Combatting device crime together – best practice to combat mobile device theft

Presented by

James Moran, Head of Security, GSMA

jmoran@gsma.com

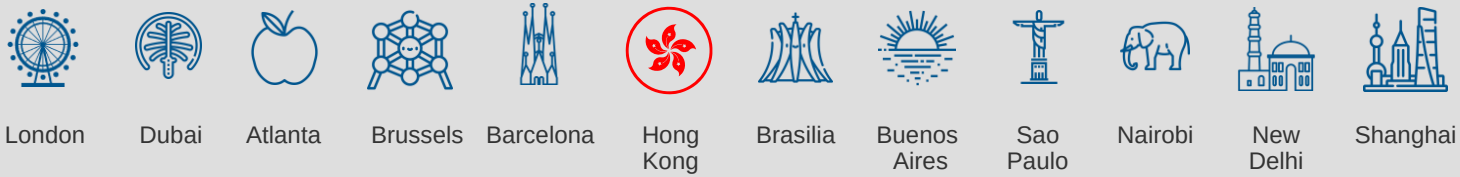
23 July 2018, ITU Workshop

Geneva, Switzerland

GSMA Overview

The GSMA was founded in **1987**

12 Offices worldwide:



The GSMA represents the interests of mobile operators worldwide

Uniting nearly **800** **mobile operators**

With **300+** **companies** in the broader mobile ecosystem

GSMA events, attract over **200,000+** **delegates** from across the global annually

The GSMA works to deliver a regulatory environment that creates value for consumers by engaging regularly with:

Connecting **24,000+** industry Experts

Exclusively for GSMA Members, InfoCentre[2] is your place to connect with a global community of industry experts

GSMA Working Groups provide frameworks and standards in commercial, operational and technical matters that help maintain and advance mobile industry ecosystems

Eight billion+ Mobile connections worldwide

Device crime and theft

Counterfeit Devices

Manufacturer loss $

Poor performance

Safety concerns

No warrantee

Illegal Import

Government

taxation loss $

Un-level playing field for legitimate device providers

Device Theft

Consumer loss $

Personal injury

Buying stolen goods

Insurance claims

Insurance fraud

Subscription Fraud

Operator loss $

Device theft impacts

Consumers

- Risk of harm during the theft
- Loss of valuable devices
- Loss of personal information

Insurers

- Increased underwriting costs
- Title to stolen goods may be transferred

Governments

- Increased crime levels
- Loss of tax revenues

Law enforcement

- Supporting organised crime
- Drain on resources

Traders

- Unknowingly buy stolen goods
- Network performance issues

Operators

- Increased churn, subsidy loss
- Insurance underwriting costs

Stakeholder Matrix

	Operator	Device Manufacturer	Government	Law/Customs Enforcement	Notes
Block Stolen Devices on Mobile Networks	X				The deployment of EIRs by MNOs is fundamental and MNOs should be willing to block devices lost or stolen
Share Stolen Handset Data Between MNOs	X				Operators should agree to collectively share data via GSMA's IMEI Database and block those devices
Globalise Data Sharing	X		X		Operators should take all IMEID data and govts should not promote national isolated data sharing solutions
Implement IMEI Securely	X	X			OEMs must comply with GSMA's IMEI security requirements and operators should only buy compliant devices
Criminalise IMEI Reprogramming			X		Nation states should implement statutory provisions to outlaw IMEI changing or ensure existing legislation is adequate
Enforcement Action against Offenders			X	X	Law enforcement and courts should use laws at their disposal to prosecute IMEI changers and handset thieves
Device Based Anti-Theft Features	X	X			Kill switch type features to locate, lock, wipe and disable missing devices can complement mobile network blocking
Feature and Support Blocking		X			App store owners, and manufacturers that have their own, should block all IMDB listed devices from their app stores
Secondary Market Monitoring			X	X	Require parties dealing in used mobile phones to check if devices have been stolen before change for cash
Black Market Disruption			X	X	Govts could reduce the black market potential by reducing duties and taxes on legitimate devices and by policing imports
Theft Level Monitoring			X	X	The production of proper theft statistics is essential to understanding the effectiveness of measures taken
Customer Education of Safe Use of Mobile	X	X	X	X	Customer education initiatives should advise on how to guard against theft and what to do if it happens

