

La arquitectura: un teléfono y la realidad que existe más allá

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

GENAI PHYSICAL · INFRASTRUCTURE PROPOSITION

De productos inteligentes controlados por Apps a capacidades físicas gobernadas por personas

La activación de diez mil millones de teléfonos no anuncia una flota comprobada de esa dimensión. Es una invitación mundial a convertir hardware personal y compartido en entradas a Work útil y autorizado. El hogar inteligente centrado en Apps apenas muestra la punta del iceberg: luces, interruptores y sensores poseen capacidades físicas, pero el acceso suele permanecer en interfaces de fabricantes. La oportunidad mayor incorpora herramientas, instalaciones, materiales, habilidades, servicios accesibles y producción.

El cambio arquitectónico reside en situar Human Authority en el límite local controlado. Un modelo remoto propone planes y un cliente MCP invoca herramientas declaradas, pero una operación física sólo procede tras una política local autorizada por el titular, permisos reales del dispositivo, interbloqueos independientes y aceptación humana. El cloud puede colaborar de forma opcional; acercar al ser humano la decisión final no implica eludir emparejamiento legal, seguridad ni derechos comerciales.

CHAPTER 7 / HSIMC BLUEPRINT

7. El teléfono es el primer nodo, no el límite del sistema

Un dispositivo apto abre una Reality bajo control humano, no un derecho a gobernarla

PROPOSITION

Un teléfono reutilizado puede combinar percepción, pantalla, interacción accesible, datos y comunicación. Su valor productivo surge al unirlo de forma segura con equipos, servicios y personas cualificados, no al declarar que la IA puede apropiarse del teléfono.

7.1 Capacidades nativas: sensores, pantalla, almacenamiento, conexión y cálculo

Un móvil sustituido puede conservar cámara, micrófono, altavoz, pantalla, sensores inerciales, ubicación, memoria, Wi-Fi, Bluetooth y cálculo limitado. Estas funciones pueden servir a informes con consentimiento, interfaces públicas accesibles e inspecciones supervisadas. No hace falta ejecutar un modelo grande en el móvil: una clasificación sencilla, un operario humano, un Local Edge común o un modelo remoto elegido pueden producir el resultado.

Ni el año de fabricación ni USB-C prueban aptitud. Batería, temperatura, parches de seguridad, permiso de cámara, accesibilidad, memoria, alimentación y red pueden descartar un equipo para cierto Work. Un NPU tampoco asegura aceleración en cualquier marco; NNAPI está obsoleto desde Android 15 y cada combinación de dispositivo y modelo requiere mediciones [E8].

7.2 Capacidades externas alcanzables: USB, objetos NFC, sensores y servicios de red autorizados

Las Apps domésticas muestran recursos físicos ya instalados: lámparas, interruptores, sensores, termostatos o hubs emparejados que entregan estados y acciones por integraciones permitidas. Un móvil apto también puede enlazar periféricos USB, Bluetooth, servicios Wi-Fi, etiquetas NFC y adaptadores. Fuera de casa, el esquema llega a bancos de ensayo, soportes de taller, relés de baja tensión, quioscos comunitarios, educación, accesibilidad y fabricación supervisada.

MCP presenta herramientas y datos, pero no crea soporte USB Host, confianza Matter, derechos de API del fabricante ni un controlador de motor seguro. Android exige permisos USB sujetos a hardware [E6]. Home Assistant documenta un MCP Server que expone entidades seleccionadas [E3]. Matter necesita incorporación segura y credenciales de Fabric incluso con administradores múltiples [E4, E5]. Cada adaptador declara sólo lo que realmente puede leer o modificar.

7.3 Un nodo compuesto puede ser Server en una capa y Client o Host en otra

Node designa una función en la composición, no necesariamente un teléfono ni una persona artificial. En un mismo equipo, la aplicación Host puede solicitar aprobación, el MCP Client llamar a un servidor local confiable y éste usar un adaptador USB, Matter o de fabricante. También puede ofrecer un servicio limitado a un puesto autorizado y utilizar un sensor externo. Los roles del protocolo no sustituyen al verdadero titular del aparato.

