手机仍可能保有摄像头、麦克风、屏幕、扬声器、惯性传感器、定位、存储、Wi-Fi、蓝牙和有限算力。它们可以参与获同意的状况记录、无障碍公共界面或有监督的检查。手机不必自行运行大模型：轻量分类器、人类操作员、共享 Local Edge 或经选择调用的远端模型都可能帮助完成结果。

不能仅凭手机年代或 USB-C 接口就判定适用。电池、散热、系统安全更新、摄像头权限、可访问性、存储、网络可靠性及供电，均可能使设备不适合某项 Work。NPU 也并非所有框架都能调用；Android 15 已弃用 NNAPI，实际端侧性能必须按设备和模型测量 [E8]。

7.2 可访问的外部能力：USB 设备、NFC 物件、传感器与授权网络服务

现有智能家居 App 说明我们已经具备怎样的物理基础：配对的灯具、开关、传感器、温控器及 Hub，可通过获准的集成提供状态和动作。合格手机还可连接 USB Host 或配件、蓝牙设备、Wi-Fi 服务、NFC 标识及专用适配器。场景不限于家庭，还可延伸到小作坊治具、检验仪器、低压继电器、共享告示站、教育、无障碍和受监督的微型制造。

MCP 负责呈现可调用工具和资料，不会凭空赋予 USB Host、Matter 信任域、厂商 API 权利或安全马达驱动。Android 的 USB 设备访问需要相应操作系统权限及硬件支持 [E6]；Home Assistant 的 MCP Server 可以有选择地暴露实体 [E3]；Matter 使用安全配对和 Fabric 凭证，多管理方也须分别具备权限 [E4、E5]。每个适配器只能声明实际可读或可操作的内容。

7.3 组合节点对某一层是 Server，对另一层可以是 Client 或 Host

Node 是组合中的职责，不是手机或 AI 人格的同义词。一台手机内，可见的 Host 应用负责用户批准，MCP Client 调用受信任的本地 Server，而 Server 再经独立 USB、Matter 或厂商适配器访问设备。手机也可以向授权工作站提供受限服务，同时消费另一节点的传感能力；协议角色与真正的设备权利人始终分开。

这种分层避免把全权控制交给通用云端模型。能力发现、推理、策略判断、执行与证据可以部署在不同位置，使用不同身份。每次跨越边界须验证调用者、权限范围与事实证据；接口调用成功并不代表上层拥有底层资产。云端提出的计划可以进入本地作为候选，由本地 Authority Gate 拒绝不合格动作，且无需上传私人凭证。

7.4 Phone → Local Hub → Personal Reality Pod → Team → Company → Community

合格手机只是起点。Local Hub 提供稳定供电、受控网络和共享运算；Personal Reality Pod 加入可负责的场所与人的生活条件；Team 形成有监督的角色；Company 提供合同内的制造与服务；Community 把各自获授权的资源协作起来。这是可能的联邦式能力网络，而不是一座由 HSIMC 中央拥有的百亿设备机房。

网络应靠自主加入的契约和结果证据扩展，而不是默认全球扫描。学生可以借助安全的摄像站，创客可以供应一件定制支架，供应商可以完成合格订单，而不需要交出企业身份或客户数据。对于不能持续使用移动互联网的人，应提供无障碍、现场监督与延迟同步选项，而不是假定人人都有合格手机 [H1]。

7.5 可访问不等于拥有、可用、安全或已获授权

设备响应 Ping 或显示在某个集成目录中，并不意味着可以调用。技术可达性必须与产权、实际占有、用户同意、个人资料、安全、固件可信度、现场条件以及商业执行权分开。厂商 App、Matter 配对及 MCP 授权令牌分别代表不同关系，都不能单独证明某项全新生产 Work 已获准。

目录既要报告合格，也要报告拒绝：REFERENCE_ONLY、DISCOVERED、AUTHORITY_PENDING、QUALIFIED_FOR_SPECIFIED_WORK、TEMPORARILY_UNAVAILABLE 或 REJECTED。系统应能解释为何没有通过。对于数字技能有限的人，清晰的拒绝原因与联系真人监督者的办法，与成功运行同样重要。

7.6 电力、网络、交互、结构与受控物理动作

真正生产力依赖 App 演示容易忽略的细节：安全供电与电池、USB 角色协商、线材质量、网络边界、安装固定、无障碍屏幕、照明、环境防护、执行器额定值、继电器隔离和紧急停止。外接显示能力取决于具体机型，USB-C 外形并不证明 DP Alt Mode；Android MediaProjection 通常需要用户对每次会话同意和满足前台服务要求 [E7]。

