

Activation mondiale : apporter un téléphone et repartir avec une capacité vérifiée

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

Activer une capacité. Préserver l'autorité humaine. Livrer des preuves.

L'activation de dix milliards de téléphones invite le monde à créer de nouvelles formes de participation productive avec les objets existants. Il ne s'agit pas d'un recensement de dix milliards d'appareils prêts. HSIMC propose un parcours du téléphone, de NFC ou d'une entrée partagée accessible vers une capacité locale qualifiée et un résultat accepté par une personne. Un refus motivé, lorsqu'un appareil est inadapté, constitue aussi un résultat valable.

Ne laisser personne de côté exige plus qu'une App prometteuse. Une personne sans NFC, sans réseau continu, avec un vieux mobile ou sans téléphone doit pouvoir choisir, là où un service existe, le QR, la voix et une station partagée sous supervision. L'IA et MCP peuvent proposer ou appeler des outils définis, non créer la propriété d'un appareil, la couverture cellulaire, une batterie sûre ou un consentement humain.

CHAPTER 13 / LOCAL COMMISSIONING & HUMAN REALITY

13. Un réseau local de mise en service pour une participation mondiale

Une méthode reproductible partout, exécutée par des personnes et installations responsables

PROPOSITION

L'échelle mondiale découle de nombreuses activations locales, volontairement autorisées et vérifiables. Elle ne suppose pas que HSIMC possède tous les téléphones. La mise en service est un travail concret : comprendre le besoin, qualifier l'appareil, configurer seulement ce qui est accepté, tester une capacité et remettre un reçu compréhensible.

13.1 Parcours d'activation autonomes, assistés et professionnels

En autonomie, le propriétaire peut suivre des instructions pour une App compatible, une entrée web sécurisée, des permissions limitées et un test simple. Le parcours assisté prévoit un opérateur formé et l'accessibilité pour les personnes qui ne peuvent utiliser de petits écrans, de longs formulaires ou un Internet continu. Le parcours professionnel s'impose pour le câblage, une modification du système, l'étalonnage et la restauration sensible.

Les trois voies partagent les mêmes critères de réception mais pas la même supervision. L'utilisateur choisit une finalité limitée et peut refuser sans perdre les informations publiques. La mise en service n'expose jamais automatiquement le téléphone au monde. Une personne qui apporte seulement une tâche peut utiliser un poste partagé qualifié, sans que cela soit compté comme son téléphone personnel activé.

13.2 Stations d'activation autorisées et kiosques de mise en service proches d'un distributeur automatique

Le kiosque de type distributeur est un concept de service accessible, non une machine habilitée à prendre le contrôle ou à reflasher un téléphone inconnu. Dans une école, un atelier ou un Hub fiable, il présente les options, vérifie le détenteur, inspecte les interfaces et propose un accord ou un refus visible. Chaque session appartient à un opérateur et un lieu identifiés, avec avis de confidentialité et restitution normale de l'appareil.

Chaque station doit prévoir responsabilité, mises à jour, alimentation sûre, protection des données, accessibilité, langues locales et contact humain. NFC ou QR ouvrent une notice, non une preuve de propriété. Le provisioning NFC d'Android Enterprise est un processus distinct pouvant attribuer de puissantes capacités de gestion [E1] ; un simple contact avec une URL publique ne doit jamais déclencher implicitement cette administration.

13.3 Vérifier la propriété et l'état du téléphone ; conserver ou effacer les données seulement avec autorisation

Avant d'accéder aux données privées, identifier le propriétaire ou gardien légitime, le but du service et la permission précise. Examiner batterie, charge, dégâts, OS, correctifs, stockage, radios, ports, accessibilité et politiques éventuelles d'école ou d'employeur. Posséder temporairement le téléphone pour réparation n'autorise pas à déverrouiller des comptes, copier des photos, imposer une gestion à distance ou transférer un rôle e-Person.

Les données demeurent par défaut sous le contrôle de leur titulaire. Sauvegarde, export, transfert et effacement exigent un choix informé et un retour vérifié. Le déverrouillage du bootloader Android peut nécessiter confirmation puis réinitialisation et modifier les garanties de sécurité [E4]. Ne jamais promettre qu'un reflash universel préservera

les données ni imposer un effacement caché pour recevoir une simple aide. Si l'appareil est dangereux ou interdit, arrêter et proposer une alternative.

