apkudo | GSMA | INTERNATIONAL DATA SPACES ASSOCIATION

WHITEPAPER: DEVICE HOMOLOGATION

Trusted Device Passports

How Data Spaces Enable Sovereign IMEI Sharing for Homologation

00

Executive Summary

Global device homologation has a trust problem, not a technical one. This whitepaper presents a proven architecture to solve it.

Regulators need granular device identity data to combat counterfeit hardware and enforce homologation compliance. Original Equipment Manufacturers (OEMs) treat that same data as core intellectual property, because it maps their manufacturing yields, regional allocations, and market strategy.

The result is an impasse. Proposals such as the ITU-T Q.5057 mandate asked OEMs to upload bulk, unencrypted International Mobile Equipment Identity (IMEI) datasets to centralized government registries. OEMs pushed back — not to avoid compliance, but because the architecture itself exposes competitive intelligence.

That impasse is solvable. By adopting a Data Space architecture grounded in the International Data Space Reference Architecture Model (IDS-RAM) and the open Dataspace Protocol (DSP), the industry can deliver exactly what regulators need — cryptographic, real-time device verification — without exposing a single row of production data.

The Device Passport™ delivers it: a policy-governed, query-only data object that answers the regulator's question — "Does this IMEI belong to an approved device?" — with a single, verifiable answer. No spreadsheets. No bulk exports. No competitive exposure.

GSMA, the neutral global administrator of the IMEI registry and Type Allocation Code (TAC) system, is the natural convening authority for this initiative. Apkudo provides the operational infrastructure that connects OEM device lifecycle data to DSP-compliant data space connectors. Together, they form the foundation of a trusted, scalable, and OEM-acceptable homologation framework.

Beyond the data spaces concept, this paper specifies the practical details that homologation participants most often seek: where OEM data physically resides and who hosts it, the connector that controls access to it, the rulebook that governs all participants, and the step-by-step lifecycle of a single verification query. These are the details that turn *What is a data space?* into *How do I participate?*

The Hidden Cost of Counterfeit Devices

Counterfeit hardware is not a fringe problem. It is a systemic threat that costs OEMs revenue, brand equity, and market access — and current regulatory tools are making it worse.

What Homologation Is, and Why It Matters

Homologation is the formal process by which a government confirms that a radio-emitting device meets national technical, safety, and legal requirements before it may be sold or operated on a domestic network. Every market has its own requirements: frequency bands, SAR limits, electromagnetic compatibility (EMC) certifications, and more. A device that passes homologation in one country may require separate certification in another.

For OEMs, homologation is not optional. Failure to obtain approval blocks market entry entirely. Homologation bottlenecks in the New Product Introduction (NPI) process delay launch dates, strand inventory in bonded warehouses, and erode the first-mover advantage that premium device launches depend on.

When a shipment is quarantined at the border due to IMEI discrepancies — whether caused by counterfeit cloning or registration gaps — the OEM absorbs warehousing costs, the inventory depreciation, and the loss of the retail launch window. Flagship devices earn most of their revenue in a 90-day peak cycle, so a two-week delay is a material financial event.

How IMEI Fraud Enables Counterfeits to Evade Detection

The IMEI is a 15-digit number uniquely assigned to every mobile device. Regulators and other industry stakeholders rely on it to verify whether a device was legitimately manufactured and approved.

Counterfeiters have industrialized IMEI fraud. The most common attack is cloning: harvest a legitimate, homologation-approved IMEI from a genuine device, then assign it to an unapproved, substandard, or outright fake device. The counterfeit passes basic network-level checks because the IMEI it presents belongs to an approved device model.

The damage cascades. Consumers receive unsafe or non-compliant devices. Legitimate OEMs bear reputational damage from quality failures attributed to their brand. Regulators, unable to trust device identity data, escalate demands for broader and more invasive data sharing from manufacturers.

THE CLONING ATTACK

One approved identity, harvested once, resold across unlimited hardware.