Descubrimiento, razonamiento, evaluación de políticas, ejecución y evidencia pueden vivir en lugares diferentes con identidades separadas. Cada salto autentica a quien llama y registra el poder delegado; una llamada exitosa no concede propiedad sobre el activo inferior. Una sugerencia de la nube sólo es candidata y un guardián local puede rechazarla sin enviar las credenciales del usuario.

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

El teléfono es un inicio modesto. Un Local Hub aporta alimentación, red protegida y cálculo común; un Personal Reality Pod añade un lugar responsable y las condiciones de la persona; una Team coordina roles supervisados; una Company entrega capacidad contractual; una Community vincula aportaciones autorizadas independientemente. Esta posible federación no constituye una flota de diez mil millones de dispositivos propiedad de HSMC.

La escala se construye con consentimiento y pruebas, no con exploración mundial automática. Un alumno puede usar una estación segura, un fabricante ofrecer un soporte y un proveedor atender un pedido conservando empresa y clientes. A quien no disfruta de Internet móvil fiable se le ofrecen interfaces accesibles, lugares con supervisión y sincronización tardía, sin presuponer un teléfono apto [H1].

7.5 Accesible no significa propio, disponible, seguro ni autorizado

Que un dispositivo responda a la red o aparezca en un conector no lo convierte en recurso libre. Deben distinguirse accesibilidad técnica, propiedad, posesión, consentimiento, privacidad, seguridad, firmware, condiciones locales y derecho de ejecución comercial. Una App, un emparejamiento Matter y un token MCP son relaciones diferentes; ninguno basta para autorizar un Work productivo nuevo.

El inventario ha de describir rechazos además de éxitos: REFERENCE_ONLY, DISCOVERED, AUTHORITY_PENDING, QUALIFIED_FOR_SPECIFIED_WORK, TEMPORARILY_UNAVAILABLE y REJECTED. El sistema debe explicar por qué no se abre la puerta. Para personas con poca alfabetización digital, un rechazo comprensible y contacto humano importan tanto como terminar la tarea.

7.6 Rutas de energía, redes, interacción, estructuras y actuación física controlada

La productividad física depende de detalles invisibles en una demostración de App: alimentación y batería, roles USB, calidad del cable, aislamiento de red, fijación, pantalla accesible, iluminación, ambiente, clasificación del relé, aislamiento y parada de emergencia. La salida de vídeo depende del modelo, no de la forma USB-C. La captura de pantalla mediante MediaProjection suele exigir consentimiento por sesión y condiciones de servicio en primer plano [E7].

Un teléfono viejo capaz de ejecutar un modelo o MCP Tool no se convierte por ello en controlador industrial seguro. Deben probarse por separado interbloqueos físicos y lógica local determinista, y limitar las órdenes generadas a parámetros validados. Sin equipamiento y personal cualificados, se captura evidencia para revisión humana en vez de activar bombas, calentadores, cerraduras o maquinaria.

7.7 De la referencia de edificio a habitación, dispositivo, tiempo y capacidad autorizados

El directorio de un edificio nombra una sala y el de dispositivos nombra un teléfono, pero ninguno prueba una Reality apta. El vínculo real de Work incluye encargado del lugar, equipo y adaptador concretos, red y entorno, cita temporal, permisos, ayuda humana, prueba de aceptación y expiración. Sólo las evidencias vigentes de todas esas condiciones permiten el estado ACTIVE_FOR_THIS_WORK.

Ejemplo propuesto: móvil prestado en un banco de reparación supervisado, permiso para fotografiar una muestra específica, comprobación de luz y referencia dimensional, aceptación o rechazo de un informe fechado. El permiso puede caducar con la cita, mientras continúan la identidad Work y las pruebas que sea lícito conservar. No se afirma que este piloto esté desplegado.

