

全球激活：带来一部手机，获得一项经过验证的能力

C0-015-PART-V-6L · 19 original TOC sections · English master frozen for this edition · AI-assisted translations (professional review pending)

激活一项能力，保留人类授权，以真实证据交付。

百亿手机激活（Ten-Billion-Phone Activation）是邀请全球人们重新利用现有物品参与生产力，并非声称已有百亿部合格手机。HSIMC 提出让人通过自己的手机、NFC、无障碍共享入口进入合格的本地能力，以真实验收结束一次服务。结果可能是经测试的工具、可信的支援入口、受监督的共享能力；设备不适用时，有证据的安全拒绝同样是正确成果。

在 GenAI Physical 时代不让任何人掉队，不能只靠令人兴奋的 App。没有 NFC、没有连续网络、使用旧手机甚至没有手机的人，仍应在有真实服务时获得 QR、语音、现场协助及共享设施的选择。AI 模型和 MCP Client 可以提出方案或调用定义明确的工具，却不能创造设备产权、移动网络、健康电池或代替人的知情授权。

CHAPTER 13 / LOCAL COMMISSIONING & HUMAN REALITY

13. 面向全球参与的本地激活服务网络

让负责任的当地人员和设施交付可全球复用的方法

PROPOSITION

全球规模来自许多独立授权、可复制的本地激活，而不是假定 HSIMC 已经拥有或能远程配置每一部手机。激活是一项需验收的服务：明确人的目的、检验设备、只在同意范围内配置、验证特定能力并向参与者交付能读懂的回执。

13.1 自助、辅助及专业三种激活路径

自助路径可以指导自愿参加的手机所有者安装兼容 App、使用安全网页入口、选择有限权限并完成一个简单能力测试。辅助路径加入受培训的人员和无障碍服务，适合无法依赖细小触屏、复杂表格、持续互联网或自有手机的人。供电布线、系统改动、仪器校准、特殊工作和数据恢复则应由合格专业人员处理。

三条路径遵循同一套验收逻辑，只是人工支持及安全条件不同。使用者自行选择具体任务，也可拒绝而不失去普通公开资讯。激活不表示整台手机向全球公开。仅带来工作需求的人可以借助合格共享站点，但不能虚报成他拥有并激活了一部个人手机。

13.2 获得授权的激活站及类似 ATM 的服务终端

ATM 式激活站是无障碍服务概念，不是可以接管或任意刷写陌生手机的机器。在获信任的作坊、学校、维修柜台或社区 Hub，它可以介绍选择、确认设备权利人、检查兼容接口并提供清楚的批准或拒绝界面。每次临时会话绑定具名操作员及真实场所，显示隐私说明；除非获得单独、明确的管理授权，否则应把手机以原来使用权归还。

每个服务点必须具备人员责任、安全更新、合格供电、保密数据处理、无障碍设施、服务语言和真人转介。QR 或 NFC 可开启说明，但不能当成所有权证书，也不能误把普通网址轻触变成设备管理员注册。Android Enterprise 的 NFC 配置属于另一种拥有强管理能力的设备入管程序 [E1]，必须严格分开。

13.3 核对所有权及设备状况；仅在授权范围内保存或清除数据

触及私人数据前，先确认真正的权利人或保管人、服务目的及获准权限。检查充电与电池安全、机身损坏、系统与安全更新、容量、无线功能、接口、无障碍需要，以及是否受到公司或学校的管理政策约束。技术人员拿着手机，并不因此有权解锁账号、复制照片、安装管理软件或转移 e-Person 的角色。

数据默认留在本人控制范围。备份、导出、搬移和删除，都需要知情同意及必要的独立回读。Android 部分 Bootloader 解锁要求用户确认并重置数据，亦可能改变系统安全状态 [E4]。不能谎称通用重刷保证保留数据，更不能把清除手机当作普通咨询的隐藏前提。设备危险、受其他机构管理或不兼容时应明确停止并提供替代服务。

