

CHAPTER 1 / HSIMC BLUEPRINT

百亿手机激活机遇

从全球倡议到可验证、有实际价值的能力

PROPOSITION

“百亿手机激活”是一项战略倡议与研究假设，并非已审计的闲置、安全、可接入或可部署手机数量。衡量成果的标准是实际用户接受的一项有用 Work，而不是仅被统计或连线的设备。

1.1 消费性淘汰与剩余生产能力

手机虽然退出个人日常使用，仍可能保留摄像头、屏幕、麦克风、传感器、存储、网络或无障碍界面。消费换机与技术失效不是同一回事。设备不需要运行大型语言模型，也能收集证据、显示同意决定、充当受监督终端，或将合格的本地能力连接到获授权的 Work。

剩余功能不等于实际就绪。必须针对具体用途检验电池、电气安全、操作系统支持、网络隔离、遗留个人数据、权限与无障碍条件。不安全或无法保护数据的设备应考虑维修或合规回收。再使用是否具环保及经济效益，应实测而非预设。

1.2 闲置手机是分散的起点，不是集中拥有的库存

潜在设备分别由家庭、企业、学校、维修商、慈善机构等独立持有。所有权、占有与使用许可仍属于各自权利人；HSIMC 不能将其视为自有库存。闲置不代表遗弃、可转让或可安全接入；参与从可识别、愿意参与的持有者和明确限定的用途开始。

可信的激活记录应包括持有者授权、必要且最少的设备描述、检查结果、预定角色，以及明确的停止或撤销途径。普通网址或 QR 可作为入口；合格 NFC 和本地适配器是可选路线，而不是前提。不预设统一恢复出厂、Root、侧载或管理权限。

1.3 现存规模、未来退役设备与 AI 采用情景

全球规模数据说明相关性，却不能直接变成可执行库存。ITU 估计 2025 年有 60 亿人使用互联网，22 亿人仍离线 [E1]。GSMA 报告 2025 年末移动互联网用户为 48 亿 [E2]。这些数字在不同定义下统计的是人，不是可用于 Work 的实物手机。ITU 与 UNITAR 记录 2022 年全球各类电子废物 6,200 万吨，其中 22.3% 有正式收集回收记录 [E3]；不能据此换算可再用手机数量。

因此，“百亿”应作为长期参与愿景接受检验，而不是当前合格节点的事实数字。必须分开统计现有留存设备、未来退出主要用途的设备、报废或回收流向，以及重复登记。低 / 参考 / 高三种情景需要实际样本、去重规则、透明的资格假设与定期修订，不能由通信订阅数直接外推。

1.4 从估计设备到合格节点、活跃贡献者与被接受的 Work

衡量链条必须清楚：观测候选设备 → 持有者授权 → 安全可操作 → 接口可访问 → 能力合格 → 动作完成 → 人类接受的 Work。每一步分别记录分子、分母、证据与拒绝原因。有 Wi-Fi 不等于 MCP Server；工具调用成功不等于服务交付；动作完成也不等于成果已获接受。

HSIMC 应衡量获取首个有效证据的时间、独立操作成功率、监督投入、重复验收率、总成本及失败 / 撤回比例。设备、操作人、工作请求与接受成果应分别去重。少量可以复制的真正成果，比大量未核验地图图标更具说服力。审核者应能沿 Intent、Authority、Reality、Action、Evidence、Acceptance、Continue 追溯整项 Work。

试点台账应区分设备记录、操作人、Work 请求和验收决定。个人资料与设备标识默认保密，仅保留合法且特定 Work 必要的信息；汇总结果的发布也须获许可。可验证 Work 意味证据可以被独立审查，而非保证手机永久在线。

1.5 手机优先的邀请及更广泛的既有资产机遇

第一个邀请应具体：带来一部已有手机，在避免不必要数据读取的前提下检查，选择受限任务，披露所需权限，并产出别人可核实的结果。例如，获授权操作员可使用合格手机记录产品可见状况，提交带日期的证据供人审阅；必须能接受、拒绝、删除或撤回。这只是候选 Work，并非已部署事实。

手机是入口，不是边界。合格充电与数据线、NFC 实体标识、固定装置、传感器、本地计算及人员服务，都可能补足手机缺少的条件。有些任务根本不需添置产品，有些不应继续。HSIMC 的基础设施机会，是找到有价值且获授权的 Work 所缺的最小条件，并在现场核验结果。

首个模板还须有真正的拒绝关卡：危险供电、无支持的软件、不清楚的证据，或持有者撤回同意，都应停止任务，仅保留获许可的失败证据。可信服务必须包括正确拒绝；不同语言、地点及法规环境应能复制方法，而不转移所有权、个人数据或企业控制权。

WORK / DECISION TEST

只有真实试点分别报告候选、授权、安全合格、能力可用及独立接受的 Work 数量后，才可推进本章主张。若成本、风险或权限不足使此路线不如其他方案，正确结果是修订或拒绝，而非夸大手机数量。