旧手机能运行模型或 MCP Tool，并不意味着适合持续高功率或安全关键控制。应使用独立测试的硬件联锁与本地确定性控制逻辑，将模型命令限制为校验后的参数。在没有合格硬件和人员时，只取得观察证据、转交人工审核，不应自动启动水泵、加热器、门锁或机器。

7.7 从建筑物参考地址到获授权的房间、设备、时间与能力证据

建筑 Registry 能说出房间或地址，设备 Registry 能给手机命名，但这不等于可执行 Work 的 Reality。真正绑定必须包括现场负责人、具体设备和适配器、网络与环境条件、预约时窗、使用许可、人员监督、验收测试及有效期。所有门槛都有当前证据，才可进入 ACTIVE_FOR_THIS_WORK。

例如在受监督的维修台借用手机，持有人允许针对某样品拍照，操作员验证光照与尺度参考，请求人对带日期的报告验收或拒绝。预约结束后能力许可可以失效，但获准保留的证据与 Work 身份延续。这只是候选契约模板，不是已经完成实机部署的宣称。

WORK / DECISION TEST

第 7 章的验收标准是：另一位测试者能分别识别手机的真实职责、外部能力、负责人员、本地条件及安全拒绝，而不会把联网设备误当作 HSIMC 拥有的全球执行节点。

8. Tools、Resources 与 Capability Contracts

将技术可访问性转化为准确、可撤销的能力承诺

PROPOSITION

MCP 可以发现和调用工具，但实际 Work 还需要独立契约，说明某项物理能力由谁、在哪里、在何期限内、以什么成本和风险、按怎样的证据与验收方式提供。Capability Contract 是 HSMC 的设计层，不是 MCP 自动附送的功能。

8.1 MCP Tools：明确输入、输出及执行边界的可调用函数

Tool 是具有名称、输入输出 Schema 和元数据的可调用操作。2026-07-28 MCP 规范的工具协议并不绑定某一种设备或界面；其安全规定要求 Server 校验输入、执行访问控制、限制频率和清理输出，并为有影响的动作保留人类监督 [E1]。相同工具名可能由 App 桥接、本地控制器或远端 API 实现，名称相同不代表安全性等价。

必须分开观察与执行。read_light_state、propose_fixture_inspection 可以是低影响操作；set_lamp_level 应规定设备、范围、当前上下文和回读；energize_heater 或 operate_machine 还可能独立安全系统和合格人员批准。不得把任意 execute_hex、Root 指令或不受限 GPIO 当作普通模型工具。结果必须是设备真实回读或明确失败，不能编造成功。

8.2 MCP Resources：URI 可寻址的资料与上下文，不代表实体资产所有权

Resource URI 可以指向规范、Schema、观察记录、状态快照或工作证据；它不能转移设备产权、数据权利或执行器控制权。获准读取房间温度不等于能修改加热器；指向产品记录的二维码也不是权利人签署的委托。

Resource 必须注明来源、时间新鲜度、拥有者、保留期限、敏感性和允许接收者。公开的机器规格应与私人设备身份、客户历史、位置轨迹及访问凭证分开。用户应清楚哪些信息会离开 Local Edge、哪些汇总证据允许同步；把数据放进模型上下文，并不能取代正式的数据治理。

8.3 以受治理的接口呈现外部设备、场所、材料与专业技能

既有“智能产品”只是实体能力冰山可见的一角。合格手机通过适配器，可观察继电器状态、带标识的产品、作坊检测仪、摄像治具、供电线缆、房间条件、本地技能或授权供应商。Home Assistant 与 Matter 说明已有家庭设备如何进入标准化接口；工业、社区服务还依赖材料、安全和专业人工 [E3、E4]。

可互通不等于无条件绕开 App。Matter 设备通过加密凭证加入 Fabric，并且必须在获准配对后才能工作；某些厂商的特定功能仍可能依赖云端 [E4、E5]。涂鸦、Aqara 等集成必须满足真实协议、厂商条款与设备兼容性。伙伴只开放部分能力时，应尊重其范围，而不是假定能够完全控制。

8.4 Capability Manifest：来源、当前状态、限制、依赖与验收证据

Capability Contract 把真实提供者、设备和特定 Work 目的绑定到一项受限操作。至少记录能力 ID 与版本、所有权人和操作员、接口、输入输出 Schema、设备及 Reality ID、动作范围、到期时间、调用额度、同意要求、物理联锁、当地或云端路径、撤销、证据格式、测量方法与验收责任人。签名和版本有助于核验，但不代表这些字段都属于原生 MCP。

