



Device Homologation Pilot FAQ

The FAQ is designed to answer common questions you may have as you evaluate participation in the GSMA Homologation pilot program. Please review the information provided. If you have further questions, please contact Paresh Modi, Senior Director, Partnerships, at +44 (0)7771 730630 or paresh.modi@gsma.com.

How the pilot works: You'll use a simplified, guided interface with real device data, real IMEIs checked against real records. No IT integration, data space setup, or technical work is required on your end. Your role is to use the interface and share feedback.

What is the purpose of this pilot?

This pilot tests a secure, permissioned way for OEMs to share that data directly with regulators, starting with device-level attestation using IMEI and related identifiers. OEMs stay in control throughout: only the specific attributes needed for homologation are shared, and no commercially sensitive data is exposed.

What is the core pilot use case?

The core pilot use case is a simulated digital ID check for hardware to confirm if a specific IMEI was manufactured.

Who is expected to participate in the pilot?

The pilot brings together the two sides of a real homologation decision: OEMs providing device data and regulators making approval decisions. We're targeting 2 to 3 OEMs and 10 to 15 regulators — enough to test the workflow across multiple markets and device types, without the complexity of a full production rollout.

The pilot runs on a short timeline, roughly 8 to 10 weeks from kickoff through testing. This keeps the commitment bounded and low-risk for participants.

Each OEM or regulator can enroll multiple team members, so the right people can be involved without creating a bottleneck around a single point of contact.

What are the expectations of pilot participants?

Pilot participation is minimal. You will be invited to a kickoff/onboarding call, which includes a walkthrough of the Homologation Program app. Pilot participants will evaluate the application's

user interface, the ability to set up and configure user access and permissions, and the audit logs.

You will receive a brief survey to share your feedback and experience. We'd like to understand both positive and negative experiences with sharing and accessing data. Your feedback will influence broader program rollout across OEMs and regulators worldwide.

A final feedback session will be scheduled. You will receive a recap of the pilot feedback. Ad hoc communication channels will be established.

How many devices are needed to participate in the pilot?

Participation requires only ten (10) real devices. This is an intentional design choice. The pilot is focused on validating the data-sharing framework and workflow, not on volume. Ten devices are sufficient to demonstrate the process end-to-end, and we've deliberately kept the bar low to make pilot onboarding as simple as possible.

Devices can come from existing test inventory, warehouse stock, or devices already in use for internal testing. No new procurement is required.

Only the device identity attributes needed for homologation attestation (such as IMEI/TAC and serial number) will be accessed. No commercially sensitive product, supply chain, or manufacturing data will be requested or exposed.

What data is required from OEMs?

The core requirement from OEMs for this pilot is simply to confirm whether a specific IMEI was manufactured. The pilot will not ask OEMs to provide TAC, make, or model information, as GSMA already possesses this data within its existing TAC database.

What identifiers are supported?

The primary identifier for this pilot is the IMEI. To reduce unnecessary queries, a Luhn check will be used as a preliminary step to validate the IMEI format before any OEM request is made.

OEMs will have the option to share additional identifiers attached to the IMEI. While the Apkudo platform can support other identifiers like serial numbers, eUICC IDs (EID), and MEID/ESN, the pilot will **strictly focus on the IMEI** to ensure simplicity.

How can OEMs provide data?

Suggested method for pilot simplicity.

- Submit via CSV, PDF, XLSX, or similar. Files will be submitted via secure SFTP or secure email.

- If data is shared via SFTP, OEM-specific access permissions will be configured for that OEM.

How will regulators access data?

Regulators will query the system using an IMEI and receive a highly controlled response. The response will specifically focus on confirming whether the device was manufactured. The pilot response will not include make-and-model visual validation, as regulators can already access that information by subscribing to the GSMA TAC database.

Example response:

- Valid TAC (Yes or No)
- Manufactured (Yes or No)
- Shipped (Yes or No)

What is the benefit of OEM participation?

Without a shared standard, OEMs face a growing patchwork of regulatory demands, different rules, and different data requests, market by market. **Participating now gives OEMs a seat at the table in defining the alternative: one standardized, OEM-controlled way to share device data with regulators**, rather than many.

Early participants also shape how that standard works, rather than adapting to a version built without their input.

What is the benefit of Regulator participation?

Participating in the pilot gives regulators early access to a standardized way to query OEM device data directly. Early participants also help shape how the standard query-and-response process works, rather than adopting a system built without regulatory input.

Does my participation in the pilot commit my organization to post-pilot production?

No. The pilot is a time-bound test of the workflow, not a procurement process or a commitment to any production service. GSMA's own pilot terms are explicit on this: participation creates no obligation to proceed further. [GSMA Terms of Reference](#).

About this section: Everything below describes the data spaces framework and governance model on which this pilot is built, as well as the production version of this system. It's included for participants who want to understand the technology, not as a list of things you need to set up. Nothing here requires action from you during the pilot.

Technical Context Informing the Pilot

What is a data space?

A data space refers to a controlled data-sharing environment where:

- OEMs remain the data owners
- Access is permissioned and purpose-bound
- Data is not replicated or broadly exposed
- Queries return limited, governed responses

This is implemented using Apkudo's policy-based access control (PBAC) model. Learn more in this [data spaces framework PDF](#).

Will regulators see full OEM datasets?

No, regulators will not see full OEM datasets. The system is intentionally designed for controlled disclosure, meaning regulators receive only the necessary outputs required for validation, ensuring that underlying OEM datasets are never exposed.

How is access controlled?

Access is strictly governed through Policy-Based Access Control (PBAC), which utilizes role-based permissions and purpose-bound data access. OEMs have complete authority to define who can access their data, exactly what data is accessible, and under what specific conditions. **The pilot simulation provides access to this functionality.**

Is data access logged?

Yes, all data access is immutably logged. Audit logs are generated at the device, query, and user/account levels. These logs record the requesting entity, timestamp, query type, and the result status of every interaction. **The pilot simulation provides access to this functionality.**

Can OEMs revoke access?

Yes, OEMs retain full control over their data sharing at all times. They have the ability to revoke access at any point and can dynamically modify their sharing policies as needed. **The pilot simulation provides access to this functionality.**

How is data secured?

The platform utilizes robust security measures, including tenant isolation, encrypted data transfers, and role-based access control. Furthermore, the platform is fully GDPR-compliant for data handling and maintains SOC 2 Type 2 compliance.