

The Architecture: A Phone and the Reality Beyond It

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

GENAI PHYSICAL · INFRASTRUCTURE PROPOSITION

From App-Controlled Smart Products to Human-Governed Physical Capabilities

The ten-billion-phone vision is not a proposed inventory of ten billion online machines. It is a global invitation to make existing personal and shared hardware a doorway into authorized, useful work. Today's App-controlled smart home is a small visible example: lights, switches and sensors already encode physical capability, while access often remains inside product-specific interfaces. The greater opportunity joins devices, places, materials, people, manufacturing and accessible services without requiring one brand or one cloud to own the whole work.

The architectural change is to make human authority explicit at a controlled local boundary. A remote model can suggest a plan and an MCP client can invoke a declared tool, but only an authenticated and purpose-limited local policy, actual device permissions, independent physical interlocks and named human acceptance may enable consequential action. Cloud services remain optional collaborators; moving the final enforcement decision closer to a person must not be confused with bypassing lawful device commissioning, safety rules or partner rights.

CHAPTER 7 / HSIMC BLUEPRINT

7. The Phone Is the First Node—not the Boundary of the System

A qualified handset is an entrance to a human-owned Reality, never an entitlement to control it

PROPOSITION

A reused phone may combine sensing, display, accessible interaction, data and transport. Its productive value emerges when its specific abilities are safely joined to other qualified equipment, services and people—not when an AI agent is simply said to 'take over a phone'.

7.1 Native phone capabilities: sensing, display, storage, connectivity and computation

Even after retirement from everyday consumer use, a handset may retain camera, microphone, screen, speaker, inertial sensing, positioning, local storage, Wi-Fi, Bluetooth and limited computation. These provide possible entry points for work such as a consented condition report, an accessible public interface or a supervised inspection. An AI service need not run a large local model for the phone to contribute: the result may come from a small classifier, a human operator, a shared Local Edge node or a selectively invoked remote model.

Hardware eligibility must be inspected rather than inferred from product age or connector shape. Battery integrity, thermals, security updates, camera permissions, accessible controls, storage health, network reliability and power supply can each disqualify a device from a particular role. A phone's NPU is not guaranteed usable by any framework; Android's NNAPI was deprecated in Android 15, and runtime performance or support must be measured model by model [E8].

7.2 Reachable external capabilities: USB devices, NFC objects, sensors and authorized network services

The familiar smart-home App offers a glimpse of already installed capability: a commissioned light, switch, sensor, thermostat or hub can expose states and commands through a permitted integration. A qualified phone may reach additional tools through USB host or accessory mode, Bluetooth, a Wi-Fi service, an NFC tag or a dedicated adapter. Beyond homes, the same pattern reaches workshop fixtures, test equipment, low-voltage relay interfaces, shared kiosks, education, accessibility and supervised micro-manufacturing.

MCP describes how callable tools and data can be presented to an AI client; it does not manufacture USB host support, a Matter fabric, vendor API rights or a safe motor driver. Android USB permissions are granted through the operating system and vary by hardware [E6]. Home Assistant documents a practical MCP Server with deliberately exposed entities [E3]. Matter requires secure commissioning and fabric credentials, including

separate administrator domains where supported [E4, E5]. Each adapter must state what it can actually read or change.

7.3 A composed node as a server to one layer and a client or host to another

Node is a role in a composition, not a synonym for smartphone or artificial person. On one handset, a visible host application might approve a user request, an MCP client might call a trusted local server, and that server might use a separate USB, Matter or manufacturer-specific adapter. The same device could expose a narrow service to an authorized workstation while consuming a sensor service from another node. The protocol roles and the human owner are separate.

This layered view avoids assigning unrestricted control to a generic cloud model. Discovery, inference, policy evaluation, device execution and evidence collection may run in different places, under different identities. Each hop authenticates its caller and records the exact capability and authority passed; no successful interface call implies that the upstream party owns the underlying asset. A cloud suggestion may cross the boundary as a proposal, while a local guard rejects it without exporting personal device credentials.

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

An eligible phone is a modest starting node. A Local Hub can contribute stable power, secure connectivity and shared computation; a Personal Reality Pod adds an accountable place and a person's practical conditions; a Team links supervised roles; a Company contributes contractual production capacity; a Community coordinates independently authorized resources. This is a possible federation, not a centrally owned ten-billion-device fleet or permission to enroll everyone's hardware.

