

L'architecture : du téléphone à une réalité bien plus vaste

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

GENAI PHYSICAL · INFRASTRUCTURE PROPOSITION

Des objets intelligents pilotés par des Apps aux capacités physiques gouvernées par l'humain

L'activation de dix milliards de téléphones n'est pas l'annonce de dix milliards de machines opérationnelles. C'est une invitation mondiale à faire des équipements personnels et partagés existants une porte d'entrée vers des travaux autorisés et utiles. La maison intelligente contrôlée par des Apps n'est que la partie visible d'un iceberg : lampes, interrupteurs et capteurs possèdent déjà des capacités matérielles, mais leur accès est souvent enfermé dans des interfaces de marque. Le potentiel va bien au-delà du domicile, vers les outils, les lieux, les matériaux, les services et les personnes.

Le changement architectural est de rendre l'Human Authority explicite à la frontière locale contrôlée. Un modèle distant peut proposer un plan et un client MCP appeler un outil déclaré, mais une action réelle doit satisfaire la politique locale voulue par l'ayant droit, les permissions du dispositif, les verrouillages de sécurité indépendants et l'acceptation humaine. Le cloud reste un collaborateur facultatif ; rapprocher la décision finale de l'humain ne signifie pas contourner l'appairage légal, la sécurité ou les droits commerciaux.

CHAPTER 7 / HSIMC BLUEPRINT

7. Le téléphone est le premier nœud, pas la limite du système

Un téléphone admissible donne accès à une Reality appartenant à quelqu'un ; il ne donne pas le droit de la contrôler

PROPOSITION

Un ancien téléphone peut fournir capteurs, affichage, interaction accessible, stockage et transport. Sa valeur productive naît d'une composition sûre avec des équipements, services et personnes qualifiés, non du fait de laisser un agent d'IA « prendre le contrôle » de l'appareil.

7.1 Capacités natives : perception, affichage, stockage, connexion et calcul

Un téléphone remplacé peut encore disposer de caméras, microphone, écran, haut-parleur, capteurs inertiels, positionnement, stockage, Wi-Fi, Bluetooth et calcul limité. Il peut servir à un constat consenti, à une interface publique accessible ou à une inspection supervisée. Il n'a pas à exécuter un grand modèle : un petit classificateur, un opérateur humain, un Local Edge partagé ou un modèle distant choisi peuvent produire le résultat.

L'âge ou le connecteur ne prouvent pas l'aptitude. Batterie, chaleur, correctifs de sécurité, permission caméra, accessibilité, stockage et alimentation peuvent écarter l'appareil d'un Work. L'accélérateur NPU n'est pas exploitable universellement : NNAPI a été abandonnée à partir d'Android 15 et les performances doivent être mesurées par appareil et par modèle [E8].

7.2 Capacités externes accessibles : USB, NFC, capteurs et services réseau autorisés

Les Apps domotiques montrent la capacité physique déjà installée : lampe, interrupteur, capteur, thermostat ou hub appairé peut offrir états et commandes par intégration permise. Un téléphone qualifié peut joindre des périphériques USB, du Bluetooth, un service Wi-Fi, un objet NFC ou un adaptateur. Hors du domicile, le même principe rejoint outillages d'atelier, tests, relais basse tension, kiosques communs, éducation et fabrication supervisée.

MCP expose des outils et des données ; il ne crée ni la fonction hôte USB, ni la confiance Matter, ni les droits d'API du fabricant, ni un actionneur sûr. Android exige des permissions USB liées à son matériel [E6]. Le serveur MCP de Home Assistant expose sélectivement des entités [E3]. Matter nécessite commissioning et identifiants cryptographiques de Fabric [E4, E5]. Chaque adaptateur ne déclare que ce qu'il sait réellement lire ou modifier.

7.3 Un nœud composé peut être Server à un niveau et Client ou Host à un autre

Node désigne une fonction dans l'assemblage, pas une personne artificielle ni forcément un smartphone. Sur un appareil, le Host visible peut demander l'accord humain, le MCP Client appeler un serveur local de confiance et ce serveur utiliser un adaptateur USB, Matter ou propriétaire. Le même téléphone peut exposer un service borné à un poste autorisé tout en consommant un capteur externe. Les rôles protocolaires restent distincts du propriétaire.