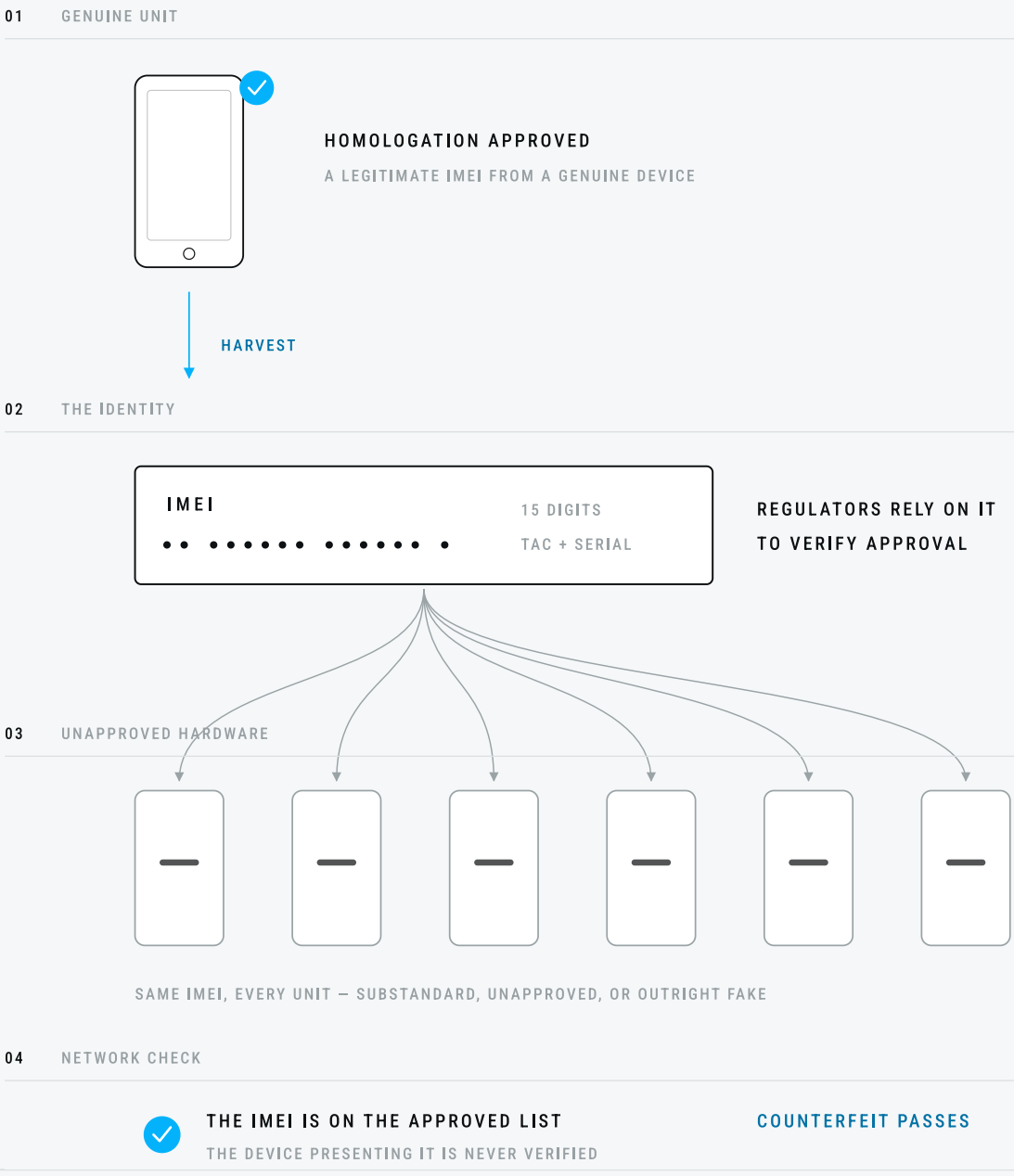


FIGURE 1

The counterfeit passes basic network-level checks because the IMEI it presents belongs to an approved device model. The identity is verified. The hardware carrying it is not.

Why Bulk Sharing Falls Short

The instinct to centralize device identity data is understandable. The consequences of doing so are not.

The ITU-T Recommendations

The International Telecommunication Union (ITU) has developed a number of recommendations and guidelines for national device management policies. The latest proposes a centralized repository where OEMs would upload bulk IMEI datasets paired with device specifications and target market identifiers. The intent is sound: give regulators a verified source of truth for device identity. The execution is the problem.

Why OEMs Reject Bulk Sharing

A bulk IMEI list is not simply a list of serial numbers. It is a precise, time-stamped map of an OEM's global production strategy. From a sufficiently large IMEI dataset, competitors or adversarial actors can reverse-engineer:

- Total manufacturing yield for a specific device model
- Regional allocation volumes — how many units were produced for each market
- Launch timing and sequencing strategy
- Inventory positioning
- Possibly confidential commercial arrangements

This is not theoretical. Production volume data is among the most sensitive pieces of competitive intelligence that manufacturers hold. Revealing it — even to a government registry with ostensibly secure controls — creates risk that OEM legal, finance, and strategy teams uniformly reject.

The architecture compounds the risk. Once data is uploaded to a centralized repository via legacy API or FTP transfer, the OEM loses all downstream visibility and control. There is no mechanism to audit who accessed the data, revoke access if policy changes, or verify that usage complies with the original intent of the data submission.

Centralized databases are also high-value targets: a single breach exposes the production data of every participating manufacturer simultaneously.

The Trust Gap

The result is a standoff. Regulators cannot effectively combat IMEI cloning without reliable device identity data. OEMs will not provide that data in a form that exposes their commercial interests. Neither party is acting irrationally — the current architecture simply cannot satisfy both requirements simultaneously.

What Is Missing

A mechanism for verifiable disclosure without full exposure — one that allows a regulator to confirm device authenticity without an OEM ever surrendering bulk production data. That mechanism now exists.

Introducing Data Spaces
A New Model for Trusted Data Exchange

Data spaces do not move data to where it is needed. They move trust.

