GSMA Services Showcase LIVE

How new device status attributes will further support best in class device verification techniques

Jason Smith, GSMA Senior Director

GSMA

GSMA Device Registry Ecosystem

Contributors

Insurer

Retailer

Distributor

OEM

MVNO

Network Operator Access

Device Status Exchange

- **120+** Mobile Network Operators
- **42** countries
- help protect **1+ billion** users

GSMA Device Registry

Safer Device handling

GSMA Device Check™

- Trade / recycle / repair / insure
- **250+** organisations
- **50+** countries
- **100+ million** devices queried per year

Block List
- Lost or stolen
- Broken or faulty
- Fraudulently obtained
- Court ordered blocking

New List (September 2023)
Inventory
Financial encumbrance

GSMA

GSMA Device Registry

Be part of the collective fight against device crime. Flag fraudulent and stolen devices.

Why choose this service?

Flagging devices makes them less valuable for resale

Reduce financial losses from device crime and fraud

Prevent lost and stolen devices from reentering your supply chain

Deter criminals by making theft and fraud less rewarding

Why customers use GSMA Device Registry

Operators
- Sharing flagged devices helps protect your customers and your business against loss
- Acting on other operators' data is a deterrent to criminals

Recyclers and Repairers
- Protect brand reputation by either reporting irreparably damaged devices, stopping them from re-entering the supply chain
- Identifying reported stolen /fraudulent devices before they enter the recycling stream

Insurers
- Reduce fraudulent claims by alerting claimants that their device will be on the global registry
- Registering ownership increases the likelihood that your property will be returned

Distributors
- Devices stolen from storage facilities or in transit can be immediately flagged
- Reduces the value of stolen devices and deters criminals
- Law enforcement and customs & excise agencies can check flagged devices

GSMA™

GSMA Device Check™

Remove risk of handling stolen or fraudulent devices, by checking a device's status

Why choose this service?

Identify and eliminate compromised devices from sale or use

Confirms device model to help calculate its correct value

Trusted by retailers, repair shops, insurers and LEAs

Why use GSMA Device Check?

Insurers
- Confirmation if a device has been reported to the operator as lost or stolen
- Confirmation of exact device type for accurate replacement value and claims
- Most authoritative and up-to-date device data to support new policy issuance
- Check the reported lost/stolen status of devices being used as replacements

Law Enforcement
- Discourages mobile device theft by reducing the value of the device
- Confirm the status of any found or turned-in devices
- Gather evidence, e.g. identify where the sale of a stolen device was attempted
- Device model characteristics for identification

Device Recyclers
- Identify and eliminate devices before they enter your recycling stream
- Protect your reputation
- Confirm device model for authenticity and to calculate the value of its parts

Retailers / Pawn Brokers
- Identify and eliminate devices before they are accepted into the reselling stream
- Protect your reputation
- Confirm device model for authenticity and to calculate its value

GSMA™

eSIM Devices

Background

- eSIMs are used to easily, remotely obtain service from MNOs
- The eSIM Subscription Manager Data Preparation (SM-DP+) is a platform for storing and helps to deliver and install digital MNO eSIM profiles to the secure element within the mobile device (eUICC)
- Each eUICC has a unique 32-digit identifier (EID)
- GSMA Intelligence forecast that by the end of 2025, there will be 2.4 billion eSIM smartphone connections globally, representing 1/3 of all smartphone connections.

Problems

- With eSIM simplicity comes a new attack vector for bad actors
- eSIM Fraud: account takeover and subscription fraud variants that exploit weaknesses in eSIM provisioning and portability processes within MNOs
- Formally captured in FF.21 Fraud Manual and CR1010 *Add eSIM Fraud section*
- MNO blocking of a device engaged in eSIM Fraud
- The device IMEI is not always accessible; estimated at 50% or less of all SM-DP+ interactions requesting a subscription profile

Solution

- EID uniquely identifies a device in use by a bad actor to commit eSIM Fraud
- Victim MNO blocks the EID to prevent any further eSIM downloads to the eSIM enabled-device
- GSMA established a database so that victim MNOs can report the EID used to commit eSIM Fraud
- Others query the GSMA database and use the information to also help avoid losses
- A global EID Fraud List to deter fraud, reduce losses, and support investigations

Example Device Check History

Status at Point in Time

Date	List	Action	Reason	Organisation Name	Country	B List Status	G List Status
06/01/2022 10:00	General	Insert	Inventory	Device Distributor XYZ	Country 1	No	Yes
09/15/2022 14:00	General	Remove	Inventory	Device Distributor XYZ	Country 1	No	No
09/16/2022 01:00		Device Checked		Government XYZ	Country 2	No	No
10/01/2022 10:00	General	Insert	Inventory	Device Seller 1	Country 2	No	Yes
11/01/2022 15:00	General	Remove	Inventory	Device Seller 1	Country 2	No	No
11/01/2022 15:30		Device Checked		Device Insurer 1	Country 2	No	No
11/01/2022 15:45	General	Insert	Financial encumbrance	Device Insurer 1	Country 2	No	Yes
03/01/2023 02:00	Block	Insert	Lost or stolen	Operator (CNO) XYZ	Country 2	Yes	Yes
03/02/2023 10:00	Block	Insert	Lost or stolen	Device Insurer 1	Country 2	Yes	Yes
03/03/2023 11:00		Device Checked		Police Agency 1	Country 2	Yes	Yes
05/01/2023 02:00	Block	Remove	Found	Operator (CNO) XYZ	Country 2	Yes	Yes
05/15/2023 10:00		Device Checked		Device Insurer 2	Country 3	Yes	Yes
05/15/2023 11:00		Device Checked		Police Agency 2	Country 3	Yes	Yes
05/25/2023 15:00	Block	Remove	Found	Device Insurer 1	Country 2	No	Yes
05/25/2023 15:01	General	Insert	Inventory	Device Insurer 1	Country 2	No	Yes

Expanding Role in Device Lifecycle