

Архитектура: телефон и окружающая его физическая реальность

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

GENAI PHYSICAL · INFRASTRUCTURE PROPOSITION

От умных изделий в отдельных приложениях к физическим возможностям под контролем человека

Инициатива десяти миллиардов телефонов не означает, что столько пригодных устройств уже работает. Это всемирное приглашение превращать существующие личные и общие устройства во входы к полезному, разрешённому Work. Умный дом с приложениями — лишь верхушка айсберга: светильники, выключатели и датчики обладают физическими функциями, но управляются через интерфейсы производителей. Более масштабная возможность соединяет оборудование, места, материалы, людей, мастерские и доступные услуги.

Архитектурный сдвиг делает Human Authority явной на контролируемой локальной границе. Облачная модель может предложить план, MCP Client вызвать описанный инструмент, но реальные действия допустимы только при локальной политике законного владельца, системных разрешениях, независимых аппаратных блокировках и человеческой приёмке. Облако может помогать; приближение исполнительного решения к человеку не отменяет законного сопряжения, безопасности и прав партнёров.

CHAPTER 7 / HSIMC BLUEPRINT

7. Телефон — первый узел, но не граница всей системы

Пригодное устройство открывает вход в подконтрольную человеку Reality, а не право управлять ею

PROPOSITION

Старый телефон способен объединять датчики, дисплей, доступное взаимодействие, данные и связь. Его продуктивность возникает при безопасной композиции с квалифицированным оборудованием, услугами и людьми, а не от утверждения, будто агент ИИ может бесконтрольно захватить аппарат.

7.1 Встроенные возможности: датчики, дисплей, память, связь и вычисления

После замены основного телефона могут сохраниться камеры, микрофон, динамик, экран, инерциальные датчики, геопозиция, накопитель, Wi-Fi, Bluetooth и ограниченные вычисления. Это позволяет вести согласованный отчёт о состоянии, доступный общественный интерфейс или осмотр под надзором.

Большая модель на самом телефоне не обязательна: результат может обеспечить простой классификатор, оператор, общий Local Edge или избранная облачная модель.

Возраст и разъём не подтверждают пригодность. Аккумулятор, нагрев, обновления безопасности, разрешение на камеру, доступность, память, сеть и питание могут исключить устройство из конкретного Work. Использовать NPU универсально тоже нельзя: NNAPI объявлен устаревшим в Android 15, а производительность требуется проверять для каждого телефона и модели [E8].

7.2 Доступные внешние возможности: USB, NFC-объекты, датчики и разрешённые сетевые службы

Домашние Apps демонстрируют уже установленную физическую базу: сопряжённая лампа, выключатель, датчик, термостат или Hub могут передавать состояние и выполнять команды через разрешённую интеграцию. Пригодный телефон связывается также с USB, Bluetooth, Wi-Fi, NFC и адаптерами. За пределами дома сюда относятся оснастка мастерской, измерители, низковольтные реле, общие терминалы, образование, доступность и производство под надзором.

MCP описывает инструменты и данные, но не создаёт поддержку USB Host, доверенную Matter Fabric, право на API поставщика или безопасный привод. Android требует аппаратной поддержки и разрешения для USB [E6]. Home Assistant позволяет избирательно открыть сущности MCP Server [E3]. Matter

использует безопасное сопряжение и криптографические ключи Fabric, включая многопользовательское администрирование [E4, E5]. Адаптер вправе обещать только реально поддерживаемые операции.

7.3 Составной узел — Server на одном уровне и Client или Host на другом

Node обозначает роль в архитектуре, а не непременно телефон или ИИ-персону. На одном аппарате видимое Host-приложение запрашивает согласие, MCP Client вызывает надёжный локальный Server, а тот обращается к отдельному USB-, Matter- или фирменному адаптеру. Телефон может предоставлять ограниченный сервис рабочей станции и одновременно пользоваться чужим датчиком. Роли протокола отличны от прав собственника.

Обнаружение, вывод модели, применение правил, физическое исполнение и доказательства могут работать в разных местах под разными идентичностями. Каждый переход проверяет вызывающего и делегированную способность; успешный вызов не делает верхний сервис владельцем оборудования. Облачное предложение остаётся кандидатом, а местный Authority Gate отклоняет неподходящий запрос, не выдавая секреты владельца.

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

Пригодный телефон — отправная точка. Local Hub добавляет питание, защищённую связь и общие вычисления; Personal Reality Pod — ответственное место и реальные условия человека; Team организует роли под надзором; Company предоставляет договорную способность; Community соединяет независимо авторизованные ресурсы. Это возможная федерация, а не центрально принадлежащие HSIMC десять миллиардов устройств.