Découverte, inférence, décision politique, exécution et preuve peuvent se trouver à des endroits différents sous des identités distinctes. Chaque passage authentifie l'appelant et consigne le pouvoir délégué ; le succès d'un appel n'implique jamais la propriété de l'actif. Une proposition du cloud arrive comme candidate et un garde-fou local peut la rejeter sans publier les secrets du propriétaire.

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

Le téléphone admissible n'est qu'un départ. Le Local Hub apporte énergie fiable, réseau protégé et calcul partagé ; le Personal Reality Pod ajoute un lieu et les conditions d'une personne ; la Team distribue les tâches supervisées ; la Company offre une capacité contractuelle ; la Community coordonne des acteurs indépendamment autorisés. Cette fédération possible n'est pas un stock de dix milliards d'appareils possédés au centre.

L'expansion doit reposer sur l'adhésion volontaire et des preuves. Un étudiant peut emprunter une caméra protégée, un fabricant proposer un support, un fournisseur livrer une commande, chacun en conservant identité et données. Les personnes éloignées de l'Internet mobile doivent pouvoir choisir une interface accessible, un lieu supervisé ou une synchronisation différée, et non être supposées équipées [H1].

7.5 Accessible ne signifie ni possédé, ni disponible, ni sûr, ni autorisé

Un appareil qui répond au réseau ou figure dans une intégration n'est pas librement exploitable. Joignabilité, titre de propriété, possession, consentement, vie privée, sécurité, firmware, environnement et droit commercial doivent être séparés. Une App de marque, un appairage Matter et un jeton MCP attestent des relations différentes ; aucun n'autorise à lui seul un nouveau Work de production.

Le registre doit aussi afficher les refus : REFERENCE_ONLY, DISCOVERED, AUTHORITY_PENDING, QUALIFIED_FOR_SPECIFIED_WORK, TEMPORARILY_UNAVAILABLE ou REJECTED. Il faut montrer pourquoi un contrôle n'a pas été franchi. Pour une personne peu habituée au numérique, un refus compréhensible et la possibilité de joindre un superviseur comptent autant que l'exécution réussie.

7.6 Alimentation, réseaux, interactions, structures et actions physiques contrôlées

La productivité matérielle dépend de détails invisibles pendant une démonstration d'App : batterie, alimentation, rôles USB, câble, isolation réseau, montage, affichage accessible, lumière, environnement, caractéristiques des relais et arrêt d'urgence. La sortie vidéo dépend du modèle ; USB-C ne garantit pas DisplayPort Alt Mode. La capture d'écran Android par MediaProjection requiert généralement accord par session et service au premier plan [E7].

Un téléphone ancien qui exécute un modèle ou un Tool MCP n'est pas pour autant apte à piloter une machine dangereuse. Les interverrouillages matériels et la logique locale déterministe doivent être éprouvés indépendamment, les commandes du modèle limitées à des paramètres validés. Sans personnel ou équipement qualifié, on collecte des observations pour revue humaine au lieu de commander pompe, chauffage, serrure ou machine.

7.7 Du bâtiment de référence à la pièce, au dispositif, au temps et à la capacité autorisés

Un registre de bâtiment donne un nom de lieu, celui des appareils identifie un téléphone ; aucun ne garantit une Reality utilisable. Une vraie liaison de Work comprend responsable local, dispositif et adaptateur, conditions de réseau et d'environnement, créneau, permissions, supervision, test de réception et expiration. Seule la preuve actuelle de tous ces éléments permet l'état ACTIVE_FOR_THIS_WORK.

Exemple proposé : un téléphone prêté sur un établi surveillé, autorisation de photographier une pièce donnée, vérification de l'éclairage et de l'échelle puis acceptation ou refus d'un rapport daté. L'autorisation s'éteint après le rendez-vous ; l'identité Work et les preuves permises subsistent. Il s'agit d'un modèle candidat, pas d'un déploiement déjà réalisé.