例如测试灯光契约可以允许会话内 read_state，经可见批准后执行 10–60% 范围内的 set_brightness；离线执行只有事先明确授权才成立。本地控制器需要回读实际状态，对超过额度或场所不符的请求予以拒绝。我们附上非执行用途的样例契约，真实设备运行前仍须独立验证。

Non-executable Capability Contract blueprint / JSON ↗

8.5 选择性发现与贡献，不公布整台设备或所有可达资源

隐私与稀缺性决定了不能默认完整暴露。家庭可以只贡献一项相机分析结果，公司可以只提供一个维修时段，供应商可以只公开产品规格；共享社区节点不应公开全部硬盘、账号、传感器或员工身份。MCP 基于每次请求的授权可按调用者限制所见工具 [E1、E2]，HSMC 再将目的约束和选择性披露叠加其上。

发现应分阶段推进：候选参考 → 权利人批准的概要 → 资格检测 → Work 专属授权 → 有限调用 → 真实证据 → 验收或撤销。公开 Capability List 不代表永久可用。这样，一个人可以借助社区节点参与，而不用把私宅暴露成全球遥控入口。

8.6 品牌、商标及能力权利：互相独立的资产与许可

设备接口、产品品牌、数据许可、公司商业权限及权利人的设备控制权是不同对象。HSMC 不能仅凭公开兼容方式就获得 Tuya、Apple、Matter、Home Assistant、Pannex、InnoSpire 或金智维的权益。传统客户和制造商也不必先接受 HSMC 整个母架构，才可以为合格 Work 提供某件产品。

契约应清楚列明谁销售、供应、操作、保险、维修和验收；知识产权归谁，是否允许展示商标。提及厂商 API 只说明潜在技术路径，不代表获得许可、背书、保修或合作承诺。独立伙伴可以参与特定 Work，而不破坏长期形成的关系。

WORK / DECISION TEST

只有当第三方能检查 Capability Contract，明确合法操作员、调用范围、允许环境、撤销路径与实际设备回读，并区分 MCP 互通、商业许可和安全授权，第 8 章才算通过。

9. Human Authority: 可执行的权限边界

让最终重要决策靠近人，而不是交给不受约束的 Agent

PROPOSITION

GenAI 生产力变革不是取消人类同意，也不是自动把所有云端权利搬到手机上，而是让真正负责的人能够控制可验证的本地策略和执行关口；当用户授权时，云端智能仍可协同。

9.1 产权、Android 权限、Client 身份与 Work 授权是不同关系

家电拥有者、配对设备的账号、授予相机或 USB 权限的手机系统、MCP Client 身份，以及获准执行该 Work 的主体可能各不相同。本地保存厂商 Token 不能将权限无限扩张。Matter 的 Fabric 凭证建立设备信任域；MCP 传输授权可限制 Client，二者都不能取代人对特定物理动作的独立批准 [E2、E4、E5]。

Work 开始前应列出能力 / 权限映射：权利人或合法保管者、本地监督者、认证主体、物理目标、数据接收者、拟议动作及有权拒绝者。隐私敏感任务必须让人看清哪些观察会传给云端；高影响操作即使云端给出漂亮理由，仍须通过本地 Authority Gate 校验。

9.2 按目的、期限、使用次数及接收方授权特定能力

授权是一项边界狭窄的委托，不是把整台手机切换为全球公开设施。最小范围应包括 Work 名称、目标能力、允许的动作及参数、角色、过期时间、额度、场所与网络边界、获准接收证据者及监督要求。权利主体应在本地持久保存可审计版本，并让用户能够查看。

超出范围的请求必须在物理效果发生前拒绝。读取室温的授权不能开启暖气；只拍一张样品的许可不能扫描相册；承包商维修权限不能自动变成处理另一家公司客户业务的权力。模型建议、二维码及未知 Tool 输出在经过有效授权核验前都属于不可信输入。

9.3 简单批准、可见活动、无障碍撤销与执行中安全收尾

Human Authority 必须让非专家和无法依赖精细触摸操作的人理解。清楚展示会发生什么、涉及哪台设备、哪些数据离开本地、预计成本和动作是否可逆。提供批准、拒绝、暂停、撤销、人工联系方式及已尝试动作的记录。涉及生命财产风险时，单靠点“确认”仍不够，必须有独立安全联锁与合格人员。

撤销应立即阻止新请求，也要定义正在执行的动作如何进入安全状态。物理控制器而不是云端文本模型应执行超时、范围限制、停止命令和独立联锁。马达已经运转时，删除 Token 不会自动让机械系统倒回原状；契约应明确受控停机、人工覆盖和动作后的证据。