Масштаб рождается из добровольного участия и доказательств, не из глобального сканирования. Студент может использовать общую камеру, мастер изготовить держатель, поставщик выполнить заказ, сохраняя имя компании и клиентов. Людям без постоянного мобильного интернета нужны доступные интерфейсы, контролируемые площадки и отложенная синхронизация, а не предположение о дорогом телефоне [H1].

7.5 Доступен — не значит принадлежит, готов, безопасен или разрешён

Ответ на ring или запись в интеграции ещё не дают прав на использование. Техническая достижимость, собственность, владение, согласие, приватность, безопасность, доверие к прошивке, рабочая среда и коммерческие права разделяются. Фирменная App, сопряжение Matter и токен MCP отражают разные отношения; ни один из них не разрешает новый производственный Work сам по себе.

Реестр обязан показывать отказы и успехи: REFERENCE_ONLY, DISCOVERED, AUTHORITY_PENDING, QUALIFIED_FOR_SPECIFIED_WORK, TEMPORARILY_UNAVAILABLE и REJECTED. Причина закрытой границы должна быть проверяема. Для пользователя с небольшими цифровыми навыками понятный отказ и контакт с живым специалистом важны не меньше удачной операции.

7.6 Питание, сети, интерфейсы, конструкции и управляемое физическое действие

Физическая продуктивность зависит от скрытых в App-демо вещей: аккумулятора, безопасного питания, ролей USB, качества кабеля, сетевой сегментации, крепления, доступного экрана, освещения, условий среды, номиналов реле, изоляции и аварийного останова. Выход зависит от модели: USB-C не гарантирует DP Alt Mode. Захват экрана Android через MediaProjection обычно требует отдельного согласия и выполнения правил службы на переднем плане [E7].

Старый телефон с MCP Tool или моделью не становится контроллером для опасного оборудования. Нужны отдельно испытанные аппаратные блокировки и детерминированная локальная логика, а команды модели ограничиваются проверенными параметрами. Без квалифицированных устройств и персонала следует фиксировать наблюдение и обращаться к человеку, не включая насос, нагреватель, замок или машину.

7.7 От справочного здания к разрешённой комнате, устройству, времени и доказанной способности

Реестр помещений может назвать комнату, реестр оборудования — телефон, но этого мало для Reality. Реальное связывание Work включает ответственного хозяина, конкретный аппарат с адаптером, сеть и среду, временное окно, разрешения, надзор, проверку приёма и срок действия. Только актуальные доказательства открывают состояние ACTIVE_FOR_THIS_WORK.

Предлагаемый пример: заимствованный телефон на контролируемом ремонтном столе, согласие владельца на фото конкретного образца, проверенные освещение и масштаб, принятие или отклонение датированного отчёта. Разрешение прекращается после сеанса, но допустимые доказательства и идентичность Work продолжают. Это шаблон, не заявление о развёрнутом сервисе.

WORK / DECISION TEST

Глава 7 принята, если второй испытатель различает роль телефона, внешние способности, ответственного оператора, условия и безопасный отказ, не называя подключённые устройства собственной работающей всемирной сетью.

8. Tools, Resources и Capability Contracts

От технической доступности к точному, ограниченному и отзывному предложению

PROPOSITION

MCP открывает и вызывает инструменты, но производственный Work требует отдельного договора: кто предлагает способность, для чего, где, на какой срок, с какими затратами, рисками, доказательствами и приёмкой. Capability Contract — проектный слой HSMC, а не автоматическая функция MCP.

8.1 MCP Tools: вызываемые функции с явными входами, выходами и пределами

Tool — именованная операция со схемами входа и выхода и метаданными. Спецификация MCP 2026-07-28 не привязана к одной ОС или оборудованию. Её требования включают проверку входов, управление доступом, частотой, очисткой ответов и возможность человеческого контроля значимых действий [E1]. Одинаковое имя инструмента через App, локальный контроллер или API облака не доказывает одинаковую надёжность.

Нужно разделять наблюдение и воздействие. `read_light_state` имеет небольшой эффект; `set_lamp_level` должен ограничивать цель, диапазон и обратное чтение; `energize_heater` или `operate_machine` могут требовать аппаратной блокировки и специалиста. Нельзя давать модели произвольный `execute_hex`, Root или неограниченный GPIO как обычные Tools. Ответ должен отражать реально прочитанное состояние либо явную ошибку.

8.2 MCP Resources: адресуемые URI данные, а не права на физическое имущество

Resource URI указывает на документ, схему, наблюдение, состояние или доказательство Work. Он не передаёт имущественное право, лицензии на данные и управление исполнительным механизмом. Возможность прочитать температуру не разрешает включить обогрев, а QR-код на карточке изделия не является подписанным поручением владельца.