PUBLIC EVIDENCE · SOURCE LINKS

[E1] [International Telecommunication Union \(ITU\) · Measuring digital development: Facts and Figures 2025](#) (2025)

[E2] [GSMA · The State of Mobile Internet Connectivity 2026](#) (2026)

[E3] [ITU / UNITAR · The Global E-waste Monitor 2024 \(UNITAR release\)](#) (2024)

STATUS / BOUNDARY. HSIMC 基础设施研究提案；没有证据证明存在百亿合格手机，没有第三方背书，也没有部署授权。

NEXT GATE. 英文 Part I 冻结后才进行六语对齐；之后为一个具体现场试点设计 Work 接受标准。

CHAPTER 2 / HSIMC BLUEPRINT

从以 App 为中心到意图驱动的实体工具

保留人的界面，让有边界的实际结果可以计算

PROPOSITION

有价值的 GenAI Physical Tool 不以能操控屏幕为定义，而是能够在明确物理 Reality 中，以负责任的授权、证据和验收机制，协助完成具体人类意图的已声明能力。

2.1 从操作 App 到请求现实世界的成果

传统模式要求人先找到 App、操作菜单并解释结果。意图驱动的 Work 从成果出发：记录样品、验证状态、请求无障碍指导或取得可在本地使用的部件。意图本身并非执行命令；必须说明目标结果、允许范围、责任主体、环境及验收条件，才能成为 Work。

例如“识别这个连接器”可以拆为持有者同意的影像、合格的辨识工具、不确定性的证据，以及技术人员可确认的决定。错误识别必须可以被拒绝。基础设施保存请求与证据的关系；漂亮的回答不能代替实际工作完成。

2.2 保留人的界面，同时向 AI 提供受限能力

人仍需要屏幕、无障碍控制、多语言说明、同意机制和清晰的停止按钮。意图驱动不意味着废除 App 或替换人类。网页或本地程序可以作为 Host，解释后果、取得授权并展示结果；由模型协助的 Client 只能选择 Host 或独立服务提供的合格工具。

HSIMC 将界面、能力及授权分开。查看摄像头预览，与修改系统设置、删除记录、采购货品属于不同权限。敏感动作要求明确且适当限定的授权，必要时还需第二个人确认。能够调用自动化 API 或无障碍服务，不代表获准操控整部手机。

2.3 手机作为传感器、界面、计算资源和实体网关

现有手机可承担观察点、工作屏幕、网络桥接、有限本地计算或附近合格设备的输入等角色。这些是可选用途，并非所有手机的承诺。每种角色需要独立核实系统版本与补丁、电池及供电、网络、摄像头与传感器、权限、存储安全及操作人无障碍条件。

手机欠缺某项条件时，线材、夹具、NFC 标签、Edge Device 或受监督现场可能补足。此类配件不一定是智能工具；被动线材可以是必要材料，而不是 MCP Server。Work Graph 必须列明各部件的贡献，并将采购、实物检查与服务交付分开负责。

2.4 参与 GenAI 不一定需要在手机本地运行大模型

本地设备可提供结构化观察，或在授权下调用远程模型，而不必自己运行大模型，因此无需仅因算力不足而淘汰设备。但在线推理仍有延迟、传输、账户条款、安全、能耗及可用性成本。纯本地、混合与远程辅助路径都应按同一 Work 验收标准比较。

断网时可安全停止、在获许可的前提下暂存非敏感证据，或使用经过测试的离线方案；不应暗中传输私人图像，也不能无限重试有后果的动作。路线由目的、数据敏感程度、当地能力及人的时间窗口决定，不由设备贴有“AI”标签决定。

2.5 超越 App 控制：从操作程序转到授权能力

屏幕自动点击、调试桥接与特权系统 API 可以用于获授权实验室，但不宜成为通用服务契约。操作系统与设备之间权限差异大，容易赋予 AI 过度行动力。OWASP 指出，功能过度、权限过宽与自主程度失控是不同的风险来源 [E4]。应优先使用输入类型明确、副作用受限、记录可见的窄范围能力。

能力契约应说明谁可以请求、暴露什么资料、何时需要人确认、结果如何衡量或撤销。执行属于特定受监督 Work 及其真实 Reality。关键转变不是“AI 能触碰一个 App”，而是“获授权的人可通过已声明能力取得可检查的有用结果”。

WORK / DECISION TEST

候选方案须完整展示一次 Work：由人提出目标、授予有限权限、可拒绝不安全调用，并接受或否决证据。应显示 Host 界面、所调用能力、设备的实际角色与撤销途径；不能以自动点击次数代替价值。

PUBLIC EVIDENCE · SOURCE LINKS

[E4] OWASP GenAI Security Project · LLM06:2025 Excessive Agency (2025)