13.4 Configurer, lier, tester, expliquer les contrôles et remettre un reçu d'activation

Une application installée ne suffit pas. Identifier l'appareil et sa version, le Work autorisé, lieu et créneau, adaptateur ou service MCP réellement testé, superviseur, limites de données et mode de révocation. Réaliser un contrôle convenu avec résultat réel : lecture bornée de la batterie, écriture NDEF NFC autorisée suivie d'une lecture indépendante du tag, ou explication accessible effectivement reçue.

Le reçu distingue DEVICE_INSPECTED, APP_INSTALLED, TOOL_REACHABLE, HUMAN_GRANT_VALID, CAPABILITY_VERIFIED et WORK_ACCEPTED ; aucun état n'implique automatiquement le suivant. Noter versions, date, accord, essais, résultats, erreurs, identifiant des preuves, coût et opérateur sans publier les secrets. Montrer comment recommencer, suspendre ou demander de l'aide. Un test échoué reçoit un refus honnête ou une liste de conditions manquantes.

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

13.5 Un service livré localement selon des méthodes d'ingénierie réutilisables mondialement

Ce qui se reproduit est la méthode : vérification d'admissibilité, Capability Contract borné, instructions accessibles, preuve d'acceptation, test de redémarrage et raisons d'arrêt. Des opérateurs indépendants de différentes villes peuvent utiliser la langue officielle, choisir leurs propres fournisseurs licites et présenter des résultats comparables. Techniciens, universités et centres communautaires contribuent sans céder à HSIMC leur marque ou leurs clients.

Les exemples publics diffusent les conditions de test et les enseignements non sensibles, jamais les identifiants personnels ou mots de passe. Une fédération mondiale se construit avec des capacités acceptées dans leurs propres Reality ; on mesure compréhension, temps jusqu'au résultat, acceptation et reproductibilité plutôt que nombre d'Apps installées. Formation, soutien humain, assurance appropriée et juste rémunération restent nécessaires.

WORK / HUMAN ACCEPTANCE TEST

Le chapitre 13 passe si un lieu indépendant prouve propriété et consentement, aptitude mesurée de l'appareil, permission limitée, lecture réelle de la capacité et reçu compréhensible ; un appareil non pris en charge reçoit un refus sûr documenté ou une alternative assistée.

14. Plusieurs voies de mise à niveau — et non un reflash universel

Choisir la voie adaptée sans sacrifier données personnelles et sécurité

PROPOSITION

Un ancien téléphone peut déjà travailler sans nouveau système d'exploitation. HSMC doit examiner une gamme de méthodes autorisées : petite App, appareil dédié, reflash strictement admissible, Hub intermédiaire ou récupération de sous-systèmes. La voie préférée est la moins intrusive qui satisfait le Work.

14.1 Installer une application MCP-ready limitée sur un système existant compatible

Le premier choix conserve souvent un Android ou autre système pris en charge et installe, si les politiques le permettent, une App à privilèges restreints ou un service MCP local. Le propriétaire garde les contrôles habituels tout en offrant une capacité mesurée : état du téléphone, entrée NFC ou aide accessible. Vérifier version, permissions, origine du package, réseau et comportement en arrière-plan sur le modèle réel.

Le Sony H4493 a montré un outil MCP de lecture limitée, tandis que NFC Writer et lunettes USB conservent leurs contrôles d'acceptation distincts [H2]. Cela ne démontre pas qu'un APK convertit tous les anciens téléphones en nœuds d'IA fiables. L'opérateur distingue ce qui est prêt, ce qui demande une intervention et ce qui est indisponible. Une permission dangereuse ou un OS non pris en charge entraîne un refus.

14.2 Configuration d'appareil dédié lorsque le système d'exploitation la prend en charge

Un appareil admissible appartenant à une institution peut devenir kiosque, station de classe ou terminal affecté à un Work. Android Enterprise distingue profil professionnel, appareil totalement géré et appareil dédié selon le propriétaire, la version et le mode d'inscription [E1]. Ces fonctions d'administration d'entreprise n'autorisent pas à convertir sans consentement le téléphone personnel d'un visiteur.