Capability should scale through opt-in agreements and evidence rather than silent global discovery. A student may borrow a safe camera station, a maker may provide a one-off bracket, and a supplier may fulfill a qualified order without surrendering business identity or customer data. People outside conventional mobile Internet participation must be offered accessible, supervised or delayed-synchronization routes rather than assumed to have phones or uninterrupted connectivity [H1].

7.5 Accessible does not mean owned, available, safe or authorized

A device responding to a ping or appearing in an integration is not a licensed resource. Technical reachability must be separated from title and possession, user consent, data protection, safety, firmware trust, correct environmental conditions and the commercial rights to perform a task. A vendor App, a Matter pairing and an MCP authorization token are different artifacts; none alone proves authority for a new production Work.

An inventory should expose the outcome of qualification as well as success: `REFERENCE_ONLY`, `DISCOVERED`, `AUTHORITY_PENDING`, `QUALIFIED_FOR_SPECIFIED_WORK`, `TEMPORARILY_UNAVAILABLE` or `REJECTED`. The system must be able to demonstrate why the gate did not open. For someone with limited digital skills, a comprehensible refusal and a way to contact a human supervisor are as essential as a successful task.

7.6 Power paths, networks, interaction, structures and controlled physical action

Physical productivity rests on details invisible to an App demonstration: safe power and battery operation, USB role negotiation, cable quality, network boundaries, mounting, accessible display, lighting, environmental protection, actuator ratings, relay isolation and emergency-stop behavior. External video output is device-dependent; a USB-C connector does not prove DisplayPort Alternate Mode. Screen sharing through Android MediaProjection generally requires specific user consent and foreground-service rules [E7].

An old phone must not be promoted to continuous high-power or safety-critical control because it can run a model or expose an MCP tool. Use hardware interlocks and independently tested local control logic; restrict model-generated commands to validated, bounded parameters. Where no qualified hardware and operator exist, capture an observation and request human review rather than actuating a pump, heater, door lock or machine.

7.7 Building reference to authorized room, device, time and evidenced capability

A building registry may name a room or address; a device registry may name a phone; neither establishes a usable Work location. The actual Reality binding includes the room's accountable host, the exact device and adapter, local and network conditions, appointment window, permissions, available human support, acceptance test and expiry. A record becomes `ACTIVE_FOR_THIS_WORK` only when all required conditions have current evidence.

One local example may be a borrowed phone at a supervised repair bench: the owner permits image capture for a specific sample, the operator verifies illumination and a calibration reference, and the requester accepts or rejects a dated report. The capability can expire at the end of the appointment, while permitted evidence and the Work identity continue. This is a candidate template, not a claim of a completed deployment.

WORK / DECISION TEST

Chapter 7 is accepted when an independent tester can distinguish a phone's actual role, each external capability, the accountable operator, local qualifications and a safe rejection path, instead of mistaking connected devices for an owned, active global fleet.

8. Tools, Resources and Capability Contracts

Turn arbitrary reachability into a precise, revocable offer of useful capability

PROPOSITION

MCP can publish and invoke tools, but a production Work requires a separate contract describing the who, what, where, how long, cost, risk, evidence and acceptance of a particular physical capability. The contract is an HSIMC design layer, not a new feature automatically supplied by MCP.

8.1 MCP Tools: callable functions with explicit inputs, outputs and execution boundaries

A tool is a named callable operation with declared inputs, outputs and metadata. In the 2026-07-28 MCP specification, the tool protocol is deliberately independent of a particular device or user interface. Its security guidance requires servers to validate input, enforce access controls and rate limits, sanitize outputs and support clear human oversight for meaningful actions [E1]. The same tool name may be implemented by an App bridge, local controller or remote API; the name alone cannot certify them equivalent.

Physical tools should separate observation from actuation. `read_light_state` and `propose_fixture_inspection` might be low-impact; `set_lamp_level` should carry bounded range, target, context and acknowledgement; `energize_heater` or `operate_machine` may require an additional qualified safety system and human approval. Avoid exposing arbitrary `execute_hex`, root commands or unconstrained GPIO as general-purpose model tools. Always return actual device readback or an explicit failure, not invented success.

8.2 MCP Resources: URI-addressed data and context—not automatic ownership of physical assets

A Resource URI can identify documentation, a schema, an observation, a current state snapshot or evidence needed by a Work. It does not transfer legal title, data rights or actuator control. The ability to read a room's temperature is not permission to change its heating, and a QR code pointing to a product record is not a signed delegation from the owner.

Resource provenance should make freshness, ownership, retention, sensitivity and suitable audiences legible. Separate public machine-readable specifications from private device identifiers, customer histories, location traces and access credentials. The user should understand which information may leave the Local Edge and which derived observations are approved for synchronization; model context is not a substitute for information governance.