What a Data Space Is

A data space is a dynamic, federated, decentralized data infrastructure in which participants share data insights — not data copies — governed by machine-readable policies they define and control. Unlike a data lake, which aggregates data in a shared repository, a data space leaves data physically where it belongs — with its original owner. What travels across the network is not the data itself, but a policy-governed response to a specific, authorized query.

Think of it like an automated airport e-gate. You step up and tap your digital pass. The gate scans the code, receives a simple binary signal — Valid Ticket & Cleared to Pass — and the doors slide open. The gate never downloads your personal travel history, medical records, or home address. It just verifies the single proof it needs and lets you through.

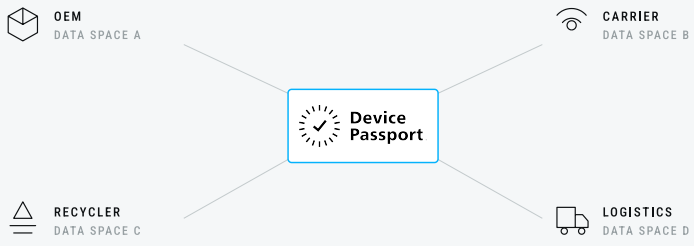
Mechanically, this works by reversing the usual approach. Most data-sharing models move data to a central place where it can be queried. A data space does the opposite: the query travels to the data, gets answered locally, and only the answer travels back.

Core Principles

- **Data Sovereignty:** The data owner retains physical and legal control at all times. Sharing is governed by policy, not trust.
- **Policy-Based Access Control:** Usage rules — who can query, how often, for what purpose, and under what jurisdictional constraints — are enforced mathematically, not contractually.
- **Decentralized Architecture:** There is no central repository to breach. Each participant operates their own data space connector, and interactions are peer-to-peer.
- **Interoperability by Agreement:** Agreed, shared protocols ensure that connectors from different vendors and jurisdictions can communicate reliably.

FIGURE 2 — PARTICIPANTS & THE SHARED OBJECT

A Device Passport only works if multiple parties contribute. The Apkudo Device Passport acts as a secure bridge between independent company data spaces.



How Data Spaces Differ
From Alternatives

DIMENSION	BULK IMEI SHARING (ITU-T Q.5057)	DEVICE PASSPORT DATA SPACE
Data Ownership	Surrendered to central registry	Retained by OEM at all times
Regulator Access	Full dataset visibility	Query-only: single status response
Competitive Risk	Production volumes exposed	Protected through policy-based access controls and cryptographic enforcement
Audit Trail	No record of downstream access	Metadata-only, tamper-evident
Scalability	Bottleneck at central node	Federated, distributed by design
Compliance Posture	Passive and mandated	Active and sovereign

FIGURE 3 — BULK IMEI SHARING METHOD COMPARED TO DATA SPACE FRAMEWORK

Legacy API integrations transfer data payloads and surrender downstream control the moment the transfer completes. Blockchain replicates data across all nodes — a fundamental architectural conflict with data sovereignty and GDPR — and introduces prohibitive latency at the query volumes required for real-time IMEI verification.

> **Data spaces are the only architecture that provides verifiable access control, auditability, and data residency simultaneously.**

Open Standards as Foundation

The IDS Reference Architecture Model (IDS-RAM) defines the roles, components, and interaction patterns for data spaces, in line with ISO/IEC 20151-1: Dataspace concepts and characteristics.

The Dataspace Protocol (DSP) — currently on the path to ISO/IEC 26450: Eclipse Dataspace Protocol (DSP) standardization — is the open-source technical standard that operationalizes key interoperability aspects of the IDS-RAM. It separates the control plane (data catalogs, policy negotiation, and contract enforcement) from the data plane (the actual query response), ensuring that no data transfer occurs before usage rights are cryptographically confirmed.

Where Your Data Lives: Hosting and Deployment

The most common question OEMs ask is the simplest one: *If we join, where does our IMEI data actually go?* The answer is nowhere.

The defining property of a data space is that data stays at its source. In the Device Passport model, your IMEI and device-lifecycle data remain inside the systems that hold it today — your ERP, your MES, your IMEI provisioning database — on the infrastructure you already run, whether that is on-premise or in your own cloud tenancy. Joining the data space does not involve uploading, copying, or migrating data to GSMA, Apkudo, or any shared repository. There is no central database of device records to populate and, therefore, none to breach.

What the data space adds is a single new software component: a connector. The connector stands between your data and the network, and it is the only element that ever communicates with the outside world. It has two parts: a control plane and a data plane.

The control plane handles identity checks, policy negotiation, and contract enforcement — it decides whether a given query is allowed. The data plane executes the approved query against your local data and returns only the permitted answer.

No query reaches your underlying systems until the control plane has cryptographically confirmed the requester's credentials and the governing policy. The data plane never emits anything the policy does not explicitly allow.