Préciser qui contrôle la politique, l'isolation des données privées, la sortie du mode et la récupération. Une station partagée exige compte restreint, outils minimaux, clôture des sessions et effacement autorisé seulement. Si le téléphone du visiteur ne peut être inscrit légalement, privilégier le navigateur ou le Hub supervisé plutôt que des droits administrateur.

14.3 Remplacement ou reflash du système par le propriétaire sur les appareils admissibles

Remplacer l'OS peut créer un appareil spécialisé pour certains modèles, mais reste une intervention risquée, jamais la méthode universelle. Vérifier chargeur de démarrage, images et pilotes propres au modèle, accord du propriétaire, récupération, provenance signée et information sur pertes de données, garantie et sécurité. Verified Boot et protection contre le retour aux anciennes versions protègent des images vulnérables et ne doivent pas être contournés pour une démonstration [E4, E5].

La documentation Android explique qu'un déverrouillage admis implique confirmation humaine et effacement des données [E4]. Ne pas promettre de préserver photos, moyens de paiement ou gestion d'entreprise ; ne pas contourner la politique d'autrui. Pour beaucoup de téléphones le reflash sera injustifié ou impossible. Arrêter lorsque le propriétaire refuse ou lorsque image, sécurité et retour ne peuvent être garantis.

14.4 Participation via Hub lorsque le téléphone ne peut travailler seul en sécurité

Un appareil limité peut encore servir d'écran, d'entrée vocale, de caméra consentie ou de point QR/NFC, tandis qu'un Hub qualifié fournit calcul, intégration réseau et Work durable. Si le mobile est dangereux même dans ce rôle, l'utilisateur peut passer à une station collective ou un assistant humain. La proximité du Hub ne lui donne ni données personnelles ni accès général aux appareils.

Préciser pour chaque direction qui transmet les observations, qui les reçoit et qui accepte le résultat. Les tâches hors ligne ne continuent que dans un périmètre local déjà autorisé, puis se synchronisent légalement. Une connexion mobile absente ou un modèle cloud inaccessible est une contrainte à signaler, pas un détail à masquer sous l'étiquette « instant ».

14.5 Récupération, retour arrière, refus des appareils non pris en charge et retrait responsable

Chaque voie doit prévoir désinstallation, arrêt, révocation des secrets, récupération, vérification de sauvegarde et redémarrage après coupure. Tester échecs d'installation, perte réseau, redémarrage, requêtes répétées et indisponibilité du service. Verified Boot et la protection anti-rollback peuvent bloquer un retour vers un OS plus ancien et vulnérable [E5] : il n'existe pas de garantie de restauration universelle.

Sans récupération responsable, marquer UNSUPPORTED_FOR_THIS_WORK. Ne pas maintenir en ligne un vieux téléphone non corrigé avec des interfaces de commande exposées pour améliorer les statistiques. Une réparation sûre, le réemploi non connecté d'un élément ou le recyclage légal peuvent être préférables. Un reçu de retrait doit confirmer l'autorisation des traitements de données et la garde des objets.

14.6 Conserver l'appareil entier, réutiliser un sous-système ou passer par un Hub qualifié

La valeur dépend de la bonne frontière matérielle : téléphone complet comme écran accessible, caméra ou affichage réutilisés par adaptateur vérifié, capteur ou câble séparé, voire Hub remplaçant le téléphone. Le choix s'appuie sur les interfaces, limites électriques, sécurité, fixation, droits logiciels, coûts et maintenance réellement disponibles.

Démonter peut endommager batterie, connecteurs ou enveloppe protectrice. Ne pas improviser de dérivation de protection de batterie ni d'adaptateur haute tension non qualifié. Comparer réemploi, réparation, transport, remplacement et récupération des matériaux ; les gains écologiques doivent être étayés par des données de cycle de vie. Donner un nouveau Work aux objets existants ne signifie pas reconnecter chaque déchet.

WORK / HUMAN ACCEPTANCE TEST

Le chapitre 14 est accepté lorsque l'opérateur justifie la voie choisie, prouve le consentement et la récupération sûre, et peut refuser reflash ou usage connecté si l'appareil, la sécurité ou les données ne répondent pas aux exigences.

