

Global Activation: Bring a Phone, Leave with a Verified Capability

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

Activate a Capability. Preserve Human Authority. Leave with Evidence.

Ten-Billion-Phone Activation is a global invitation to unlock productive participation from the things people already have—not a census of ten billion ready devices. HSIMC proposes a practical route from a person's own phone, NFC or accessible shared entry to a locally qualified capability and an honest human-accepted outcome. The activation result may be a reusable tool, a verified support entry, a supervised shared capability, or a documented safe refusal when a device is unsuitable.

No One Left Behind requires more than an exciting App. A person with an old phone, no compatible NFC, intermittent connectivity or no phone at all should be offered a comprehensible path through QR, spoken instructions and properly supervised local access where such a service genuinely exists. A capable AI model and MCP client can suggest or invoke defined functions, but they cannot grant device ownership, create a cellular signal, turn an unsafe battery into safe equipment or replace informed consent.

CHAPTER 13 / LOCAL COMMISSIONING & HUMAN REALITY

13. A Local Commissioning Network for Global Participation

A globally repeatable method delivered by accountable local people and facilities

PROPOSITION

Global scale comes from many independently authorized local activations sharing reproducible engineering methods, not from assuming HSIMC owns or can remotely configure every phone. Commissioning is a measured service: identify the human purpose, qualify the equipment, configure only what is agreed, verify a limited capability, and issue an intelligible receipt.

13.1 Self-service, assisted and professional activation pathways

A self-service path can guide a consenting phone owner through a supported App, secure web entry, limited permission choices and a simple capability test. An assisted path adds a trained local person and accessibility support for someone unable to rely on fine touch, complex forms, sustained Internet access or a personal handset. A professional path is necessary when power wiring, operating-system modification, calibration, regulated work or data restoration demands qualified expertise.

All three routes should implement the same acceptance logic while differing in the human assistance and safety controls they require. The requester chooses a bounded purpose and may decline without losing access to ordinary public information. Commissioning never means making an entire phone discoverable worldwide. A person who arrives only with a task can be referred to an eligible shared station; that outcome is not dishonestly recorded as the activation of an individually owned phone.

13.2 Authorized activation stations and ATM-like commissioning kiosks

An ATM-like activation station is an accessible service concept, not a machine that can seize or reflash unattended devices. At a trusted workshop, school, repair counter or community hub, it could explain available routes, ask who owns the phone, inspect supported interfaces and supply a visible approve/deny interaction. The station would bind each temporary work session to a human operator and a physical site, show a privacy notice and return the phone without persistent management enrollment unless that precise arrangement was separately authorized.

Each station needs operator accountability, security updates, safe power, confidential data handling, physical accessibility, support languages and a route to a real human. QR or an NFC entry can open service information but must not serve as device ownership proof or a device-administrator enrollment token by accident. Enterprise Android NFC provisioning is a distinct managed-device workflow and can have powerful administrative effects [E1]; it must never be conflated with an ordinary public NFC URL tap.

13.3 Check ownership and device condition; preserve or erase data only as authorized

Before touching private data, the station identifies the rightful owner or custodian, the purpose of service and the narrow permission actually granted. Inspect charging and battery safety, visible damage, supported OS, security update status, available storage, radio and port operation, accessibility needs and whether the device is subject to employment, school or other management policies. A technician's physical possession does not itself authorize unlocking accounts, copying photos, enrolling management software or transferring an e-Person role.

Data must default to staying under the owner's control. Backup, export, transfer or erasure requires an explicit informed choice and independently verified completion where applicable. Android bootloader unlocking typically requires a user-acknowledged factory reset and may change the device's security state [E4]. Never promise an owner-preserving reflash or perform an erasure as a hidden prerequisite to an innocuous support request. When a device is unsafe, locked by another authority or unsupported, stop and offer a suitable alternative.

13.4 Provision, bind, test, explain controls and issue an activation receipt

A commissioned capability needs more than an installed package: identify the exact handset and software build, the permitted Work, site and time, the adapter or MCP service actually used, the Human Supervisor, resource and output limits, and a revocation path. Perform the agreed test and observe real readback—such as a bounded battery observation, a permitted NFC NDEF write followed by independent tag read, or an accessible information handoff. Each result must be attributed to the device and test conditions actually observed.

The receipt should distinguish `DEVICE_INSPECTED`, `APP_INSTALLED`, `TOOL_REACHABLE`, `HUMAN_GRANT_VALID`, `CAPABILITY_VERIFIED` and `WORK_ACCEPTED`; no single state silently implies the next. It records versions, time, consent, test inputs, observed outputs, failures, evidence identifiers, costs if any, operator and acceptance contact without publishing credentials. Show the user how to repeat, pause, revoke or obtain support. If the test fails, issue a truthful refusal or further-work receipt rather than a misleading success badge.