WORK / DECISION TEST

Le chapitre 7 est recevable si un testeur indépendant distingue rôle réel du téléphone, capacités externes, responsable, conditions et refus sûr, sans confondre objets connectés et flotte mondiale active appartenant à HSIMC.

8. Tools, Resources et Capability Contracts

Transformer la connectivité technique en proposition précise, limitée et révocable

PROPOSITION

MCP permet de découvrir et d'appeler des outils. Le Work réel exige aussi un contrat distinct : qui fournit une capacité physique, pour quel objectif, dans quel lieu, pendant combien de temps, avec quels coûts, risques, preuves et critères d'acceptation ? Capability Contract est une couche conçue par HSMC, non une fonction fournie automatiquement par MCP.

8.1 MCP Tools : fonctions appelables avec entrées, sorties et limites d'exécution

Un Tool est une opération nommée, munie de schémas d'entrée et de sortie et de métadonnées. La norme MCP du 28 juillet 2026 reste indépendante du dispositif et de l'interface. Elle demande au serveur validation des entrées, contrôle d'accès, limitation du débit, nettoyage des résultats et supervision humaine d'actions importantes [E1]. Le même nom d'outil derrière une App, un contrôleur local ou une API distante ne garantit pas un comportement équivalent.

Il faut distinguer observation et action. `read_light_state` est peu intrusif ; `set_lamp_level` doit désigner la cible, l'amplitude et le contrôle de retour ; `energize_heater` ou `operate_machine` exige potentiellement verrouillages indépendants et personnel qualifié. Ne pas exposer un `execute_hex` arbitraire, Root ou GPIO sans restrictions comme outil universel. Retourner l'état physique réellement lu ou une erreur explicite, pas une réussite imaginée.

8.2 MCP Resources : contexte accessible par URI, pas propriété automatique des actifs

Une Resource URI peut désigner une notice, un schéma, une observation, un état courant ou une preuve. Elle ne transfère ni titre de propriété, ni droits sur les données, ni contrôle des actionneurs. Lire la température d'une pièce n'autorise pas à la chauffer ; le QR d'un produit n'équivaut pas à une délégation signée du propriétaire.

Documenter provenance, date, titulaire, durée de conservation, sensibilité et destinataires. Séparer les spécifications publiques des identifiants privés d'appareils, historiques clients, traces de position et secrets d'accès. L'utilisateur doit comprendre quelles données quittent le Local Edge et ce qui peut être synchronisé. Le contexte fourni à un modèle ne remplace pas la gouvernance des informations.

8.3 Représenter équipements, lieux, matériaux et compétences par des interfaces gouvernées

Les « objets intelligents » ne sont que la pointe de l'iceberg des capacités matérielles. Avec adaptateur qualifié, un téléphone peut observer relais, produit étiqueté, banc de test, caméra d'atelier, câble, pièce, compétence ou fournisseur autorisé. Home Assistant et Matter montrent l'intégration des équipements domestiques ; un Work industriel ou communautaire mobilise aussi matière, sécurité et savoir-faire humain [E3, E4].

Interopérabilité ne signifie pas contournement universel de l'App. Un appareil Matter rejoint une Fabric par appairage autorisé et identifiants cryptographiques ; certaines fonctions propres à un fabricant peuvent dépendre du cloud [E4, E5]. Tuya, Aqara ou autres services restent soumis à leurs protocoles et accords réels. Si un fournisseur n'ouvre qu'une partie de ses capacités, cette limite doit être respectée.

8.4 Manifestes de capacités : provenance, état, contraintes, dépendances et preuves

Un Capability Contract relie un fournisseur et un actif identifiés à l'opération bornée d'un Work. Il indique ID, version, propriétaire, opérateur, interface, schémas entrée/sortie, appareil, Reality, paramètres permis, expiration, quota, consentement, verrouillages, route locale ou cloud, révocation, preuves, mesures et autorité d'acceptation. Sa signature et sa révision sont propres à HSMC, pas des champs MCP automatiquement normalisés.