15. Faire travailler les actifs existants là où les gens vivent et travaillent

Le dernier mètre de la Reality décide si l'infrastructure mondiale est utile

PROPOSITION

Une capacité démontrée au laboratoire ou sur le téléphone promotionnel d'un vendeur n'est pas encore une infrastructure humaine locale. Son aptitude se prouve au lieu et au moment d'usage, avec énergie, données, montage, accessibilité, sécurité, récupération et personnes responsables.

15.1 Compatibilité par capacité testée, configuration et conditions d'exploitation

La compatibilité est propre à une capacité dans une Reality précise, pas à un logo NFC ou MCP. Documenter modèle, version système, adaptateur, réseau local, interaction, firmware, environnement et résultats. Un appareil peut lire NFC sans écrire tel type de tag ; une App peut ouvrir une URL mais exiger un appui supplémentaire. Les versions Android récentes ont changé le traitement des liens web NFC, d'où la nécessité de tester le parcours réel [E3].

Créer une matrice fondée sur les observations plutôt qu'un catalogue d'hypothèses. Un scan NFC réussi ne prouve ni authenticité de produit, ni contrat signé, ni droit de commande. Conserver QR, URL HTTPS courte, voix et soutien humain quand le tag, le navigateur ou le réseau ne conviennent pas. Une alternative fiable est elle-même une capacité qualifiable.

15.2 Batterie, alimentation, chaleur, fixation et fonctionnement continu

Un ancien téléphone sollicité longtemps n'a pas les mêmes contraintes qu'un mobile utilisé ponctuellement. Vérifier gonflement de batterie, charge, température soutenue, valeur nominale des câbles, fixation et redémarrage après coupure. Utiliser des solutions de charge approuvées et une évaluation électrique quand nécessaire. Une batterie abîmée ou un système qui chauffe n'autorise jamais à contourner les protections.

Décrire le domaine de fonctionnement : durée d'activité, température ambiante, écran allumé, connexion et entretien. Pour un poste public ou un contrôle physique durable, préférer un Hub, une alimentation qualifiée ou un dispositif dédié plutôt que forcer un téléphone retraité à devenir contrôleur industriel sans surveillance. Établir les conditions d'arrêt avant tout essai autonome.

15.3 Combiner périphériques, connexion et alimentation sans supposer la compatibilité

Le connecteur USB-C ne garantit pas hôte USB, webcam, HDMI ou DisplayPort Alt Mode, Ethernet ni charge simultanée. Tout dépend de la version OS, du contrôleur, de l'accessoire, du budget électrique, des pilotes et du câble. L'API Android USB Host permet l'énumération et les permissions, pas l'usage automatique de tout périphérique [E2].

Définir séparément alimentation, réseau, données et sécurité. Tester les lunettes/caméra avec autorisation, vraie lecture d'image, conservation et récupération ; un NFC Writer réussi ne valide pas cet ensemble. Un relais basse tension nécessite qualification de charge, isolation et arrêt indépendant. Un modèle de langage ne doit pas produire des commandes matérielles brutes sans limites.

15.4 Réseau intermittent, tentatives répétées, arrêt sûr et redémarrage

Le Work doit fonctionner avec le réseau que les personnes possèdent réellement. Une tâche peut commencer hors ligne sur une station fiable, recueillir une observation permise, attendre la synchronisation légale puis reprendre sous le même Work ID. Séparer réessais du réseau et nouvelle demande humaine, préserver seulement les preuves autorisées et annoncer quand les services ou superviseurs distants sont indisponibles.

Tester Wi-Fi coupé, réseau mobile perdu, panne d'alimentation, redémarrage d'App, Tool bloqué, jeton expiré, annulation et changement d'opérateur. La récupération lit le véritable état, pas le succès déclaré dans un ancien message. Si des effets physiques existent, un contrôleur local testé doit assurer l'arrêt sûr et permettre l'intervention d'une personne identifiée.

15.5 Mises à jour signées, réparation, vulnérabilités et décisions de fin de support

Un nœud utile peut devenir inadapté lorsque ses correctifs cessent, qu'une bibliothèque devient suspecte, qu'un composant casse ou qu'une API change. Les opérations admissibles exigent origine logicielle connue, vérification des mises à jour, compte restreint, protection des secrets, réponse aux incidents et responsable d'entretien. Verified Boot et images signées réduisent certains risques sans garantir la sécurité future [E5].