Essential enablers to combat device theft

Device Based Protection

- Delete contacts, photos, mobile payments
- “Factory Reset”
- Remote Wipe

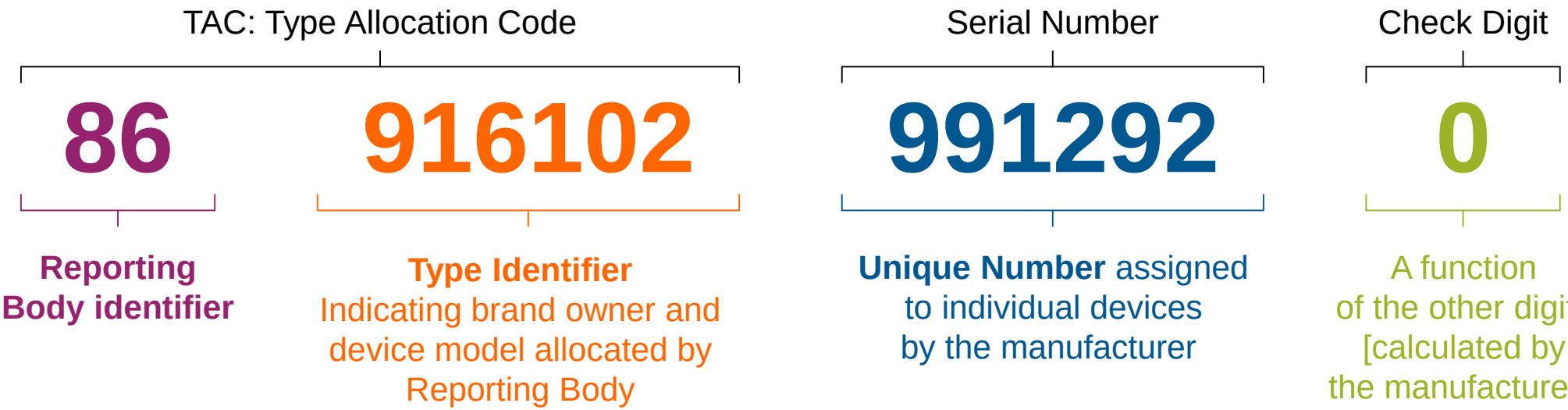
Network Based Protection

- Blocking stolen phone from accessing the network again

Device status checking

- Check device status before recycling
- Stop profiting on stolen phones

What is an IMEI?

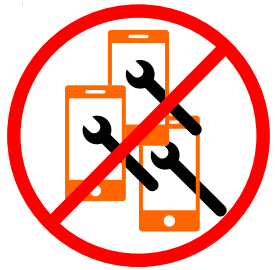


Purpose and use of IMEI defined in 3GPP TS 22.016

"Unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer."

"*The IMEI shall be unique and shall not be changed after the ME's final production process*."

IMEI security technical design principles



GSMA has defined technical security requirements to;

- help manufacturers develop a comprehensive security architecture to protect the IMEI against all known attacks
- Provide operators and other stakeholders with criteria against which device security levels can be assessed and benchmarked

1: Software Integrity

Detect, prohibit and record attempts to alter data or software

2: No Modification

Protect component code against manipulation

3: No Cloning

Prevent IMEI copying between different devices

4: No External Access

Make IMEI implementation inaccessible from outside the device

5: No fallback

Stop unauthorised reversion to old software versions

6: No tampering

Prevent, detect and respond to attempts to change IMEIs

7: Software Quality

Develop software in accordance with best process & techniques

8: No Hidden Menus

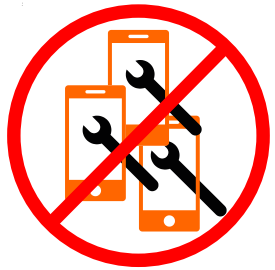
No means to access or modify areas that store the IMEI

9: No Substitution

Prevent substitution of components that contain memory

IMEIs must not change after device production.
Adopt these security requirements.