Нужно объявлять происхождение, свежесть, владельца, срок хранения, чувствительность и круг получателей. Открытые спецификации отделяются от частных ID устройств, истории клиентов, геотреков и ключей доступа. Пользователь должен понимать, что покинет Local Edge и какие агрегированные сведения разрешены к синхронизации. Контекст модели не заменяет управление информацией.

8.3 Оборудование, помещения, материалы и навыки в управляемых интерфейсах

Существующие «умные изделия» — лишь верхушка айсберга материальных способностей. Телефон с квалифицированным адаптером может наблюдать реле, NFC-метку, измеритель, оснастку камеры, кабель, комнату, местного специалиста или поставщика. Home Assistant и Matter показывают доступные бытовые интеграции, но промышленному и общественному Work нужны также материалы, безопасность и человеческая квалификация [E3, E4].

Совместимость не означает универсальный обход Apps. Устройство Matter требует разрешённого commissioning и криптографических ключей Fabric; отдельные функции производителя могут по-прежнему зависеть от облака [E4, E5]. TuYa, Aqara или другой сервис подключаются только согласно текущему протоколу и договору. Если партнёр открыл часть функций, HSMC не имеет права приписывать ему полный контроль.

8.4 Манифест способности: происхождение, состояние, ограничения, зависимости и доказательства

Capability Contract привязывает известного поставщика и актив к ограниченной операции конкретного Work. Он указывает ID и версию, собственника, оператора, интерфейс, схемы, устройство, Reality, пределы действия, срок, квоту, согласие, блокировки, локальный или облачный маршрут, отзыв, доказательства, измерение и полномочия приёмки. Подпись и ревизия принадлежат проекту HSMC и не считаются автоматически полями MCP.

Неисполняемый пример: тестовая лампа предлагает `read_state` в короткой сессии и `set_brightness` от 10 до 60 % только после видимого подтверждения. Офлайн-выполнение истекает без предварительного согласия. Локальный контроллер считывает фактическое состояние и отказывает при превышении квоты или вне контекста. Контракт требует испытаний до доступа к реальному устройству.

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

8.5 Избирательное обнаружение без публикации всего устройства и ресурсов

Приватность и ограниченность ресурсов требуют минимального раскрытия. Семья может дать только результат камеры, фирма — время ремонта, поставщик — спецификацию; общественный Hub не должен показывать все накопители, аккаунты, датчики и работников. MCP допускает проверку доступа на каждый запрос [E1, E2], а HSMC накладывает контрактный фильтр цели.

Этапы: кандидат → одобренное владельцем описание → квалификация → грант на Work → ограниченный вызов → реальное доказательство → приёмка или отзыв. Публичный список не гарантирует постоянную доступность. Благодаря этому человек пользуется общим узлом, не делая частное помещение мировым дистанционным пультом.

8.6 Бренды, товарные знаки и права способности как независимые активы

Технический интерфейс, бренд, лицензия данных, коммерческое право компании и управление владельцем — разные объекты. HSMC не приобретает права TuYa, Apple, Matter, Home Assistant, Pannex, InnoSpire или Kingsware через описание открытой совместимости. И традиционному производителю не нужно принимать всю материнскую систему HSMC, чтобы поставить подходящую деталь.

Соглашение показывает, кто продаёт, предоставляет, эксплуатирует, страхует, чинит и принимает Work, кому принадлежат права и можно ли показывать марку. Известная API — возможный маршрут, но не разрешение, поддержка или гарантия. Участники сохраняют собственность и исторические связи.

WORK / DECISION TEST

Глава 8 проходит проверку, когда третья сторона читает Capability Contract и видит законного оператора, область вызова, среду, отзыв и физическое подтверждение, не путая протокол, коммерческий договор и безопасность.

9. Human Authority как граница исполнения

Последнее значимое решение ближе к человеку, а не к агенту без ограничений

PROPOSITION

Трансформация GenAI не убирает согласие и не переносит волшебю все облачные права на телефон. Она делает возможной проверяемую местную политику и контроль действий у законного ответственного лица, сохраняя облако как партнёра, когда его разрешили.

9.1 Собственность, разрешения Android, личность Client и авторизация Work различны

Владелец прибора, аккаунт сопряжения, Android, выдающий доступ к камере и USB, MCP Client и оператор, имеющий право на конкретный Work, могут отличаться. Токен производителя не превращается в безграничное право. Matter Fabric задаёт доверие устройства, авторизация MCP ограничивает клиента, но для физического действия требуется отдельное человеческое решение [E2, E4, E5].

В начале Work строят карту полномочий: собственник или хранитель, местный руководитель, идентичность вызвавшего, объект, получатель данных, планируемое действие и тот, кто может отказать. Для конфиденциальных работ показывают данные, передаваемые облачной модели. Для значимого управления обязательный Authority Gate остаётся локальным независимо от текста обоснования.