Exemple non exécutable : une lampe de test offre `read_state` pendant une courte session et `set_brightness` de 10 à 60 % après confirmation visible. L'exécution hors ligne expire sans autorisation préalable. Le contrôleur local relit l'état réel et rejette l'usage hors quota ou hors contexte. Le modèle de contrat joint reste une proposition à tester avant toute action sur matériel réel.

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

8.5 Découverte et contribution sélectives sans publier tout l'appareil

La vie privée et la rareté imposent la divulgation minimale. Une famille peut partager un constat caméra, une société un créneau de réparation, un fournisseur une fiche technique ; un nœud communautaire ne doit pas exposer tous ses comptes, disques, capteurs et employés. MCP permet un contrôle d'accès par requête [E1, E2] ; HSMC ajoute le filtrage par finalité et contrat.

Découvrir par étapes : référence candidate → description approuvée par le titulaire → vérification d'aptitude → autorisation spécifique au Work → appel limité → preuve → acceptation ou révocation. Une liste publique ne garantit aucune disponibilité permanente. Ainsi une personne peut utiliser une capacité partagée sans faire de son domicile un point d'accès mondial.

8.6 Marques, logos et droits de capacité : actifs et permissions distincts

Interface technique, marque, licence de données, autorité commerciale et droit du propriétaire sur l'appareil restent distincts. HSIMC n'acquiert pas les droits de Tuya, Apple, Matter, Home Assistant, Pannex, InnoSpire ou Kingsware par une simple référence à leur compatibilité. Un fabricant traditionnel peut fournir une pièce pour un Work sans adopter toute l'architecture HSIMC.

Le contrat précise qui vend, fournit, opère, assure, répare et accepte, qui conserve la propriété intellectuelle et si l'usage d'une marque est autorisé. Une API connue montre une possibilité d'intégration, non un accord, une garantie ou un aval. Des partenaires indépendants coopèrent sans effacer leurs relations historiques.

WORK / DECISION TEST

Le chapitre 8 réussit lorsqu'un tiers lit un Capability Contract et identifie opérateur légal, portée d'appel, environnement, révocation et preuve physique, tout en séparant interopérabilité technique, droits commerciaux et sécurité.

9. Human Authority comme frontière opérationnelle

Rapprocher la décision conséquente de la personne, pas d'un agent sans limites

PROPOSITION

La transformation GenAI n'efface pas le consentement humain et ne migre pas magiquement tous les droits du cloud vers un téléphone. Elle rend possible un contrôle local vérifiable par le responsable légitime, tout en conservant le cloud comme collaborateur lorsque l'utilisateur l'autorise.

9.1 Propriété, permissions Android, identité du Client et autorisation Work sont distinctes

Le propriétaire d'une lampe, le compte l'ayant appairée, le système Android accordant caméra ou USB, le MCP Client et l'opérateur habilité pour le Work peuvent être cinq acteurs différents. Un jeton constructeur local ne crée pas un droit illimité. La Fabric Matter établit une confiance matérielle ; l'autorisation MCP limite un client ; aucune ne remplace l'accord humain pour une action physique précise [E2, E4, E5].

Chaque Work commence par une carte d'autorité : titulaire ou gardien légal, superviseur, identité authentifiée, cible physique, destinataire des données, action projetée et personne habilitée à refuser. Il faut montrer quelles observations seront envoyées au cloud. Pour une action importante, le point d'application local contrôle la demande même si le modèle distant la justifie brillamment.

9.2 Accorder une capacité selon objet, durée, quota et destinataire

Une autorisation est une délégation étroite, pas une conversion du téléphone en service public. Elle définit Work, capacité cible, action, paramètres, rôle, expiration, quota, lieu ou réseau, destinataire approuvé des preuves et supervision. Le titulaire responsable conserve localement le registre versionné et accessible à l'inspection.

Toute demande hors de cette enveloppe est refusée avant l'effet matériel. Lire la température n'autorise pas à activer le chauffage ; prendre une photo de pièce n'ouvre pas l'album entier ; un contrat de maintenance ne permet pas de traiter les clients d'une autre entreprise. Texte d'IA, QR et sortie d'outil sont non fiables jusqu'à validation contre la permission active.