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

13.5 A locally delivered service with reusable global engineering methods

The scalable asset is a reproducible method: a device-eligibility checklist, bounded Capability Contract, accessible commissioning script, accepted proof template, restart test and clear stop reasons. Independent operators in different cities may translate the interface into their official local language, use different lawful suppliers and still report comparable outcomes. A technician in Hong Kong, a university lab, a repair partner or a community hub can contribute without transferring its brand, customer database or business identity to HSMC.

Public examples should publish test conditions and non-sensitive lessons, not private serial numbers or credentials. A global federation grows from local capabilities verified in their own Reality; it should track participant comprehension, time to a useful result, acceptance and repeatability rather than advertising a count of Apps installed. Services need sustainable training, insurance where relevant, human support and transparent compensation; inclusion remains valuable even when a participant produces no commercial revenue.

WORK / HUMAN ACCEPTANCE TEST

Chapter 13 succeeds when an independently operated activation location can show ownership/consent, measured device eligibility, a bounded operating grant, actual capability readback and a receipt a participant can understand; an unsupported device must receive an equally auditable safe stop or assisted alternative.

14. Multiple Upgrade Routes—not One Universal Reflash

Choose an appropriate route; never sacrifice a person's data or security for a universal story

PROPOSITION

An older phone may already be productive without a new operating system. HSMC should evaluate a ladder of permissioned routes—from a small supported application and dedicated configuration to carefully qualified reflashing, Hub-mediated operation and subsystem reuse—choosing the least disruptive option that satisfies the Work.

14.1 Installing a bounded MCP-ready application on a supported existing system

The least invasive route is often to keep a supported Android or other operating system and install a narrowly scoped application or local MCP-compatible service where platform policies allow it. A consenting owner can use the phone's ordinary security controls while exposing only a measured tool such as device status, NFC entry or accessible assistance. Verify required OS features, permissions, package provenance, network mode and background-service behavior on the actual model, not merely on a development computer.

The Sony H4493 research demonstrates bounded read-only MCP Phone capability while later NFC Writer and USB-glasses tests retain their separate acceptance conditions [H2]. This does not mean one APK turns every old phone into a fully trusted AI Node. The local operator must make clear which abilities are ready, which require user interaction and which are unavailable. A service that needs unsafe permissions or an unsupported OS must not receive a green READY label.

14.2 Dedicated-device configuration where the operating system supports it

An eligible organization-owned device may be configured for a supervised kiosk, accessible demonstration, classroom station or task-specific terminal. Android Enterprise supports different management modes, including work profiles, fully managed and dedicated devices, with distinctions based on device ownership, supported Android versions and enrollment methods [E1]. Those are enterprise governance features, not blanket permission to convert a visitor's personal phone into corporate property.

The commissioner must state who controls policy, whether personal data is separated, how the user leaves the mode and how a device is recovered or returned. A shared kiosk should use restricted accounts, minimal declared tools, clear session boundaries and safe data deletion only where the proper authority requests it. If a visitor's equipment cannot be lawfully or safely enrolled, provide browser-only or Hub-assisted service instead.

14.3 Owner-authorized OS replacement or reflashing on eligible devices

Operating-system replacement may enable a dedicated role on a narrowly supported device, but it is a high-risk engineering branch rather than the standard consumer activation method. Eligibility requires a supported bootloader state, model-specific images and drivers, owner authority, a credible recovery route, signed component provenance and disclosure of data-loss, warranty and security implications. Verified Boot and anti-rollback protections protect devices against untrusted or older vulnerable images and must not be casually bypassed [E4, E5].

Android documentation describes an explicit user confirmation and data reset when unlocking supported bootloaders [E4]. Consequently, do not promise that a universal flash can preserve photos, banking credentials or enterprise management, and do not guide unauthorized unlocks around another party's policies. For many devices, replacing the OS will be unjustified or impossible. An observed unsafe state, missing image support or unwilling owner is a true stop and may point to a managed App or shared Hub route.

14.4 Hub-mediated participation when a phone cannot safely operate independently

A low-end or unsupported handset may still serve as a screen, speaker, camera with consent, QR/NFC service entry or local input, while a qualified nearby Hub carries computation, network integration and persistent Work records. If the handset is unsafe even for these tasks, the person can use a supervised shared terminal or human assistant instead. The Hub does not inherit personal data or permission to act on other people's devices merely because it is nearby.

Hub-mediated commissioning requires a contract for each direction of information: who can provide observations, who may receive them, how remote services are invoked and who accepts the output. Offline-first tasks may continue only inside an already approved local scope, with lawful deferred synchronization. An unreachable cloud model, missing cellular coverage or insufficient power must appear as a documented operating constraint rather than being hidden by marketing language.