9.4 维护权限与普通 MCP Work 权限严格分离

安装 Android 服务、更新 Ubuntu 或替换继电器驱动，维护人员可能需要短时管理员权限，但不能复制给日常 Work 身份。系统部署、凭证轮换、软件修补、恢复操作，与低权限感知或任务执行必须分开；任何紧急提权都要记录和复核。

本地 MCP Server 本身可能带来代码执行和数据暴露风险：本地启动的进程若未隔离，可能继承宿主账号的文件、浏览器和网络权限。官方 MCP 安全文档明确区分主机层隔离与协议认证 [E9]。HSMC Local Edge 应默认受限服务账号、已声明资源、短时授权，并禁止向不可信网络暴露调试端口。

9.5 仅本地、私有小组或选择性共享，不默认全球公开

参与方式应明确分层。LOCAL_ONLY 把工作资料和执行许可留在受控现场；PRIVATE_GROUP 允许具名家人、员工或学生共享限定能力；SELECTIVELY_SHARED 在明示商业与同意条件下向社区发布经过筛选的贡献。新发现的手机、智能插座、传感器、Hub 和办公室设备，默认不应全球发现。

云端可提供语言理解、计划与可选同步，本地 Authority Gate 负责最后的动作合法性判断；有些 Work 可安全离线继续，有些必须等待获准联网。这不是回到封闭 App 围墙，也不是不受治理的万能遥控。共享设施可以帮助没有自有优质手机的人参与，但不能宣称 22 亿离线人士已经具备合格设备 [H1]。

9.6 个人关系或维护访问不自动继承公司授权

创始人与 Pannex、InnoSpire、合作伙伴及供应商的长期角色，是真实重要的关系，却不自动允许 HSMC 操作其公司资产、读取客户数据、展示标识或将员工绑定到新 Work。必须分开个人信任、交谈、技术可达性、商业协议及有责任主体的企业正式批准。各家公司按独立权限作出贡献。

这样的边界不会缩小全球号召，反而使之可信。世界各地独立的手机持有人和物理能力提供者可以加入，不必将身份出售给中央平台。第一个可复制证明不应是炫目的继电器自动演示，而是获授权请求、本地受限动作或拒绝、观察到的物理结果、人的验收和可重读证据。

当真正的权利人能够授权一项受限动作、看见尝试与实际结果、拒绝或撤销，并证明未经授权的模型请求被安全拒绝，同时没有泄露秘密或转移公司权利时，第 9 章才通过。

Evidence and verified technical boundaries

1. [E1] [Model Context Protocol · Tools specification \(2026-07-28\)](#) — Tool schemas and mandatory server controls; human oversight.
2. [E2] [Model Context Protocol · HTTP Authorization \(2026-07-28\)](#) — Transport authorization distinct from local operating-system privilege.
3. [E3] [Home Assistant · MCP Server Integration](#) — Official integration and selectively exposed devices/entities.
4. [E4] [Google Home Developers · Matter commissioning](#) — Device pairing and cryptographic operational commissioning.
5. [E5] [Google Home Developers · Matter fabric and multi-admin](#) — Secure fabric domains, credentials and multi-admin boundaries.
6. [E6] [Android Developers · USB host overview](#) — Device-dependent USB hardware and user permission.
7. [E7] [Android Developers · Media projection](#) — Per-session capture consent and foreground-service requirements.
8. [E8] [Android Developers · NNAPI migration guide](#) — NNAPI deprecated; inferencing runtime performance not universal.
9. [H1] [HSIMC · C0-009 archived 30-chapter blueprint and Part II](#) — Internal design history and boundary, not independent official field certification.
10. [E9] [Model Context Protocol · Local Server Security \(official source\)](#) — A local MCP child process can inherit host access; isolation and least privilege matter beyond protocol auth.

[Exploratory-source claim audit / evidence scope ↗](#)

STATUS / BOUNDARY. HSIMC 研究白皮书；实际资产始终归其权利主体控制。本章不代表已经操作外部设备或获得公司授权。百亿手机是全球参与愿景，不是经核实的设备数量。AI 辅助翻译仍需独立专业审校。

NEXT GATE. 冻结英文 Part III 主稿；五语按全部 19 个小节一致翻译，生成可阅读的 A4 和网页版本，独立检查引用、阿拉伯语排版及浏览器跳转，再发布新的独立版本，不改动 C0-009、C0-010-R1 或 C0-012。