Where the connector runs is a deployment decision, not an architectural one. An OEM has two options, and both preserve the guarantees above:

- **Self-hosted.** The OEM deploys and operates the connector inside its own environment, alongside its data. This gives the OEM direct physical custody of both the data and the enforcement point. It requires the OEM to run and maintain the connector software.
- **Operated on the OEM's behalf.** The OEM engages an infrastructure service provider — in this case, Apkudo — to deploy and run a connector that reads from the OEM's systems under the OEM's policies. The data still originates from and is controlled by the OEM; the OEM is simply relieved of the task of running the connector software itself. Apkudo operates the system, yet does not own the data or gain rights to the data flowing through it.

In neither case does the data come to rest anywhere new. This is the architectural inversion at the heart of a data space: instead of moving data to a central place where it can be queried, the query is moved to the data, answered locally, and the answer alone travels back.

The rest of the network is deliberately thin. GSMA operates two components, and neither holds device data.

The trust anchor is the identity and credential infrastructure that lets participants prove who they are. The clearing house keeps the transaction record: that a query happened, who asked, when, and under what policy. It records neither the queried IMEI nor the returned answer.

A federated catalog lets participants discover which data services exist and on what terms, but it holds service descriptions, not the data itself. Every one of these components is designed to carry metadata and trust, never payload.

IN SHORT

Your data stays in your possession. A connector stands between your data and the network, and answers approved questions with a single status. Nothing is ever uploaded to a central database. GSMA and regulators never see the underlying data, and if Apkudo runs your connector, it does so under your policies and gains no rights to the data.

The Device Passport Data Model
A Shared Language

Two connectors from different vendors in different countries must mean the same thing when they say "approved."

The data model is what guarantees that. It is the smallest possible shared vocabulary — precise enough to answer a regulator, narrow enough to expose nothing else.

A data space only works if participants agree not just on how to exchange data (the Dataspace Protocol) but what the data means. The Rulebook's data interoperability building block specifies that shared meaning: a single Device Passport schema that every connector implements identically, so a query from a Brazilian regulator and a query from an Indian regulator are answered using the same definitions.

Without a fixed model, every OEM–regulator pair would negotiate a bespoke format, and the network would collapse into point-to-point integrations — exactly the cost a data space exists to remove.

What Data is Exposed

The Device Passport carries only the fields required to answer the homologation question, each with a defined type and source:

- **IMEI:** the 15-digit identifier under query, used as the lookup key, is never returned in bulk.
- **TAC-linked model identifier:** the device model, derived from the first eight digits of the IMEI and resolved against GSMA's authoritative TAC registry, which anchors the model definition to a source both OEMs and regulators already trust.
- **OEM identity:** the manufacturer, expressed as the participant's verified credential rather than a free-text name, so the claim of authorship is cryptographically backed.
- **Homologation approval status:** a controlled value (approved · pending · rejected · not applicable) scoped to the querying jurisdiction, so the same device can return "approved" for one market and "not applicable" for another.
- **Certification validity (optional):** an expiry or effective date, where a jurisdiction's rules make approval time-bound.

That is the extent of data exposure. By design, all other data held by the OEM is outside the model and has no representation that a query could ever reach:

- Total production volumes for any device model
- Regional or country-level allocation figures
- Commercial pricing or carrier agreement terms
- Manufacturing facility identifiers
- Consumer personally identifiable information (PII)
- Inventory positioning or forward-looking supply chain data

Controlled Vocabularies and Jurisdictional Scoping

Status is chosen from a fixed list, not written as free text. "Approved" is a defined term with the same meaning to every participant, and it is always paired with a jurisdiction identifier from a standard country/market code list. That pairing is what lets a connector answer a jurisdiction-scoped question with exactly one correct answer, and what lets the clearing house record the interaction without ambiguity.

06

Semantics, Provenance, and Versioning

The Rulebook documents exactly what each field means, what values it can hold, and the data source — so each participant's connector builds to the same specification instead of guessing at each other's assumptions.

That last part matters more than it sounds. For every field in a Device Passport, the model states its source: whether it came from the OEM's systems or was resolved against GSMA's TAC registry. A regulator or auditor can trace any answer back to its source. The Data Interoperability building block refers to this as traceability.

Homologation rules change over time, so the schema is built to adapt. If a new jurisdiction joins the network, or a regulator needs a new status value, it can be added under governance — without breaking any connectors already running in production.

> The data model says as little as possible, on purpose. It can state that a device is approved in a market and prove who says so. **It is structurally incapable of expressing anything a competitor would want to know. What makes it safe to share is the same thing that makes it easy to adopt.**

How the Data is Queried

When a regulator needs to verify a device presented at the network edge or at customs, it submits a structured query to the data space: *Is IMEI [X] associated with a device approved for operation in [jurisdiction Y]?*

That single question triggers a fixed sequence, shown in Figure 4:

01 **The regulator submits the query.** The regulator connector sends the structured request into the data space, and the query is automatically routed to the OEM that owns the relevant TAC range.

02 **The OEM's connector checks the requester's credentials.** The control plane confirms that the regulator is who they claim to be, using the verifiable credentials that GSMA issued when the regulator onboarded.

03 **The control plane evaluates the query against policy.** Is this entity authorized to ask this question? Has it exceeded its rate limit? Is the request within an approved time window? If any check fails, the query is rejected before it ever reaches the OEM's data.