STATUS / BOUNDARY. HSIMC 架构提案，不代表通用设备权限、第三方 App 背书、规模化部署或已验收 Work。

NEXT GATE. 将 Work 契约与可见的同意测试随 Part I 一同冻结，再经新授权评估一个实体物件至证据的本地工作流。

CHAPTER 3 / HSIMC BLUEPRINT

MCP 是促成互通的工具，不是完整生产系统

协议互通、运行就绪和 Work 验收是不同事情

PROPOSITION

MCP 能让不同实现中的工具及上下文资源被发现和调用，但协议本身不能建立行动授权、执行所需的实体条件，或证明结果已被人接受。

3.1 2026 年 7 月 28 日协议变化及其对分布式能力的意义

正式发布的 MCP 2026-07-28 版本取消了协议层 initialize 握手及 Mcp-Session-Id。每个请求携带版本与能力元数据，需要时可执行 Server Discovery，HTTP 路由因此较容易实现。这是具体的协议变化，不意味着所有已部署 Client、旧版 Server 或手机已经采用新协议 [E5]。

合格的物理能力可由获授权的 Server 提供，而不必将持久传输 Session 作为其身份。但设备仍可能需要校准、操作员、供电、法律许可及持久证据。HSIMC 把 MCP 视为大型 Reality / Work 系统中的一个互通层；兼容性和部署测试必须标明实际协议版本。

3.2 独立实现之间的发现、调用与互通

MCP 将可调用工具与提供上下文的资源区分开。Host 可向模型辅助的 Client 提供适当可用功能，Client 以有类型边界的参数请求工具调用。独立供应者可以使用不同实现提供相近成果。Schema 有助互通，但不验证供应商、不保证输入真实，也不授予物理行动权限 [E6]。

能力记录应列明工具及版本、提供方、输入、输出、错误状态、限制、权限、环境及证据格式。发现、调用成功及安全操作是三个不同关卡。Client 须校验返回资料，并将不可信工具描述、注释及检索文字视为数据而非新授权；重要操作保留人类批准。

3.3 无协议会话、持久 Work 身份与实体状态

无状态通信意味着协议不要求跨请求隐藏的服务端对话 Session，不意味着应用没有记忆或物理任务没有状态。Work 可凭明确 Work ID、可核验的证据、由权利人控制的持久存储及声明的续作句柄延续，而不是把网络连接当作授权。

实体状态独立存在：电池充电、夹具移动、包裹到场、人撤回许可。每次新调用在行动前必须重新比对 Reality。响应丢失不应自动执行第二次不可逆操作。幂等、重试、停止条件、独立回读及操作员覆盖权，应写进 Work 契约，不论传输协议是否带 Session。

3.4 协议符合性、设备就绪与交付验收是三个里程碑

需要三类测试。协议符合性核实 Client 与 Server 能否以指定版本交换有效信息；Reality 就绪核实特定设备、地点、输入、适配器、安全与授权在此刻是否适合任务；交付验收核实结果证据是否满足指定人或组织的接受规则。

通过其中一关不能代替另外两关。Wi-Fi 连通或 tools/list 成功不能证明相机权限、电源安全或商业权利。相反，人工演示可能产出真实证据，却不构成 MCP 合格产品。失败测试与正确拒绝应被记录为研究成果，而不是隐藏以夸大节点数。

3.5 按日期标记协议符合性及 Sony 试点旧版基线

HSIMC 的 Sony Reference Journey 属于历史研究案例，不能自动证明符合后来的协议版本。已有实验应保留日期、硬件、传输、软件修订、测试范围与原始回执。如果早期原型使用旧版 MCP 握手或 App 专用适配器，应如实标记。2026-07-28 版本涉及不兼容变化，迁移是需要重新验证的 Work，不能回溯改写历史 [E5]。

新试点应报告协议版本、已认证身份、最小工具集合、同意决定、可观察动作、证据摘要、失败行为及独立验收。只能在实际通过的配置范围内宣称 MCP-ready。未来目标是让独立实现按可检查契约协同，而不是依靠名词宣布普遍兼容。

WORK / DECISION TEST

对同一获明确授权的配置，分别展示指定 MCP 版本的消息互通、安全且有限的物理就绪，以及由第二人审查的 Work 结果。部分成功不能冒充生产级部署。

PUBLIC EVIDENCE · SOURCE LINKS

[E5] Model Context Protocol Core Maintainers · The 2026-07-28 Specification (2026)

[E6] Model Context Protocol specification · 2026-07-28 Tools (2026)

STATUS / BOUNDARY. 协议事实对应 MCP 2026-07-28 正式版本；不声称 Sony 或其他本地设备已通过新版符合性测试，也不代表合作伙伴背书或扩大权限。

NEXT GATE. 撰写第 11、16–18、30 章时沿用三个关卡；任何现场执行前另建测试专属 Work 验收记录。