13.4 配置、绑定、测试、解释控制权并签发激活回执

真正完成配置不只是安装一个 APK：还需记录实际手机和软件版本、获准 Work、地点及时间、确实使用的适配器或 MCP 服务、Human Supervisor、数据与输出限制、撤销方式。现场完成商定的测试并回读真实结果，例如有限的电量观察、获准 NFC NDEF 写入加独立标签读回，或者无障碍资讯交接。每个结果只能证明对应设备和当时条件。

回执应分开 DEVICE_INSPECTED、APP_INSTALLED、TOOL_REACHABLE、HUMAN_GRANT_VALID、CAPABILITY_VERIFIED 和 WORK_ACCEPTED，不能由前一状态自动跳到下一状态。记录版本、时间、同意、输入、观察结果、失败、证据 ID、费用、操作员和验收方式，但不公开凭证。教会使用者重复测试、暂停、撤销和求助。测试失败也应出具真实拒绝或待补条件回执。

[Non-executable local commissioning receipt template ↗](#)

13.5 当地实际交付，全球复用的工程方法

可以放大的不是某一个品牌，而是可重复的方法：设备资格清单、受限 Capability Contract、易读激活说明、证据验收模板、重启测试和明确停止原因。不同城市的独立运营者可以采用当地法定语言、选择合规供货和服务方，同时交付可比较的

结果。香港技术员、大学实验室、维修机构和社区 Hub 可以参加而不必把客户、品牌或公司身份交给 HSIMC。

全球共享的案例应提供测试条件及不敏感的经验，不应公开私人序号和密码。全球协作网络来自各自 Reality 中验收成功的当地能力，指标应是使用者是否理解、交付时间、真实验收和独立复现，而非安装 App 数量。服务也需要人员培训、适当保险、支持安排和公平报酬；即使没有商业收入，包容性参与依然有价值。

WORK / HUMAN ACCEPTANCE TEST

第 13 章的通过标准：另一个独立服务点能够证明权利人同意、设备真实合格、有限授权、能力实际读回和可理解的验收回执；对不兼容设备也能提供有证据的安全停止及辅助替代路径。

14. 多种升级路径——而非万能系统重刷

选择适当升级方式，不以所谓统一方案牺牲人的数据与安全

PROPOSITION

旧手机不一定需要新操作系统才能重新贡献能力。HSIMC 应按照风险和需求比较：既有系统上的受限应用、专用设备配置、极少数合格机器的授权刷机、Hub 中介和零件复用，以满足 Work 的最小干预路径为优先。

14.1 在受支持的既有系统上安装受限 MCP-ready 应用

通常先保留原本获支持的 Android 或其他系统，在政策许可时安装权限较小的 App 或本地 MCP-compatible Service。持有人仍掌握系统安全设置，按需要开放有限能力，例如设备状态、NFC 服务入口或易读支援。必须在实际机型核对 OS 功能、授权、软件来源、网络、后台运行，而不是只看开发电脑演示。

Sony H4493 的 MCP Phone 研究证明了有边界的只读能力，而 NFC Writer 和 USB 眼镜依旧有各自待测条件 [H2]。它并不证明一个 APK 就能把全部旧手机变成可信 AI Node。当地人员应告诉用户哪些能力已可用、哪些需要逐次点击、哪些根本不可用；过时系统和危险权限不能被标为 READY。

14.2 操作系统支持时的专用设备配置

经组织合法拥有的合格设备，可以经批准配置成无障碍服务终端、课堂设备或专用工作台。Android Enterprise 根据所有权、版本与 Enrollment 方式区分个人 Work Profile、企业 Fully Managed 及 Dedicated Device 等模式 [E1]；这些是企业管理体系关系，绝不是将访客私有手机自动转为公司资产的许可。

激活人员须说明谁制定策略、个人数据如何隔离、用户如何退出以及异常时如何恢复和交还。共享服务终端应使用受限账号、最少 Tools、清晰会话边界和合规数据清除；没有权利人的要求不得擅自擦机。不满足组织管理资格的设备，应转向浏览器入口或受监督的 Hub 服务。