04 **Only an approved query reaches the data plane.** The data plane executes the lookup against the OEM's own systems — locally, without the data ever leaving the OEM's environment.

05 **A single answer travels back.** Approved, pending, rejected, or not applicable for that jurisdiction — nothing else.

06 **The clearing house logs that the exchange occurred.** Who asked, when, and under what policy — never the IMEI, never the answer.

The underlying dataset — including all the competitive intelligence it contains — is never exposed and never leaves the OEM's possession. The connector answers the question without revealing how it arrived at the answer.

Where your data lives: the Device Passport query path

Your IMEI data stays put. Only a single answer crosses the boundary.

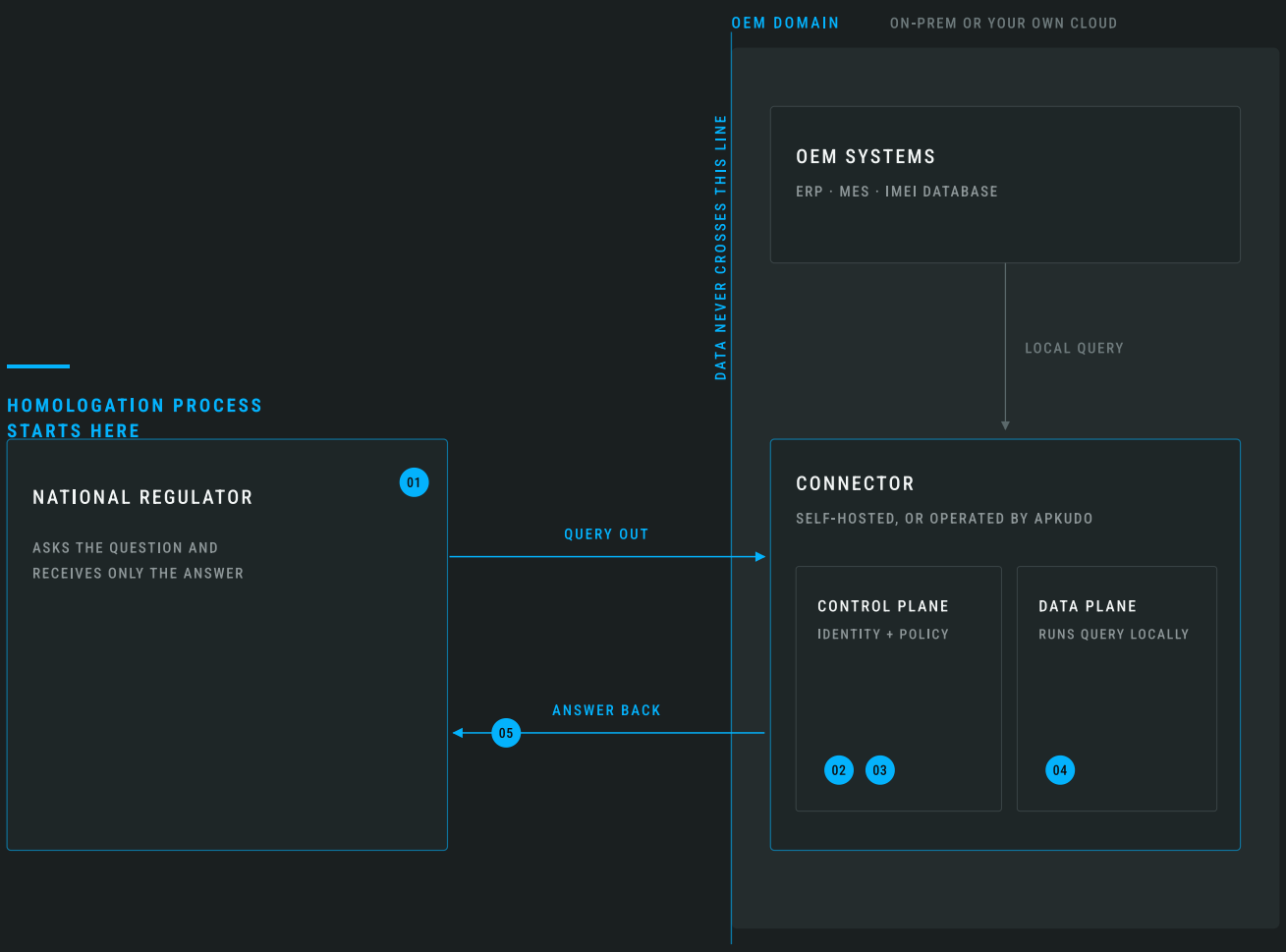


FIGURE 4 The Device Passport query path. Data stays inside the OEM domain; only a single answer and a metadata log cross the boundary.

07

Benefits for OEMs

Participating in the Device Passport framework is a strategic move that protects OEM interests while eliminating the threat that counterfeits pose to brand and revenue.