IMEI security monitoring



The GSMA is now actively monitoring IMEI hacking tools

The GSMA test hacking tools on target devices

Test Lab

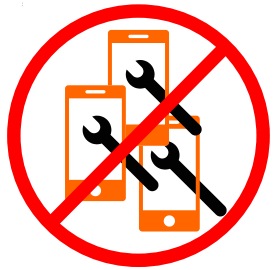
Member states may report weakness to the GSMA and we will seek remedy with manufacturers

Weaknesses are reported to the manufacturer for remedy

Manufacturer

Improved devices re-tested to verify fix

IMEI security monitoring services



Detection of IMEI Security Compromise Claims

Identify and qualify claims of IMEI compromise and availability of hacking tools and provide to GSMA monthly reports and statistics on affected devices and manufacturers.

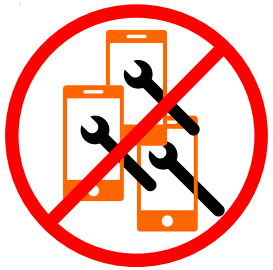
Validation of IMEI Security Compromise Claims

GSMA's IMEI Security Interest Group (ISIG) reviews the monthly reports and selects devices and hacking tools that the service provider obtains and then observes and documents hacking performance.

Evaluation of Corrective Measures

Device manufacturers may propose technical measures to remediate reported security breaches and GSMA can assess their effectiveness by using hacking tools against fixed devices.

IMEI security reporting and correction process



GSMA has defined a process to which manufacturers centrally contract to;

- Receive and refer reports of compromised IMEI implementations
- Assess and investigate reports received
- Fix issues and provide correction dates to GSMA within 42 days

Operators

Government & regulators

- Log and assess reports
- Refers reports to OEMs
- Log results
- Notify stakeholders

Manufacturers

- Acknowledge report
- Technically assess
- Respond to GSMA
- Fix reported issue

Device blocking

Handset stolen from user

User reports device theft to their operator who flags the device's IMEI on their own local blacklist

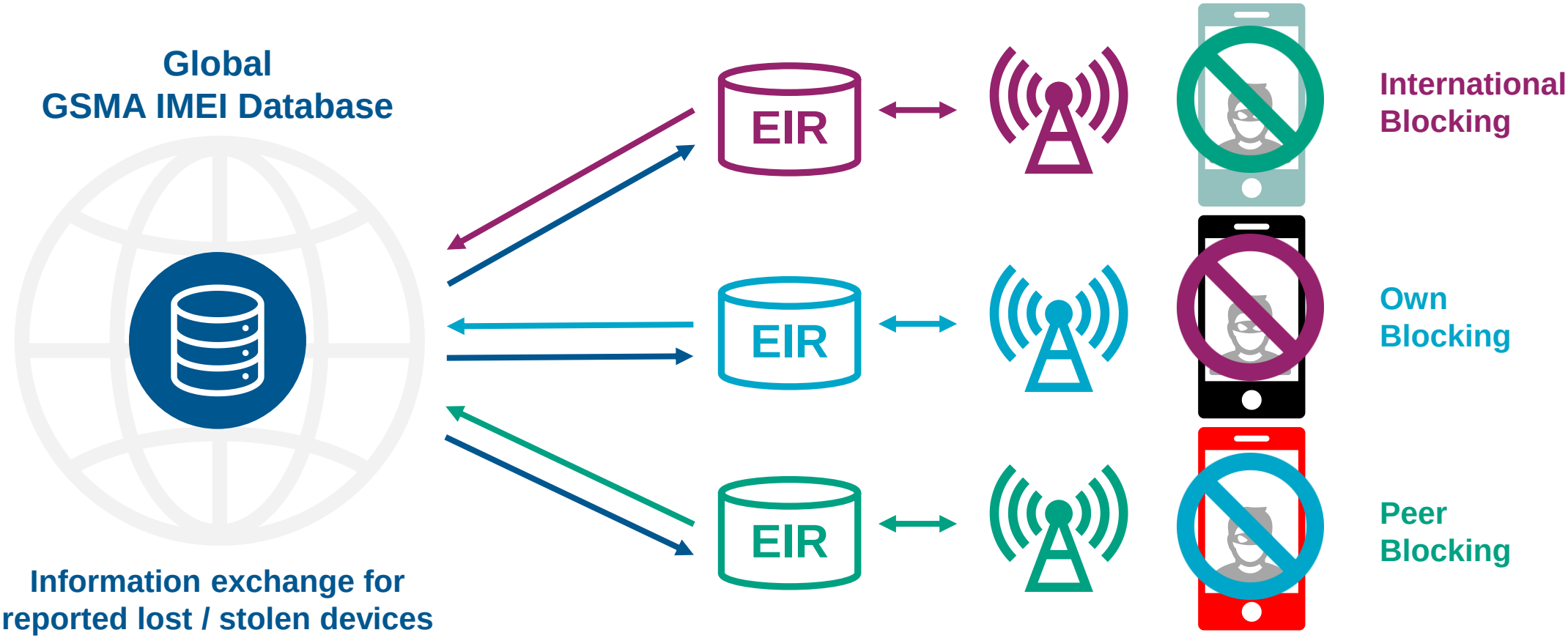
Operator uploads their own IMEI blacklist to the GSMA IMEI database