14.3 对合格设备进行持有人授权的系统替换或重刷

更换 OS 可能让极少数机型承担专用角色，但这应是高风险工程分支，不能成为默认激活方式。资格包括实际 Bootloader 状态、该型号可用系统镜像与驱动、权利人同意、可信恢复路线、签名来源，以及清除数据、保修和安全影响的充分说明。Verified Boot 与防回滚保护本来用于抵御不可信或旧漏洞镜像，不能为了快速演示随意绕过 [E4、E5]。

Android 官方资料指出，合格设备解锁 Bootloader 往往要求用户确认并恢复出厂资料 [E4]。因此不能承诺刷机保留照片、支付凭证或企业管理，也不能绕开另一机构的限制。许多旧设备根本没有安全、合法的重刷路径；缺少恢复方案、系统支持或持有人不愿意时应 STOP，改用受限 App 或共享 Hub。

14.4 手机不能独立安全运行时，经合格 Hub 参与

低端或不再获支持的手机，也许只适合提供显示、音频、在获同意下拍照、QR / NFC 入口或本地输入，由旁边合格 Hub 承担计算、网络互通和持久 Work。如果手机连这些任务都不安全，仍可提供受监督终端或真人服务。Hub 不能因为靠近手机就继承照片、文件或执行权限。

Hub 方案须说明双向资料权限：谁提供观察、谁接收、怎样调用远端服务、谁负责验收。断网时只有事先明确获准、实际上可本地完成的工作才能继续；联网恢复后依法同步。云模型不可用、无移动网络或供电不足，都应成为公开限制而非营销词遮盖的事实。

14.5 恢复、回滚、不支持设备的决定与负责任退役

每条升级路径都必须有后退方法：如何卸载和停止、撤销凭证、恢复配置、确认本人备份，以及断电后安全重启。测试应覆盖安装失败、网络中断、重启、重复请求和服务不可用时拒绝。Android 的 Verified Boot 和回滚保护可能主动阻止不安全旧版本 [E5]；因此不能保证随时回到任意旧系统。

不存在可信恢复方案时，应标记 UNSUPPORTED_FOR_THIS_WORK，不能为了激活数字让缺乏安全补丁的设备长期在线暴露控制接口。合格维修、拆出低危险度非联网零件或合规电子废弃物处理可能更好。数据处理和物品移交有证据的退役回执，可以同时保护原主人和下一位使用者。

14.6 保留完整设备、复用子系统或接入合格 Hub

应选择适当的物理层级形成价值：整台手机可以用作无障碍显示站，合格摄像头或屏幕可能通过已支持的适配方式复用，传感器或线材可独立提供能力，或者由 Hub 完全取代手机角色。选择依据接口、额定电气条件、安全、结构固定、软件授权、维护人及真实成本，而不是单看“可拆下”。

拆改可能损害锂电池、连接器和防护外壳。HSIMC 不建议未经验证地绕过电池保护或自制危险高压适配。再用应与维修、零件更换、运输及材料回收比较，环境减排必须用可比生命周期证据证明。Give Existing Things New Work，是形成有用、被验收的能力，不是强迫每件报废设备重新联网。

WORK / HUMAN ACCEPTANCE TEST

第 14 章通过标准：服务人员能解释为何选择某条升级路径，展示持有人同意与真实恢复能力，并在系统、安全或资料条件不合格时拒绝重刷或在线使用。

15. 让已有资产在人的生活与工作现场真正发挥作用

物理 Reality 的最后一米决定全球基础设施是否有用

PROPOSITION

只在实验室或某款演示手机上可运行的能力，尚未成为人类现实基础设施。必须在真正使用的地点与时刻验证供电、数据、结构适配、无障碍、安全、恢复，以及由谁使用、维护和验收。

15.1 依实际能力、设备配置和运行条件验证兼容性

兼容性属于特定 Reality 下的具体 Capability，而不是某个品牌或通用 NFC / MCP 标识。记录设备型号、系统版本、适配器、本地网络、用户交互、固件、环境边界和测试证据。手机能读 NFC 不等于能写所有标签；App 打开网址可能需要额外点击。Android 近期不同版本对 NFC 网页地址分派方式作出了变化，说明必须在实际 OS 与用户路径测试 [E3]。