Brand Protection Without Compromise

Counterfeits damage OEM brands in two ways: by directly harming consumers who believe they are buying genuine products and by triggering regulatory scrutiny. The Device Passport framework allows OEMs to actively support enforcement action against counterfeit devices — by providing regulators with the verification tools they need. **OEMs can fight counterfeiting without surrendering the bulk datasets that create competitive risk.**

Regulatory Confidence and NPI Acceleration

Pre-approved data-sharing agreements within the data space can be established before a new device launches. When regulatory authorities in a target market are already onboarded as credentialed data space participants, the homologation verification process becomes a real-time query rather than a manual review cycle. **This directly compresses NPI timelines and reduces the risk of launch-day inventory disruption.**

Future-Proofing for Digital Product Passports

The EU Ecodesign for Sustainable Products Regulation (ESPR) will require Digital Product Passports (DPPs) for consumer electronics by 2030. The ESPR DPP mandate shares the same architectural requirements as the Device Passport framework: tiered access, data sovereignty, and the separation of publicly accessible sustainability data from restricted compliance documentation. **OEMs that build data space infrastructure for homologation today are simultaneously building the foundation for ESPR compliance — avoiding a parallel investment cycle later.**

Total Sovereignty and Dynamic Control

Under the Device Passport model, OEMs do not simply agree to share data — they define the machine-readable rules that govern every interaction with that data. If a jurisdiction exceeds its query rate limit, the connector automatically enforces the limit. If an OEM needs to modify or revoke sharing rights — due to a policy change, a regulatory dispute, or a market exit — it can do so in real time without relying on a third party. **Control is not delegated. It is retained.**

Policy Enforcement: Rules Baked In, Not Bolted On

The critical distinction between a data space governance model and a conventional data-sharing agreement is how the terms are enforced. Traditional agreements rely on legal contracts and the good faith of counterparties. Data space policies are machine-readable rules — encoded in Open Digital Rights Language (ODRL) — that the connector evaluates and enforces before issuing any response. Compliance is architectural, not behavioral.

This means an OEM does not need to audit whether a regulator is respecting agreed-upon access limits. The connector enforces those limits automatically. **If a query violates policy — the wrong jurisdiction, an exceeded rate limit, or a non-credentialed requester — it is rejected without human intervention.**

Dispute Resolution and Auditability

The clearing house audit log provides the factual foundation for any dispute between participants. Because every query interaction is logged with a cryptographic timestamp and the identity of the requesting party, disputes about unauthorized access or policy violations can be resolved with reference to an immutable record. **The log captures what happened — who queried, when, and under what policy — without storing what was exchanged.**

08

The Homologation Data Space Rulebook

A data space is not defined by its software. It is defined by its Rulebook — the single agreement every participant accepts before they connect. The Rulebook is how "trust" stops being a hope and becomes a set of enforced rules.

Every operational data space is governed by a Rulebook: a structured document adopted by all participants that records the collective decisions about how the data space works — who is allowed to do what, on whose authority, and under which rules.

A homologation-specific Rulebook will adapt an established framework used by other data spaces and organized into the building blocks below. Pilot feedback will inform the official production Rulebook.

Scheme Owner and Oversight: Who Runs the Data Space

The Rulebook names the body that owns the rules, admits participants, and arbitrates disputes. For homologation, this role is fulfilled by GSMA, leveraging its established position as the global administrator of the Type Allocation Code (TAC) and IMEI allocation system. The scheme owner does not touch device data; it governs the rules under which device data is exchanged.

The scheme owner also designates who operates the shared trust and audit components. In this scheme, GSMA runs the clearing house, so the audit record resides with the same entity trusted to administer TAC and IMEI, not with any single OEM or regulator.

Entry records are immutable, meaning append-only and cryptographically tamper-evident: they can be verified but not altered or deleted. This is deliberately not a blockchain — there is no replication of records among participants, which is what prevents sensitive metadata from spreading across the network.

PARTICIPANT ROLES AT A GLANCE

Data Provider (OEMs)

Own and selectively expose Device Passport data via certified connectors. Define all usage policies; retain the right to modify or revoke access.

Identity Provider (GSMA)

Issues and manages cryptographic credentials (X.509 and Verifiable Credentials), anchoring trust to a globally recognized authority.

Clearing House (GSMA)

Maintains the tamper-evident audit log of interactions — metadata only, no payload.

Data Consumer (Regulators / CEIRs)

Query device status through certified interfaces. Access is limited to policy-authorized query types and jurisdictional scope.

Infrastructure Service Provider (Apkudo)

Bridges OEM ERP/MES systems to the DSP-compliant network; normalizes data into Device Passport format; enforces OEM policies in real time.

The Building Blocks

Participation management: how you join

The Rulebook defines onboarding: how an OEM or a regulator applies, how its identity is verified, and how it is issued the credentials that allow it to participate. It also defines connector certification — the requirements a connector must meet (correct DSP behavior, correct policy enforcement) before it is trusted on the network — and the conditions under which a participant can be suspended or removed.

Legal and regulatory framework

The Rulebook sets the contractual baseline that every participant signs and demonstrates how the data space complies with the laws that govern it: GDPR, where any personal data is involved; the EU Data Act on access and portability; and the homologation obligations of each participating jurisdiction.