9.3 Approbation simple, activité visible, révocation accessible et fin sûre

Human Authority doit rester intelligible sans expertise, y compris pour les utilisateurs ayant besoin d'accessibilité. Montrer action, appareil, données sortantes, coût et réversibilité. Donner des choix approuver, refuser, suspendre et révoquer, un contact humain et un journal des tentatives. Pour les risques sérieux, une simple confirmation ne remplace pas un verrouillage indépendant ou une qualification professionnelle.

Révoquer bloque immédiatement les nouveaux appels et définit l'arrêt sûr de ce qui est en cours. Le contrôleur physique, non le modèle cloud, applique délais, amplitudes, arrêts et interverrouillages. Effacer un jeton ne fait pas reculer un moteur déjà en mouvement : le contrat prévoit arrêt contrôlé, commande manuelle et preuve après action.

9.4 Séparer privilèges de maintenance et accès MCP normal au Work

Installer un service Android, mettre à jour Ubuntu ou réparer un contrôleur peut exiger temporairement des droits administrateur. On ne les donne jamais à l'identité du Work ordinaire. Provisionnement, renouvellement des secrets, mise à jour et récupération sont distincts de la perception ou l'exécution bornée, avec traçabilité de toute élévation exceptionnelle.

Un MCP Server local est aussi un risque : sans isolation, le processus peut hériter des fichiers, profils navigateur et accès réseau du compte hôte. La documentation officielle distingue ces droits système de l'authentification protocolaire [E9]. Le Local Edge devrait utiliser comptes de service restreints, ressources déclarées, permissions courtes et aucun port de débogage exposé publiquement.

9.5 Participation locale, groupe privé et partage sélectif sans exposition mondiale par défaut

Trois modes volontaires : LOCAL_ONLY conserve données et autorisation sur site ; PRIVATE_GROUP relie quelques membres nommés ; SELECTIVELY_SHARED diffuse une offre filtrée dans des termes de consentement et de commerce explicites. Téléphone, prise connectée, capteur, Hub ou équipement d'entreprise récemment découvert ne devient pas automatiquement visible partout.

Le cloud peut aider au langage, à la planification et à une synchronisation choisie ; l'Authority Gate local garde la décision finale d'action. Certains Work peuvent avancer sans réseau, d'autres attendent une connexion autorisée. Ce modèle évite à la fois l'enfermement dans une App et la télécommande universelle incontrôlée ; une installation partagée ne signifie pas que les personnes hors ligne possèdent déjà un téléphone apte [H1].

9.6 Aucun droit d'entreprise hérité d'une relation personnelle ou d'un accès de maintenance

Les relations anciennes du fondateur avec Pannex, InnoSpire et les fournisseurs comptent réellement, mais n'autorisent pas automatiquement HSMC à commander leurs biens, lire les clients, afficher leurs logos ou enrôler leurs salariés. Il faut séparer confiance personnelle, conversation, accès technique, contrat commercial et autorisation officielle de chaque entreprise. Chaque organisation contribue sous sa propre responsabilité.

Cette protection rend l'appel mondial plus crédible. Détenteurs de téléphones et fournisseurs de capacités peuvent participer sans céder leur identité à une plateforme centrale. La première preuve reproductible n'est pas un relais spectaculaire commandé par IA, mais une demande autorisée, une action limitée ou refusée, un résultat physique observé et une acceptation humaine audité.

WORK / DECISION TEST

Le chapitre 9 réussit quand le propriétaire peut autoriser une opération limitée, voir tentatives et effets, refuser ou révoquer, et prouver le rejet sûr d'une demande non autorisée, sans divulguer de secrets ni céder de droits d'entreprise.

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. Architecture de recherche HSMC ; les actifs appartiennent à leurs titulaires légitimes. Aucun appareil extérieur ni partenaire n'a été commandé ici. Les dix milliards sont une invitation mondiale, non un inventaire certifié. Relecture linguistique professionnelle indépendante en attente.

NEXT GATE. Geler le maître anglais de la Partie III ; aligner cinq traductions sur les 19 sections, produire PDF A4 et pages web, contrôler citations et arabe RTL, puis publier une édition immuable sans modifier C0-009, C0-010-R1 ou C0-012.