Other contributing operators download the GSMA Black List

Stolen devices cannot be used as typically blocked by all operators, at a national and international level

Stolen device data sharing

Global
GSMA IMEI Database



Information exchange for reported lost / stolen devices

EIR = Equipment Identity Register

Device based anti-theft solutions

Consumer Enabled Capability to track, lock and wipe stolen devices

GSMA defined requirements

- Render the device inoperable
- Prevent reactivation of the device
- Wipe user data
- Wiping and disabling must be reversible
- Withstand hard reset
- All devices sold in some markets must support these features

Device based solutions disable devices regardless of access technology and help protect consumer content

Device Check services

- Helps identify and eliminate stolen devices before they can enter supply chains
- Used by resellers / traders / recyclers / insurers / law enforcement agencies
- Helps to further discourage device theft by reducing the value of a stolen devices

GSMA supports range of enablers

TAC Allocations

Device type identity numbers (Whitelist)

Device Database

Catalogue of global devices by TAC code

Device Blacklisting

Exchange stolen device IMEIs between operators for blocking

Device Check

Reported stolen phone look up service by IMEI

IMEI = International Mobile Equipment Identity | TAC = Type Allocation Code

Device theft prevention requires cooperation

Multi-stakeholder involvement

Users can report stolen devices to their network operators, enable anti-theft features on their devices and, in countries where operators are connected to the GSMA IMEI Operator Blacklist users can be encourage to check the IMEI status of used devices they plan to buy

Mobile network operators can block stolen devices from their networks, connect to GSMA IMEI Operator Blacklist to share and collect blacklist data and encourage their device suppliers to adequately protect the integrity of the IMEI implementations in their products

Device manufacturers / brand owners can ensure the integrity of the IMEI in all their products, design more secure devices (i.e. make it impossible to reprogram IMEIs) and implement kill switch functionality to allow users to remotely disable lost and stolen devices

App store operators can obtain the IMEIs of stolen devices from GSMA and use those to deny app store access to devices that have been reported stolen

Where we are

- No silver bullet solution – goal is to make theft economically unattractive
- Device theft is a global problem that requires cross border alignment and action
- Industry initiatives have had a positive, but limited, impact
- Activities to date have been based on global non-proprietary standards
- Some national efforts not entirely aligned with global industry efforts
- Fragmentation unhelpful when a globally aligned approach is required
- Inactivity by many countries undermining effectiveness of deployed measures
- Much work has been done and much remains to be done

What needs to happen

- Engagement and involvement of law enforcement
- Policing of distribution channel to tackle trafficking of stolen devices
- Legislative and judicial enablers need to support anti-theft initiatives
- Focus on devices and avoid discommoding users
- Renew emphasis on collective efforts and all countries to play their role
- Support existing capabilities rather than replicating / undermining them
- Effectiveness of deployed approaches to be measured and reported on
- Learn from what has worked well, what has not and identify why
- Embrace emerging technologies and solutions to bridge gaps

Wish list for governments and regulators

- Operator deployment of EIRs to block stolen devices on local networks
- Observe best practice guidelines for the blocking of devices and sharing of data
- Connection of operator EIRs to IMEI Database to ensure international blocking
- Increased IMEI security levels and reporting and resolution of known problems
- IMEI checking by law enforcement, customs, retailers and consumers
- Enforcement action against criminals – IMEI changing, theft and trading
- Education of consumers and promotion of kill switch capabilities
- Agreement and reporting on measurement metrics to track progress

GSMA willing to assist with capacity building and solution development

To subsequently clarify any of this material, request additional information or report IMEI security issues please contact:

jmoran@gsma.com