Critically, because the Device Passport exposes only approval status and never bulk production data or PII, the Rulebook can make the compliance posture explicit rather than leaving each OEM's legal team to reason about it alone.

Identity and trust framework

The Rulebook specifies how trust is established: GSMA issues the credentials that anchor every participant's identity, and the trust framework defines how those credentials are validated, rotated, and revoked. This is where *Where is it hosted?* meets *Who do I trust?* The trust anchor is hosted by GSMA; the data is not.

Access and usage policy: the enforced rules

This is the heart of the Rulebook for an OEM. It defines the machine-readable ODRL policies that every connector enforces: which query types are permitted, which jurisdictions may ask, rate limits, time-bound access windows, and purpose constraints.

These are not contractual promises to be audited after the fact — they are evaluated by the connector before any response is issued. The Rulebook is where the OEM's sovereignty becomes concrete: **the OEM defines these rules, and can revoke or amend them in real time.**

This also settles dispute resolution. Because every query is logged by the clearing house with a cryptographic timestamp and the requester's identity, disputes about unauthorized access or policy violations are resolved against an immutable record of what happened — who queried what, when, and under which policy — without that record ever storing the data that was exchanged.

Data interoperability: the shared language

The Rulebook defines the Device Passport data model — the visible fields, their semantics, and their linkage to GSMA's TAC system. It also mandates the Dataspace Protocol as the exchange standard, so connectors built by different vendors can communicate with each other. Without a common model and protocol, every OEM and regulator pair would need its own custom integration. With them, a participant onboards once and can exchange with everyone.

09

A Call to Action
Industry Must Lead

The technology is production-ready. What remains is the industry decision and framework to shape one solution before a patchwork of market-by-market approaches makes that harder to do.

The Default Outcome Is Not Neutral

The choice is not between regulation and no regulation — it is between one framework and many. Regulators are solving a real problem, and without an industry-led solution, they will each solve it their own way: different data, different formats, and different rules for each jurisdiction.

For an OEM operating in hundreds of countries and territories, that fragmentation is a far larger operational burden than any single mandate — and it's the outcome a coordinated data space is designed to prevent.

> **The window to shape this outcome is open now. It will not remain open indefinitely.**

Why GSMA Is the Right Leader

GSMA administers the Type Allocation Code (TAC) system — the foundation of every IMEI ever issued. It has the trust of both OEMs and national regulators across more than 220 countries and territories. No other organization can anchor the cryptographic identity infrastructure of a global device homologation data space with comparable legitimacy and neutrality.

A GSMA-convened Device Homologation Data Space is not a new system competing with existing regulatory frameworks. It is an upgrade to the verification layer that regulators already rely on — delivering the same assurance they seek from bulk IMEI sharing, through an architecture OEMs can accept.

Apkudo: The Operational Bridge

OEMs already hold the data a homologation data space needs. It sits in ERP platforms, MES records, and IMEI provisioning workflows, but in formats those systems were built for rather than for external exchange. What OEMs lack is a DSP-compliant connector that speaks the protocol required to participate in the data space. Apkudo closes that gap.

As a trusted connector, Apkudo reads device lifecycle data from OEMs' existing systems, normalizes what it finds into the Device Passport format, enforces OEM-defined usage policies in real time, and manages credential and query interactions with national regulators. OEMs participate in the data space without rebuilding their internal infrastructure.

Three Steps for OEMs

- **Endorse the principle.** Publicly support privacy-preserving homologation as the industry standard. This signals to regulators that a credible alternative to bulk sharing exists and is backed by manufacturers.
- **Participate in the pilot.** Validate the Device Passport architecture with real IMEI data in a controlled pilot environment. The pilot is designed to demonstrate the full query lifecycle — from regulator request to OEM connector response — under production-realistic conditions.
- **Prepare for what's next.** The pilot is the first step. It leads into a live test data space and, ultimately, an operational program. OEMs that engage now help shape the Rulebook and credential standards that will govern every stage of that path.

10

Conclusion and Next Steps

THE CASE FOR EARLY PARTICIPATION

> The Device Passport Homologation framework is being defined now. OEMs that participate will shape what the model requires, how policies are enforced, and what stays confidential. OEMs that do not will inherit and implement whatever the participants decide.

The trust deficit between OEMs and regulators in global device homologation is real, consequential, and solvable. The architecture exists, and the standards behind it are advancing toward formal status. Catena-X, the automotive industry's data space, demonstrates that federated, sovereign data exchange works reliably at scale across complex, multi-stakeholder environments.

What the telecommunications industry now requires is the institutional will to act. GSMA convenes, because it is the only body both OEMs and regulators already trust. Apkudo has the connector infrastructure to make participation practical for OEMs. The Dataspace Protocol provides the interoperability layer that connects participants.

The Device Passport framework does not ask OEMs to choose between complying with regulators and protecting their commercial interests. It is designed explicitly to do both — regulators get verification they can cryptographically confirm, and OEMs disclose only a status, a market, and a signature, because the data model lacks a field for anything else.