应建立实际行为的兼容矩阵，不用推测性的销售清单代替。成功扫到 NFC 不代表产品真伪、合同签名或机器控制权限。标签、读卡器、浏览器或网络不适用时，保留 QR、短 HTTPS、语音和本地真人服务。一个可靠替代入口本身也是值得资格确认的能力。

15.2 电池状况、供电、温升、固定和长时间运行

连续使用旧手机的工况不同于偶尔发消息。应检查电池鼓胀或损坏、充电状态、持续温升、线材与接头额定值、机械固定和断电重启行为。适当使用厂商认可的充电方案，必要时由专业人员测量电气安全。手机发热、电池异常和不稳定电源，不应成为绕过温控或电池保护的理由。

为设备明确工作包：占空比、环境、屏幕点亮时间、连接要求和维护周期。如果控制任务或公共站点需要长时间运行，应优先评估合格电源、Hub 或专用设备，而非强迫退休手机担当无人值守工业控制器。在第一次无人值守试验之前必须确立独立的停止条件。

15.3 组合外设、联网和供电，但不假设必然兼容

手机有 USB-C 不等于支持全部 USB Host、外接摄像头、HDMI / DisplayPort Alt Mode、以太网适配器及同时充电的组合。实际可行性受 OS、控制器、配件、功率预算、驱动和线材协商影响。Android 的 USB Host API 支持设备枚举及权限机制，却不保证自动驱动任何接入设备 [E2]。

必须把供电、网络、数据和安全分开规定。对 Webcam / USB 眼镜须独立检查应用支持、设备许可、画面回读、照片保存及恢复，不能借 NFC 写入的结果替代。低压继电器只有在负载额定、隔离与独立停止逻辑合格后才可用作执行界面。不能让语言模型直接发出无限制的裸硬件命令。

15.4 间歇网络、重试、安全停止和重启行为

本地能力应接受人们真实拥有的网络条件。Work 可以在可信站点离线开始、取得获准观察、等待合法同步，再以相同 Work ID 接续。必须区分网络自动重试与人的新请求，对证据按权限保存；远端认证、服务或监督不可用时，状态应明确标注。

激活验收要包含 Wi-Fi 消失、移动网络中断、断电、App 重启、Tool 超时、Token 到期、取消和操作员更换。恢复必须回读实际状态，而非依赖上一轮 AI 宣称成功。若有真实物理动作，应由经过验证的本地控制器保证安全停止，并让具名人类可以介入。

15.5 签名更新、维修、安全漏洞响应和停止支持的判断

旧节点曾经可用，并不代表永远安全。系统停止打补丁、依赖软件失去可信来源、零件损坏或厂商 API 改变，都可能使它不适合再承担工作。需要明确软件来源、更新检查、受限服务账号、本地凭证处理、事故响应和维护责任人。Verified Boot、签名映像及回滚保护能降低部分风险，但不保证未来永远安全 [E5]。

全球协作不应强迫每位私人手机持有人或维修机构采用同一个管理政策。按每项能力发布支持期限与迁移办法，区分本人安装与企业管理更新，并让受侵害节点暂停，而不擅自删除获准 Work 历史。无法支持安全联网时，转为低风险离线用途、共享 Hub 或退役才是负责任的结论。

15.6 在人实际工作的末端提供稳定电力与数据，而不只看电源标称值

产品规格常标称充电器或线材功率，但真实工作取决于设备负载下实际到达端口的电压与数据质量。线长、铜导体电阻、连接器、共享 USB-C 输出、功率协商、干扰和磨损，都可能影响现场摄像头、Hub 或手机。漂亮的 100 W 标签不能证明同时连接两台设备时都获得稳定供电，更不证明数据长期正常。

