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, and if you still have further questions, please contact Paresh Modi, Senior Director, Partnerships, +44 (0)7771 730630, paresh.modi@gsma.com.

What is the purpose of this pilot?

GSMA seeks to address the ongoing challenge of device attestation for regulatory homologation and compliance activities by leveraging new technological capabilities. This pilot validates a production-ready approach for enabling regulators to access OEM-provided device data in a secure, permissioned manner to support homologation and compliance workflows. The focus is on device-level attestation using IMEI and/or related identifiers, without requiring OEMs to expose commercially sensitive data.

What is the core pilot use case?

The core pilot use case is a digital ID check for hardware to confirm if a specific IMEI was manufactured. It will utilize the GSMA TAC database for initial validation before querying the OEM to confirm if a device was manufactured with that specific identifier.

What is the expected pilot scale?

The pilot is intended to test and confirm the ability to access and share data between a small, targeted group. We anticipate involving a minimum of two to three OEMs and 20-30 regulators. The pilot will utilize a limited dataset and will run on a short timeframe of approximately 8 to 10 weeks from the kickoff date through the testing phase.

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 are the expectations of pilot participants?

A successful pilot demands a constant feedback loop. 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 30-minute weekly feedback session will be scheduled as well as ad hoc communication channels will be established.

Additional technical expectations and requirements are included in the FAQ.

Technical FAQ

What is a data space in this context?

In this pilot, a data space refers to a controlled data sharing environment where:

- OEMs remain 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.

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 their existing TAC database. We are also not requesting intended market or country applicability, as devices frequently move across borders.

What data is not required?

To reduce friction, the pilot does not require any commercially sensitive data. This includes production volumes, regional allocation data, pricing, full lifecycle history, or any consumer Personally Identifiable Information (PII). Additionally, lost and stolen data status is excluded from this pilot, as GSMA already operates a separate API for that service.

What identifiers are supported?

The primary identifier for this pilot is the IMEI. To reduce noise, a Luhn check will be utilized as a preliminary step to validate the format of the IMEI 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 and maximize OEM participation.

How can OEMs provide data?

Supported ingestion methods - all production

- API integration
- SFTP / batch upload
- File-based submission (for pilot simplicity)

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)

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

Is data access logged?

Yes, all data access is immutably logged. Audit logs are generated at the device level, query level, and user/account level. These logs record the requesting entity, timestamp, query type, and the result status of every interaction.

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.

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 handling data and maintains SOC 2 Type 2 compliance.

Does this require new development?

No, the pilot does not require new development. It leverages Apkudo's existing Device Passport production capabilities, which currently manage data sharing for numerous OEMs across other device passport use cases. Homologation is a newly defined program within this existing infrastructure, and the pilot is designed to test and validate the specific configuration requirements.