This paper is intended as a contribution to ongoing industry collaboration and is expected to evolve with input from GSMA and industry stakeholders.

Immediate Next Steps

- **For OEMs:** Contact GSMA or Apkudo to discuss pilot participation. Pilot onboarding is designed to integrate with existing IMEI provisioning workflows and minimal infrastructure change.
- **For Regulators:** Engage GSMA on the data space credentialing framework. Regulator onboarding requires establishing verifiable credentials within the GSMA identity infrastructure.
- **For the Industry:** The GSMA Device Homologation solution is the venue for shaping governance policy, technical standards, and the dispute resolution framework. Participation is open to OEMs, operators, and national regulatory authorities.

APPENDIX A

Glossary of Key Terms

Catalog	The federated directory where participants publish and discover available data services and the terms attached to them. Holds service descriptions, not data.
CEIR	Central Equipment Identity Register. A national database used by regulators to track and verify device IMEIs.
Clearing House	The component that records an immutable, metadata-only log of each query interaction — who, when, under which policy — without storing the IMEI or the response.
Connector	The software component that fronts a participant's data. Its control plane negotiates policy and identity; its data plane executes approved queries locally.
Data Space	A federated data infrastructure enabling sovereign, policy-governed data exchange without centralizing data in a shared repository.
Device Passport	A policy-governed data object containing minimal device identity and homologation status, queryable via data space connector.
DSP	Dataspace Protocol. Open-source standard for policy-governed data space interactions. Draft International Standard ISO/IEC DIS 26450 candidate. Governance of DSP sits with the Eclipse Dataspace Working Group as of DSP 2025-1.
DID	Decentralized Identifier. A cryptographic identifier enabling verifiable, self-sovereign digital identity without a central registry.
Homologation	The formal regulatory process confirming a device meets national technical and safety standards for market entry.
IDSA	International Data Spaces Association. The body that developed the IDS Reference Architecture Model (IDS-RAM).
IDS-RAM	IDS Reference Architecture Model (IDS-RAM). Defines roles, components, and principles for data spaces.
IMEI	International Mobile Equipment Identity. A unique 15-digit identifier assigned to every mobile device.
ODRL	Open Digital Rights Language. A machine-readable policy language used to define and enforce data usage rules within data spaces.
Rulebook	The structured agreement, adopted by all participants, that records the business, governance, legal, and technical decisions governing a data space.
TAC	Type Allocation Code. The first eight digits of an IMEI that identify the device model and manufacturer. Administered by GSMA.
VC	Verifiable Credential. A cryptographically signed digital credential used to authenticate participant identity within a data space.

APPENDIX B

Standards and Regulatory References

- ITU-T Q.5057: Proposed global IMEI registry mandate and bulk sharing framework.
- IDS-RAM: IDS Reference Architecture Model (IDS-RAM). Defines roles, components, and principles for data spaces.
- Dataspace Protocol (DSP): Open-source standard for policy-governed data space interactions. Draft International Standard ISO/IEC DIS 26450 candidate.
- ISO/IEC FDIS 20151-1 *Cloud computing and distributed platforms — Dataspaces Part 1: Concepts and characteristics:* International Standard describing the key aspects of Data spaces.
- IDSA Rulebook: Governance framework covering functional, technical, operational, and legal requirements for data spaces.
- EU Data Act (2025): European legislation governing data access, portability, and sovereignty.
- EU ESPR / Digital Product Passport: Ecodesign for Sustainable Products Regulation mandating DPPs for consumer electronics by 2030.
- GSMA TAC Global Decimal Administrator (GDA): GSMA's existing authority over Type Allocation Codes and the IMEI assignment system.

apkudo

ABOUT APKUDO

Apkudo is the Device Passport Platform for the connected device ecosystem. We capture and unify data from every program, transaction, and touchpoint across the device lifecycle, creating a single, trusted Device Passport™ for every asset. For companies that manage, sell, or buy devices, this means a verified record they can act on: restore buyer confidence, maximize value, and reduce risk at every decision point. Our unique advantage is data fidelity and veracity, built on precision-automated robotics that have processed millions of devices, generating objective, machine-verified data that no competitor can match. To learn more, visit apkudo.com.

GSMA

ABOUT GSMA AND GSMA FOUNDRY

The GSMA is a global organization unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

The GSMA Foundry is the Home of Mobile Innovation. We're the go-to hub for cross-industry collaboration and business development, where GSMA members rapidly develop real-world solutions, nurture new ideas, and scale proven solutions globally to shape our digital future.

INTERNATIONAL DATA SPACES ASSOCIATION

ABOUT IDSA

The International Data Spaces Association (IDSA) is on a mission to create the future of the global, digital economy. Its 180+ member companies and institutions have created the International Data Spaces (IDS) standard: a secure system of sovereign and trusted data sharing in which all participants can realize the full value of their data. IDS enables new smart services and innovative business processes to work across companies and industries, while ensuring that the control of data remains in the hands of data providers. We call this data sovereignty.

apkudo