WORK / DECISION TEST

El capítulo 7 se acepta si otra persona distingue la función real del teléfono, cada capacidad externa, el responsable, los requisitos y el rechazo seguro, sin confundir equipos conectados con una flota mundial propia.

8. Tools, Resources y Capability Contracts

Convertir acceso técnico en una oferta precisa y revocable de capacidad

PROPOSITION

MCP descubre e invoca herramientas, pero el Work productivo requiere otro contrato que detalle quién ofrece una capacidad, para qué, dónde, durante cuánto tiempo, con qué riesgos, costes, evidencias y aceptación. Capability Contract es una capa de diseño de HSMC, no una función incluida automáticamente en MCP.

8.1 MCP Tools: funciones invocables con entradas, salidas y límites de ejecución

Un Tool es una operación identificada con esquemas de entrada/salida y metadatos. La especificación MCP del 28 de julio de 2026 no depende de un dispositivo ni interfaz. Su guía exige que el servidor valide entradas, controle acceso, limite frecuencia, sanee resultados y mantenga supervisión humana de operaciones relevantes [E1]. El mismo nombre detrás de App, controlador local o API remota no demuestra equivalencia.

Hay que separar observación y actuación. `read_light_state` tiene impacto reducido; `set_lamp_level` requiere objetivo, intervalo y lectura de vuelta; `energize_heater` u `operate_machine` pueden necesitar interbloqueos certificados y aprobación especializada. No publicar `execute_hex` arbitrario, Root ni GPIO ilimitado como herramientas genéricas del modelo. Devolver la lectura física verificada o fallo explícito, jamás éxito inventado.

8.2 MCP Resources: contexto identificado por URI, no propiedad física automática

Una Resource URI identifica una norma, esquema, observación, instantánea de estado o evidencia de Work. No transfiere propiedad, derechos sobre datos ni mando del actuador. Poder leer temperatura no autoriza a subir la calefacción; un QR hacia ficha de producto no equivale a delegación firmada del dueño.

Debe declararse procedencia, fecha, titular, conservación, sensibilidad y audiencia autorizada. Separar fichas técnicas públicas de identificadores privados, historiales de clientes, recorridos y credenciales. El usuario debe saber qué sale del Local Edge y qué resultados pueden sincronizarse. El contexto de un modelo no sustituye el gobierno de los datos.

8.3 Equipos, lugares, materiales y experiencia mediante interfaces gobernadas

Los actuales productos inteligentes son apenas la punta del iceberg de capacidades materiales. Con adaptador cualificado, un móvil puede conocer relés, objetos NFC, instrumentos, cámaras, cables, habitaciones, conocimiento local o proveedores autorizados. Home Assistant y Matter muestran conectividad del hogar, mientras industria y comunidad precisan materias, seguridad y personas [E3, E4].

Interoperar no significa saltarse Apps universalmente. El equipo Matter entra en una Fabric con credenciales criptográficas y emparejamiento consentido; algunas funciones del fabricante todavía dependen de la nube [E4, E5]. Tuya, Aqara u otro servicio requiere compatibilidad y términos vigentes. Si el proveedor sólo ofrece parte de la función, esa frontera se respeta, no se presume control total.

8.4 Manifiestos de capacidad: origen, estado, restricciones, dependencias y pruebas

Un Capability Contract vincula proveedor y activo identificados con una acción limitada para un Work. Declara ID, versión, titular, operador, interfaz, esquemas, equipo y Reality, parámetros autorizados, expiración, cuota, consentimiento, interbloqueos, ruta local o nube, revocación, evidencia, medición y autoridad de aceptación. Firma y revisión pertenecen al diseño HSMC; no son campos que MCP entregue de manera automática.