测试应在使用者工作位置量测电压、温度、角色协商、持续运转与通信，不只看充电器输出。比较性工程声明要保留仪表校准和协议记录。Pannex 长期实体产品工程经验有助于合格线材研究，但这种关系及一次实验读数，都不能转化为其他公司的授权或全球普遍认证。

15.7 机械配合、无障碍交互、恢复能力和独立保护

设备必须真正适应使用者、场所与任务：伸手范围、抓握、视觉与听觉辅助、文字可读性、语音或触觉反馈、安装高度、绊线风险、紧急触达、清洁、振动与环境暴露都须考虑。共享 Hub 应让人无需记技术指令，也能理解权限、选择安全替代方式并联系真人。

当 AI、移动机械与能力受限的使用者同时出现，独立安全保障更重要。用户同意、访问控制和硬件联锁是三套不同机制；紧急停止与物理隔离须在模型之外验证。即使技术 Demo 运行，也要拒绝危险或不可访问的配置。目标是独立生活和自主选

择，不是让人被迫适应设计不良的机器。

15.8 办公室级研发制作：选择合适工序、外部专家和经过验证的界限

HSIMC 的小型研发现场可以在具备工具与监督时准备样品治具、合格低压适配、标签、支架和测试组件，也可以委托专业机构承担机械加工、电气工程、光学调整、无障碍设计和材料分析。这是模块化工程路径，不代表任何办公室、图书馆或学校都获许可开展全部制造工艺或危险废弃物处理。

每个试点必须说明实际使用的工序、材料来源、设备极限、合格操作员、保护措施、许可要求、测量结果与验收。中性 NFC / QR Accessible Product Passport 和低风险 Human-Guided Circular Work 是合理候选；涉及 FIFA 商标、授权数字内容、危险锂电池、医疗或安全关键机械则需独立批准。可重复的证据才是负责任全球复制的基础。

WORK / HUMAN ACCEPTANCE TEST

第 15 章在第二个现场能根据真实物理条件复制指定能力、核验末端供电数据、结构适合、无障碍、安全、恢复和授权，并说明不合格设备为何拒绝时才通过。全球网络只能由各地实际被接受的 Work 逐步形成。

Evidence register and technical boundary

- 1. [H0] HSIMC C0-009-6L · Immutable 30-chapter Table of Contents — Original Part V chapter and subsection identities.
- 2. [H1] HSIMC C0-014 · e-Person and Work Graph (Part IV) — Persistent Work, bounded Human Authority and actual Reality qualifications.
- 3. [H2] HSIMC Android/Sony/MCP Phone and NFC Writer engineering handoffs — Different bounded research states; no universal read/write or camera execution acceptance.
- 4. [H3] HSIMC Part III · Phone, Capability Contracts, Human Authority — Protocol invocation distinct from local physical and human authorization.
- 5. [E1] Google · Enroll and provision Android devices — Personal ownership versus company-managed/dedicated provisioning and scope.
- 6. [E2] Android Developers · USB host overview — Hardware/OS support and explicit USB permissions.
- 7. [E3] Android Developers · NFC basics — NDEF handling and version-dependent URL dispatch, not identity or Work authorization.
- 8. [E4] AOSP · Lock and unlock the bootloader — User confirmation, unlocking effects and factory data reset risk.
- 9. [E5] AOSP · Verified Boot — Integrity and rollback security requirements.
- 10. [E6] ITU · Facts and Figures 2025 — Global inclusion context; not a measured inventory of reactivatable phones.

Claims and source scope ↗

STATUS / BOUNDARY. HSIMC Part V 是经本人自愿授权的本地激活与全球复制研究蓝图。百亿手机激活是长期开放邀请，不是已检查合格的手机数量。没有手机或网络的人可能需要受监督共享服务。AI 辅助翻译仍待独立专业审校。出版内容不会配置真实设备、SIM、Bootloader、合作方资产或制造生产 Work。

NEXT GATE. 冻结完整英文 Part V，按相同 19 个小节同步其他五语言，验收六份 A4 及网页，再只在 SHA256 / HTTPS / Chrome 验收通过时增量发布。白皮书总目录保留此前所有历史版本。