9.2 Разрешать конкретную способность на цель, срок, квоту и получателя

Грант — узкое делегирование, а не перевод всего телефона в публичную службу. В нём есть Work, целевая способность, действие и параметры, человек или роль, окончание, число вызовов, местоположение или сеть, одобренный адресат доказательств и надзор. Ответственный хранит локально проверяемый журнал версий и обеспечивает доступный просмотр.

Запрос за пределами рамки отклоняется до материального эффекта. Чтение температуры не разрешает включать отопление; согласие на одно фото не открывает галерею; техническое обслуживание не даёт доступ к клиентам другой фирмы. Текст модели, QR и результаты неизвестной функции недоверенны до проверки активного гранта.

9.3 Простое подтверждение, видимые действия, доступный отзыв и безопасное завершение

Human Authority должен быть понятен неспециалисту и людям, использующим доступные интерфейсы. Показать что будет сделано, устройство, выходящие данные, стоимость и обратимость. Нужны одобрение, отказ, пауза, отзыв, контакт человека и журнал попыток. При риске для жизни и имущества одного подтверждения недостаточно — требуются независимые блокировки и компетентный персонал.

Отзыв немедленно прекращает новые запросы, но для выполняемого процесса требуется безопасная остановка. Физический контроллер, а не облачная текстовая модель, ограничивает диапазоны, время и аварийный останов. Удаление токена не останавливает автоматически движущийся мотор: контракт задаёт останов, ручное управление и запись результата.

9.4 Привилегии обслуживания отдельно от обычных MCP прав Work

Для установки Android-сервиса, обновления Ubuntu или замены драйвера иногда нужны временные администраторские права. Их нельзя копировать на обычную идентичность Work. Настройка, смена ключей, обновления и восстановление отделяются от низкопривилегированного наблюдения и выполнения, а экстренное повышение прав документируется.

Локальный MCP Server тоже риск: без изоляции запущенный процесс может наследовать права на файлы, профили браузера и сеть. Официальные рекомендации разделяют защиту хоста и авторизацию протокола [E9]. Local Edge должен применять ограниченные служебные аккаунты, объявленные ресурсы, короткие гранты и закрытые для чужих сетей порты отладки.

9.5 Локальный, частный и выборочно общий доступ без публикации всего мира

Участие имеет разные добровольные режимы. LOCAL_ONLY хранит данные и право действия на месте; PRIVATE_GROUP открывает отдельные функции названным родственникам, сотрудникам или учащимся; SELECTIVELY_SHARED публикует проверенное предложение на явных коммерческих условиях. Только что найденный телефон, датчик, Hub или офисный прибор не становится автоматически глобально доступным.

Облако помогает с языком, планом и разрешённой синхронизацией, но местный Authority Gate окончательно проверяет действие. Некоторый Work можно безопасно продолжать офлайн, другой ждёт

соединения. Это альтернатива и закрытым App-системам, и неуправляемому дистанционному контролю. Общий Hub не доказывает, что все люди вне интернета уже имеют пригодные смартфоны [H1].

9.6 Права компании не наследуются из личных отношений или технического обслуживания

Долгосрочные функции основателя в Rannex, связи с InnoSpire и поставщиками важны и реальны, но не дают HSMC автоматических полномочий управлять чужими объектами, читать клиентские данные, использовать логотипы и назначать сотрудников. Нужно разделять личное доверие, разговор, технический доступ, договор и официальное решение компании. Каждая фирма участвует в собственных границах.

Такая защита делает мировое приглашение убедительнее, а не меньше. Владельцы телефонов и поставщики физических возможностей могут участвовать, не продавая свою идентичность центральной платформе. Первая повторяемая проверка — не эффективная команда реле от ИИ, а разрешённый запрос, ограниченное действие или отказ, измеренный физический эффект и принятый человеком результат.

WORK / DECISION TEST

Глава 9 проходит, когда законный владелец может разрешить одну ограниченную операцию, видеть попытки и эффекты, отказать или отозвать право и доказать безопасное отклонение команды модели без утечки секретов и уступки корпоративных прав.

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. Исследовательская архитектура HSMC. Активы остаются в ведении законных владельцев; здесь не выполнялось управление чужими устройствами. Десять миллиардов — мировая инициатива участия, не проверенный парк. Требуется независимая профессиональная вычитка переводов.

NEXT GATE. Зафиксировать английский оригинал Part III; сопоставить пять переводов с 19 разделами, создать читаемые A4 PDF и сайты, проверить источники и арабское RTL, затем опубликовать неизменяемую версию, сохраняя C0-009, C0-010-R1 и C0-012.