Ejemplo no ejecutable: una lámpara de prueba ofrece `read_state` en sesión breve y `set_brightness` de 10 a 60 % con confirmación visible. Una ejecución desconectada expira salvo autorización previa. El controlador local comprueba el estado real y rechaza uso fuera del cupo o contexto. El contrato de ejemplo requiere ensayos independientes antes de operar equipos.

[Non-executable Capability Contract blueprint / JSON ↗](#)

8.5 Descubrimiento selectivo sin publicar todo el dispositivo ni sus recursos

Privacidad y escasez exigen exposición mínima. Una familia comparte sólo un informe visual, una empresa un turno de reparación y un proveedor una ficha técnica; el nodo comunitario no revela todos sus discos, cuentas, sensores o trabajadores. MCP admite autorización por petición y exposición filtrada [E1, E2], mientras HSMC añade finalidad y contratos específicos.

El descubrimiento sigue etapas: referencia candidata → resumen aprobado por titular → aptitud → concesión específica de Work → llamada limitada → prueba real → aceptación o revocación. Una lista pública no promete

disponibilidad perpetua. Así una persona puede usar un Hub comunitario sin abrir su casa como control remoto universal.

8.6 Marcas, señales comerciales y derechos de capacidad: activos separados

Interfaz del dispositivo, marca, licencia de datos, autoridad empresarial y derecho del titular son diferentes. HSIMC no obtiene derechos de Tuya, Apple, Matter, Home Assistant, Pannex, InnoSpire o Kingsware por describir compatibilidad pública. Tampoco debe exigirse a fabricantes antiguos aceptar toda la arquitectura antes de suministrar una pieza cualificada.

El contrato identifica quien vende, suministra, opera, asegura, repara y acepta; quien conserva propiedad intelectual y cuando se puede mostrar un logo. Una API documentada evidencia una vía posible, no permiso, respaldo, garantía ni asociación formal. Los colaboradores mantienen su independencia y relaciones históricas.

WORK / DECISION TEST

El capítulo 8 pasa cuando alguien externo inspecciona un Capability Contract y reconoce titular legítimo, alcance, entorno, revocación y lectura física, diferenciando protocolo, contrato comercial y seguridad.

9. Human Authority como límite operativo

Acercar a la persona la decisión decisiva, no darla a un agente sin restricciones

PROPOSITION

La revolución GenAI no elimina consentimiento ni migra mágicamente todas las cuentas de la nube al teléfono. Permite que el responsable legítimo gobierne una política local verificable y su control de ejecución, conservando la nube como colaboradora cuando haya autorización.

9.1 Propiedad, permisos Android, identidad de Client y autorización Work son relaciones distintas

El dueño de un dispositivo, la cuenta que lo emparejó, Android que otorga cámara o USB, el MCP Client y el actor autorizado para un Work pueden ser diferentes. Un token local del fabricante no concede derechos universales. Las credenciales Fabric de Matter crean confianza de dispositivo y la autorización MCP limita clientes; ninguna sustituye el permiso humano para una acción concreta [E2, E4, E5].

Cada Work empieza con un mapa: titular o custodio, supervisor local, identidad autenticada, objetivo físico, receptor de datos, acción propuesta y quien puede negarla. Para privacidad, mostrar qué observaciones irán a un modelo de nube. Para controles importantes, la última validación sigue en el Authority Gate local por convincente que sea la explicación remota.

9.2 Conceder capacidad para un fin, una duración, un cupo y un receptor

Una autorización es delegación estrecha, no conversión de un móvil en infraestructura pública. Debe especificar Work, objetivo, acción y parámetros, persona o rol, vencimiento, número de usos, ubicación o red, receptor de la evidencia y supervisión. El propietario conserva el permiso versionado de manera duradera y revisable en su propio entorno.

La petición ajena al marco se rechaza antes de causar efecto. Lectura de temperatura no habilita calefacción; permiso de una fotografía no permite explorar álbumes; mantenimiento de una empresa no concede acceso a clientes de otra. Sugerencias del modelo, QR y salida de herramienta no son fiables hasta pasar por la concesión activa.