14.5 Recovery, rollback, unsupported-device decisions and responsible retirement

Every upgrade route needs a return path: how to uninstall or stop the service, revoke local credentials, recover a configuration, confirm backed-up user data and safely restart after interrupted power. A test includes failed installation, network loss, power cycling, repeated requests and refusal when the receiving service is unavailable.

Android Verified Boot and version rollback protection can deliberately prevent insecure downgrades [E5], so a generic claim of rollback to any older system is unsafe.

When no responsible recovery path exists, label the device UNSUPPORTED_FOR_THIS_WORK. Do not keep an unpatched device online with exposed control services merely to raise an activation count. Independent repair, reuse as a non-networked low-risk component and compliant e-waste processing may be better outcomes. A clear retirement receipt, with approved data handling and custody transfer where applicable, can protect both the owner and subsequent users.

14.6 Retain a whole device, reuse a subsystem or integrate through a qualified Hub

Consider value at the most appropriate physical boundary. A complete phone may operate an accessible kiosk; its tested camera or screen might instead become a subsystem through a supported adapter; a sensor, cable or fixture may contribute separately; or a hub can replace the need for the phone altogether. Selecting the route requires evidence on interfaces, electrical ratings, security, physical mounting, software rights, actual cost and who can maintain it.

Disassembly or modification can make batteries, connectors or protective enclosures unsafe. HSIMC's engineering recommendation is not to improvise unsafe battery bypasses or unverified high-voltage adapters. Reuse should be weighed against repair, transport, component replacement and material recovery; claimed environmental savings need comparable lifecycle evidence. ****Give Existing Things New Work**** means creating useful, accepted capability, not insisting that every discarded device must be put back online.

WORK / HUMAN ACCEPTANCE TEST

Chapter 14 passes when a commissioning operator can explain why one of several upgrade routes is selected, demonstrate owner consent and safe recovery, and reject reflashing or continued online use when the device, security or data boundary cannot be qualified.

15. Making Existing Assets Work Where People Live and Work

The last meter of physical Reality determines whether global infrastructure is useful

PROPOSITION

A capability that works only in a laboratory or on a vendor's demonstration phone has not yet become local human infrastructure. Readiness must be proven at the place and time of use, accounting for power, data, fit, access, security, recovery and the people who will operate, maintain and accept it.

15.1 Compatibility by tested capability, device configuration and operating conditions

Compatibility belongs to an exact capability in a specified Reality—not to a brand or generic NFC/MCP logo. Record model, system version, adapter, local network, user interaction, firmware, environmental limits and test evidence. A phone may read NFC tags yet not write a particular tag type; an App may open a web URL but require an additional user tap. Android's NFC web-link dispatch behavior has changed across recent versions, illustrating why acceptance must be tested with the actual OS and user journey [E3].

Build a compatibility matrix of actual observed behavior rather than a sales list of possible pairings. A successful NFC scan does not prove a genuine product, a signed contract or authority over a physical tool. Keep QR, short HTTPS URLs, accessible speech and local human support available when the tag, reader, browser or network path is unsuitable. A safe fallback is a qualified capability in its own right.

15.2 Battery condition, power, heat, mounting and sustained operation

Continuous use can stress a retired phone differently from occasional messaging. Inspect battery swelling or damage, charger behavior, sustained temperature, cable and connector ratings, mechanical support and the ability to restart safely after power loss. Use manufacturer-approved charging and independent electrical assessment when needed. A warm phone, swollen battery or unreliable power supply is not an invitation to override thermal or battery protection.

Document an operating envelope: duty cycle, allowed location, ambient conditions, screen-on duration, expected connection and maintenance interval. When a physical control or shared station must operate for long periods, consider a separately qualified supply, Hub or purpose-built device rather than demanding that a retired handset become an unattended industrial controller. An independent stop condition should exist before the first unattended trial.

15.3 Combining external peripherals, network access and power without assuming compatibility

A phone with USB-C may not support every USB host mode, external camera, HDMI/DisplayPort alternate mode, Ethernet adapter or simultaneous charging configuration. Actual compatibility depends on the particular OS, controller, accessory, power budget, drivers and cable negotiation. Android USB host support exposes enumeration and device permission mechanisms, not automatic ability to operate any connected peripheral [E2].

Specify separate paths for power, network, data and safety. Test a webcam or glasses camera with its own approved application, device permissions, frame readback, image retention and recovery; do not borrow acceptance from a successful NFC writer. A low-voltage relay can provide a switching interface only after load rating, electrical isolation and independent stop logic are qualified. No language model should issue unrestricted raw hardware commands.

15.4 Intermittent connectivity, retries, safe stopping and restart behaviour

A local capability must handle the connections people actually have. A Work may begin offline at a trusted station, record a permitted observation, wait for lawful synchronization and resume with the same Work ID. It must distinguish duplicate network retries from new human requests, persist only approved evidence and keep an explicit status if remote authentication, service or required supervision is unavailable.