8.3 Representing external equipment, places, materials and expertise through governed interfaces

The installed base of 'smart products' is only the visible tip of a larger physical capability iceberg. A phone with a qualified adapter may observe a relay state, a tagged product, a workshop test instrument, a camera fixture, a charging cable, a room, a locally available skill or an authorized supplier. Home Assistant and Matter illustrate how existing home equipment can participate through defined integration layers, while industrial and community Work also depend on physical materials, safety and human expertise [E3, E4].

Do not reinterpret interoperability as universal App bypass. A Matter accessory joins an operational fabric with cryptographic credentials and permissioned commissioning; vendor-specific cloud access may still be required for particular features [E4, E5]. A Tuya, Aqara or other service must be integrated under its actual agreements and current device support. A provider may offer only a subset of capabilities; HSIMC should accept the subset rather than invent full control.

8.4 Capability manifests: provenance, current state, constraints, dependencies and acceptance evidence

A Capability Contract binds an independently identified provider and physical asset to one Work purpose and a narrow operation. At minimum it declares capability ID and version, owner and operator, interface, approved input/output schema, device and Reality identity, allowable action range, expiry, quota, required consent, safety interlocks, local or cloud route, revocation, evidence format, measurement and acceptance authority. The manifest's signature and revision allow later verification without implying that all listed fields are native MCP protocol fields.

For example, a test lamp capability could allow `read_state` at any time within a short authorized session and `set_brightness` in the range 10–60 percent after a visible confirmation; offline execution expires unless pre-approved. The local controller must read back the physical state and reject a call outside quota or context. A companion sample contract is published as a non-executable blueprint; it must be independently tested before operating a real device.

8.5 Selective discovery and contribution without publishing the whole device or every reachable resource

Privacy and scarcity make selective exposure a design requirement. A family may lend only a camera result, a business only a repair slot, and a supplier only a product specification; a shared community node must not reveal every attached drive, account, sensor or employee. MCP's per-request authorization model permits tools to be scoped to the requester [E1, E2]. HSMC would layer contract-based filtering and purpose-bound disclosure on top of that protocol behavior.

Discovery proceeds in stages: candidate reference → owner-approved summary → eligibility check → explicit Work-specific grant → limited invocation → actual evidence → acceptance or revocation. A published capability list is not a promise of perpetual availability. This allows individuals without their own premium phone to participate through a community node without turning private premises into a global remote-control endpoint.

8.6 Brands, trademarks and capability rights: distinct assets and permissions

A device's technical interface, a product's brand, a dataset's license, an organization's commercial authority and the owner's right to control equipment are separate things. HSMC cannot acquire Tuya, Apple, Matter, Home Assistant, Pannex, InnoSpire or Kingsware rights merely by referencing their public compatibility patterns. Nor must any traditional customer or manufacturer adopt HSMC's entire architecture before contributing a qualifying product.

Contracts must identify who sells, supplies, operates, insures, repairs and accepts the actual Work; who retains intellectual property; and whether a trademark may be displayed. A reference to a vendor's API is evidence of a possible integration route, not proof of permission, endorsement, warranty or production partnership.

Governance remains mutually respectful: independent contributors may join a Work without dissolving existing relationships.

WORK / DECISION TEST

Chapter 8 passes only if a third party can inspect a sample Capability Contract, identify the legal operator, call scope, permitted environment, revocation and physical readback, and tell protocol interoperability apart from commercial and safety authorization.

9. Human Authority as an Operational Boundary

Move the final consequential decision closer to the human, not into an unconstrained agent

PROPOSITION

The GenAI production shift is not the removal of a person's consent or an automatic migration of every cloud right to a handset. It is the ability to put a verifiable local policy and enforcement gate under the rightful operator's control, while still using cloud intelligence when that person authorizes it.

9.1 Ownership, Android permissions, client identity and Work authorization as distinct relationships

The person who owns an appliance, the account that commissioned it, the mobile operating system that grants camera or USB access, the MCP client identity and the actor authorized for this Work can be different. A locally stored vendor token cannot be repurposed into unlimited rights. Matter's fabric credentials establish device-domain trust; MCP transport authorization can constrain a client; neither replaces the separate human decision to execute a specific physical task [E2, E4, E5].

The work begins with a capability/authority map: owner or lawful custodian, local supervisor, authenticating principal, physical target, data recipient, proposed action and who can refuse it. For privacy-sensitive jobs the person should be shown which observations, if any, will be transmitted to a cloud model. For high-impact control the local node remains the mandatory policy-enforcement point even if a remote model provides a convincing explanation.