9.3 Aprobación comprensible, actividad visible, revocación accesible y cierre seguro

Human Authority debe entenderse sin formación técnica, también mediante interfaces accesibles. Mostrar acto, equipo, datos que saldrán, costes y reversibilidad. Ofrecer aprobar, rechazar, pausar, revocar, contacto humano y registro de intentos. Para alto riesgo, pulsar confirmar no sustituye interbloqueos independientes ni personal competente.

Revocar bloquea llamadas nuevas de inmediato y define cómo llevar las operaciones iniciadas a estado seguro. El controlador físico, no un modelo textual de nube, impone límites, expiraciones, paradas e interbloqueos. Un motor en marcha no retrocede al borrar el token: el contrato debe describir detención controlada, intervención manual y evidencia posterior.

9.4 Separar privilegios de mantenimiento del acceso MCP normal al trabajo

Instalar un servicio Android, actualizar Ubuntu o sustituir un controlador puede precisar permisos administrativos temporales, que nunca deben copiarse al Work ordinario. Aprovisionamiento, cambio de secretos, reparación y recuperación se separan de lectura o ejecución limitada; cualquier elevación de emergencia necesita auditoría.

El MCP Server local puede ejecutar código con permisos excesivos: sin aislamiento, hereda acceso a archivos, navegador y red del usuario. La guía oficial distingue protección del sistema anfitrión frente a autenticación del protocolo [E9]. Local Edge debe usar cuentas restringidas, recursos declarados, concesiones cortas y puertos de depuración cerrados a redes inseguras.

9.5 Participación sólo local, grupo privado y compartición selectiva sin exposición global

Existen modalidades elegidas: LOCAL_ONLY conserva datos y poder de actuación en el sitio; PRIVATE_GROUP comparte funciones específicas con personas nombradas; SELECTIVELY_SHARED publica ofertas revisadas según consentimiento y contrato. Un móvil, enchufe, sensor, Hub o aparato empresarial recién descubierto no se hace visible mundialmente por defecto.

La nube puede ayudar con lenguaje, planificación y sincronización permitida, pero el Authority Gate local valida toda actuación final. Algunos trabajos siguen sin conexión; otros esperan red autorizada. Es alternativa al

encierro en Apps y al control remoto sin gobierno; compartir instalaciones tampoco significa que toda la población sin Internet tenga móvil apto [H1].

9.6 Ningún poder empresarial se hereda de relaciones personales o mantenimiento

Las funciones históricas del fundador con Pannex, InnoSpire y proveedores merecen respeto, pero no permiten por sí mismas operar activos, leer clientes, usar logos o asignar empleados a un Work de HSMC. Distinguir confianza personal, conversación, acceso técnico, acuerdo comercial y aprobación corporativa responsable. Cada organización participa con autoridad propia.

Así la invitación mundial es más creíble, no menor. Titulares de teléfonos y proveedores de capacidades pueden sumarse sin entregar su identidad a una plataforma central. La primera prueba reproducible no es un relé espectacular activado por IA, sino solicitud autorizada, acción limitada o rechazo, resultado físico observado y aceptación humana con pruebas.

WORK / DECISION TEST

El capítulo 9 se acepta cuando el dueño concede una operación limitada, ve intentos y efectos, puede denegar o revocar y demuestra rechazo seguro de una petición no autorizada sin revelar credenciales ni transferir derechos empresariales.

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. Arquitectura de investigación HSMC. Los bienes permanecen bajo sus titulares; aquí no se ha controlado equipo externo. Diez mil millones es una visión mundial de participación, no un inventario certificado. Las traducciones necesitan revisión profesional independiente.

NEXT GATE. Congelar la fuente inglesa de Part III, alinear cinco traducciones con las 19 secciones, generar PDF A4 y páginas web, revisar citas y árabe RTL, y publicar versión inmutable sin alterar C0-009, C0-010-R1 o C0-012.