Commissioning tests should include dropped Wi-Fi, loss of mobile data, interrupted power, app restart, stalled tool calls, token expiry, cancellation and a changed local operator. Recovery needs readback of the actual state, not a claimed success from a prior model turn. If the task could physically act, safe stopping is enforced locally by validated controls, with a named human able to intervene.

15.5 Signed updates, repair, vulnerability response and end-of-support decisions

A previously useful node can become unsuitable when security patches stop, libraries become untrusted, a component fails or a vendor API changes. Acceptable operations require known software provenance, update checks, restricted service accounts, local credential handling, defined incident response and a real person or organization responsible for maintenance. Verified Boot, signed images and rollback protections reduce certain risks but are not a guarantee of future security [E5].

A global network cannot impose one update policy on every privately owned phone or repair shop. Publish support limits and migration options per capability, distinguish owner-installed updates from managed enterprise policies, and provide a way to suspend a compromised node without deleting its permitted Work history. Where safe online use is no longer supportable, a non-networked role, shared Hub or retirement is an accountable result.

15.6 Stable power and data at the human work position, not merely at the source

Product specifications often quote a charger or cable's nominal rating, but meaningful operation depends on voltage and data quality at the ****actual device under load****. Lead length, conductor resistance, connectors, shared USB-C outputs, power negotiation, interference and cable damage can affect a camera, hub or phone in the field. An attractive 100 W label is not proof that two simultaneously connected devices receive stable power or that data communication will remain reliable.

Test voltage, temperature, role negotiation, sustained device operation and communication at the workstation—not only at the charger. Keep engineering traces and instrument calibration when making comparative claims. Pannex's long physical product history is a useful path for qualified cables and connectors, but neither the brand relationship nor a laboratory reading grants other companies' rights or certifies every global deployment.

15.7 Mechanical fitting, accessible interaction, recoverability and independent safeguards

A useful device must physically fit the person, workspace and task. Check reach, grip, vision and hearing support, screen legibility, audible or tactile feedback, mounting height, cabling trip hazards, emergency access, cleaning, vibration and environmental exposure. A shared Hub should permit the participant to understand a permission, choose a safe alternative and reach a human without memorizing technical commands.

Independent safeguards matter most when AI, a moving mechanism and a vulnerable user meet. Design consent, access control and hardware safety as different mechanisms; validate emergency stops and physical isolation outside the model. Reject unsafe or inaccessible arrangements even if a technical demo functions. The goal is independent living and productive choice, not forcing the person to adapt to a poorly designed machine.

15.8 Office-scale research fabrication: selected processes, external specialists and verified limits

A small HSMC research site may prepare sample fixtures, safe low-voltage adapters, labels, brackets or test assemblies using suitable tools and qualified supervision. It can also coordinate a separate specialist for machining, electrical work, optical alignment, accessible design or materials analysis. This is a modular engineering pathway and does not mean that every office, library or school is licensed for all fabrication processes or hazardous waste treatment.

Each pilot should describe the fabrication process actually used, material origin, equipment limits, skilled operator, protective measures, applicable approvals, measured output and acceptance result. A neutral NFC/QR Accessible Product Passport and a Human-Guided Circular Work inspection are sensible low-risk candidates, but any FIFA trademark, licensed digital content, dangerous battery, medical device or safety-critical machine requires its own approval path. Reusable evidence is the foundation for responsible replication globally.

WORK / HUMAN ACCEPTANCE TEST

Chapter 15 succeeds when a second site can reproduce the specific capability under tested local physical conditions—stable power, data, fit, access, recovery, human authority and safety—and can prove why a non-ready device was refused. Global participation grows only from locally accepted Work.

Evidence register and technical boundary

1. [H0] HSMC C0-009-6L · Immutable 30-chapter Table of Contents — Original Part V chapter and subsection identities.
2. [H1] HSMC C0-014 · e-Person and Work Graph (Part IV) — Persistent Work, bounded Human Authority and actual Reality qualifications.
3. [H2] HSMC Android/Sony/MCP Phone and NFC Writer engineering handoffs — Different bounded research states; no universal read/write or camera execution acceptance.
4. [H3] HSMC 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. HSMC Part V is a research blueprint for opt-in local commissioning and global replication. Ten-Billion-Phone Activation / 百亿手机激活 is an invitation, not ten billion inspected phones. A participant without a phone or Internet may need a shared and supervised alternative. AI-assisted translations await independent professional language review. No external device, account, SIM, bootloader or real manufacturing Work is commissioned by this publication.

NEXT GATE. Freeze the entire English Part V for this edition, align the same 19 section IDs across five translations, verify six A4 PDFs and six web editions, and publish only after immutable version and HTTPS/browser QA. Official Whitepaper navigation must preserve all earlier historical editions.