9.2 Granting a specific capability for a purpose, duration, usage limit and recipient

An authority grant is a narrow delegation, not a switch that turns an entire phone into public infrastructure. Its minimum scope covers named Work, target capability, permitted operation and parameters, person or role, expiry, count or quota, location or network boundary, approved recipient of evidence, and required supervision. The grant should be stored durably by the rightful local operator, with an auditable revision and an accessible way to inspect it.

A request outside that envelope must be rejected before any physical effect. A grant to read a room's temperature cannot actuate the heating; permission to capture one sample photo cannot scan personal albums; a contractor's maintenance access must not become authorization to run another company's customer service. Model suggestions, QR content and arbitrary tool output are untrusted until evaluated against the active grant.

9.3 Simple approval, visible activity, accessible revocation and controlled in-flight completion

Human authority must be understandable to a non-expert and accessible to someone who cannot rely on fine touchscreen controls. Show what will happen, which device, what data leaves the location, expected cost and whether the action is reversible. Provide clear approve, deny, pause and revoke choices, a human contact and a log of attempted as well as completed operations. For safety-critical effects, confirmation may not be sufficient: independently certified interlocks and qualified personnel remain necessary.

Revocation should prevent new requests immediately and define how in-flight operations reach a safe state. The physical controller, not a cloud text model, must enforce timeouts, range limits, stop commands and independent interlocks. A motor already moving cannot always be rolled back merely by deleting an API token; the contract must specify controlled stopping, manual override and post-action evidence.

9.4 Separate maintenance privileges from normal MCP work access

A maintainer who installs an Android service, updates Ubuntu or replaces a relay driver may need administrator permission for a limited maintenance interval. That level of access must never be copied to normal production Work identities. Split provisioning, credential rotation, software patching and system recovery from low-privilege sensing or task execution; log and review any emergency elevation.

Local MCP servers are themselves a code-execution and data-exposure risk: a locally launched process may inherit powerful file, browser or network permissions unless explicitly sandboxed. The official MCP security guidance treats host-level isolation and permission hygiene as distinct from protocol authentication [E9]. HSMC's local edge should default to restricted service accounts, declared resources, short-lived grants and no exposure of development/debug ports to untrusted networks.

9.5 Local-only, private-group and selectively shared participation—without default global exposure

Participation has multiple deliberate modes. LOCAL_ONLY keeps work data and action enforcement inside a person-controlled site; PRIVATE_GROUP lets named family members, staff or students share specific

capabilities; SELECTIVELY_SHARED exposes a screened offer to a wider community under explicit commercial and consent terms. The default for a newly found phone, smart plug, sensor, Hub or office device should not be worldwide discoverability.

The cloud can supply language understanding, planning and optional sync while a local Authority Gate remains the final validator of action; some Work must continue safely offline or wait for permitted reconnection. This separation is the strategic alternative to both vendor App lock-in and ungoverned universal remote control. It also makes participation possible through shared infrastructure without claiming that every one of the 2.2 billion offline people already owns an eligible handset [H1].

9.6 No company permission inherited from personal relationships or maintenance access

The founder's long-standing roles with Pannex, InnoSpire, partners and suppliers remain valuable real relationships, but they do not automatically authorize HSMC to operate those firms' assets, use their customer records, display logos or bind their employees to a new Work. Distinguish personal trust, a conversation, technical access, a commercial agreement and accountable corporate approval. Each company contributes under its own independent authority.

This boundary makes the global call more credible rather than smaller. The vision invites a world of independent phone holders and physical-capability providers to join without selling their identity to a central platform. The first repeatable proof is not a flashy automatic relay demo: it is an authorized request, locally constrained action or refusal, observed physical outcome, human acceptance and replayable evidence.

WORK / DECISION TEST

Chapter 9 passes when a rightful owner can grant one bounded operation, see its attempted and actual effects, deny or revoke it, and demonstrate a safe refusal to an unauthorized model request—without disclosing secrets or transferring company rights.

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] [HSMC · 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. HSMC research architecture. Human-owned assets remain under their rightful authority; no programmatic access to external devices or partners was performed. The ten-billion-phone initiative is a global participation vision, not verified fleet size. AI-assisted translations require independent professional review.

NEXT GATE. Freeze this English Part III source; translate the same 19 subsection IDs into five languages, generate readable A4 and web editions, independently verify citation links, Arabic RTL and browser navigation, then publish a new immutable Part III release without mutating C0-009, C0-010-R1 or C0-012.