Une fédération mondiale ne doit pas imposer la même politique à tous les propriétaires ou réparateurs. Publier les limites de support et routes de migration par capacité ; distinguer mises à jour volontaires et politiques d'entreprise. Suspendre un nœud compromis sans effacer l'historique Work légal. Quand l'exploitation connectée n'est plus défendable, l'usage hors réseau, le Hub ou le retrait sont des réponses responsables.

15.6 Alimentation et données stables au poste humain, pas seulement à la source

Les fiches indiquent souvent la puissance nominale du chargeur ou câble, alors que le résultat dépend de la tension et des données au dispositif réel sous charge. Longueur, résistance du cuivre, connecteurs, sorties USB-C

partagées, négociation de puissance, parasites et usure affectent caméras, Hub et téléphones. Une étiquette 100 W ne garantit pas une alimentation stable pour deux appareils simultanés ni des données fiables.

Mesurer tension, température, rôles, fonctionnement continu et communication au poste, pas uniquement au chargeur. Les comparaisons techniques nécessitent instruments étalonnés et traces de protocole. L'expérience de Pannex en produits physiques peut contribuer à des câbles qualifiés, sans transférer automatiquement les droits des autres entreprises ni certifier chaque installation mondiale.

15.7 Montage mécanique, interaction accessible, récupération et protections indépendantes

Le dispositif doit réellement s'adapter à la personne et au travail : portée, prise, aide visuelle et auditive, lisibilité, retour vocal ou tactile, hauteur, câbles au sol, accès d'urgence, nettoyage, vibration et environnement. Un Hub partagé doit permettre de comprendre l'autorisation, choisir une alternative et contacter un humain sans maîtriser des commandes techniques.

Quand IA, mécanisme mobile et utilisateur vulnérable se rencontrent, les protections indépendantes deviennent essentielles. Consentement, contrôle d'accès et sécurité matérielle sont trois systèmes différents ; valider arrêt d'urgence et isolation hors du modèle. Refuser une installation dangereuse ou inaccessible même si la démonstration fonctionne. Le but est le choix autonome, non l'adaptation forcée à une machine mal conçue.

15.8 Fabrication de recherche à l'échelle du bureau : procédés choisis et limites vérifiées

Un site de recherche HSMC peut préparer des supports, étiquettes, adaptations basse tension et assemblages d'essai avec outils appropriés et supervision qualifiée. Il peut confier usinage, travaux électriques, réglage optique, conception accessible ou analyse de matériaux à des spécialistes extérieurs. Cela ne signifie pas qu'un bureau, une école ou une bibliothèque possède les autorisations de toutes les industries ou du traitement de déchets dangereux.

Pour chaque essai, documenter procédé, origine des matériaux, limites de l'équipement, opérateur qualifié, protections, accords nécessaires, mesures et réception. Accessible Product Passport neutre par NFC/QR et Human-Guided Circular Work à faible risque sont des candidats ; marques FIFA, données licenciées, lithium dangereux, dispositifs médicaux et machines critiques exigent des parcours distincts. La répétition responsable part de preuves vérifiables.

WORK / HUMAN ACCEPTANCE TEST

Le chapitre 15 réussit lorsqu'un deuxième lieu reproduit la capacité dans des conditions physiques vérifiées — énergie et données au bon endroit, accès, fixation, reprise, pouvoir humain et sécurité — et sait expliquer un refus. La participation mondiale ne grandit qu'à partir de Works locaux acceptés.

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. La Partie V est un plan de recherche pour une mise en service locale volontaire. Dix milliards désigne une invitation, pas une population d'appareils inspectés. Sans téléphone ni Internet, un lieu supervisé peut être nécessaire. Les traductions assistées par IA attendent une relecture professionnelle. La publication n'enrôle aucun appareil, SIM, bootloader ni partenaire.

NEXT GATE. Geler l'anglais de Part V et aligner les cinq traductions sur 19 sections ; valider six PDF A4 et HTML, puis publier une édition additive après contrôles HTTPS et navigateur en préservant les versions antérieures.