Device Blocking and Data Sharing Recommended Practice

Version 2.0

27 January 2022

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Contents

1. Introduction

Mobile devices are an integral part of daily life for a significant portion of the global population and the ability to remain connected is highly valued.

The GSMA and its members have engaged in dialogue with regulators, governments, Operators and mobile device manufacturers in order to find solutions to combat device crime. The GSMA's contribution to the global fight against mobile device crime consists of a multi-faceted programme of initiatives that includes the promotion of stolen device blocking, the upgrade and expansion of its global database of blocked device identities, and engagement with manufacturers to make the electronic identities of mobile devices more secure to ensure the effectiveness of device blocking.

Whilst the problem of device theft is not of the industry's creation, the GSMA recognises device crime as being a major public policy concern for Operators and national authorities. The GSMA has developed a number of initiatives to help address this problem and these are centred on the blocking of flagged device identities across mobile networks in a consistent, efficient and effective manner.

1.1 Purpose

The purpose of this document is to set out best practices for Operators to block mobile devices on their networks which are the subject of device crime and to share such Mobile Device Crime Data with others using the GSMA's Device Registry.

The document is designed to address inconsistencies that may exist between the individual policy, technical and process approaches adopted by individual Operators.

Operator alignment of approaches on a variety of aspects has the potential to resolve common problems and shortcomings that have been reported and encountered by early adopters. Key areas for improvement include the following;

- Comprehensive blocking of devices within and across all networks
- Timely blocking of devices within and across all networks
- Consistent treatment of device crime victims across all networks

It is not intended that the provisions contained in this document are legally binding or that they, in any way, imply legal obligations for, or between, the Operators.

1.2 Scope

The GSMA recognises there are a number of technology and solution options open to Operators when it comes to blocking devices and sharing data. Consequently, the best practices outlined in this document are not intended to be prescriptive to the point that they are technology or tool specific but rather that they provide a high-level description of the intention and objective. Neither are the best practices put forward as being superior, but they are capable of delivering desired improvements in terms of increased consistency and efficiency.

This document is written for Operators and it is recognised that best practices such as those recommended in this document are transferable to, and are likely to be of interest to, stakeholders in all markets.

The scope of this document is focussed on device blocking on networks and the sharing of data pertaining to those devices via the Device Registry. It does not extend to aspects such as consumer education, device checking capabilities, IMEI security, or remote locate lock and wipe solutions, all of which are essential to a holistic approach to combat device theft but are outside the scope of this document.

Device blocking described in this document is cellular network based and only controls access to cellular networks. Blocking does not extend to other networks and technologies, such as Wi-Fi, that do not have the same device blocking capabilities.

This document is primarily focussed on 3GPP defined technologies such as GSM, UMTS, LTE and 5G but does not preclude blocking of devices, (and sharing of information pertaining to them), designed to support other technologies such as CDMA and CDMA2000 in which devices use Electronic Serial Number (ESN) or a Mobile Equipment Identifier (MEID).

1.3 Document Structure

This document is structured as follows:

- Section 1 contains the introduction to this document including its purpose, scope, and structure.
- Section 2 provides an overview of how this document evolved and was developed
- Section 3 highlights the need to ensure data sharing activities do not breach customer privacy and data protection legal and regulatory requirements
- Section 4 describes the role of device blocking to combat device crime
- Section 5 sets out the best practice on local device blocking policy and process
- Section 6 outlines the best practice on use of the Device Registry to share Block List information
- Section 7 describes some general principles that should be taken into consideration

1.4 Abbreviations, Terms and Definitions

Abbreviation/Term	Definition
3GPP	3rd Generation Partnership Project
Best Practice	This document upon which the cooperation and common agreement between CNOs is based
Block List	A device status list in the Device Registry that holds IMEI numbers of devices that may be blocked from use on cellular networks, including the reason for being inserted or removed
CDMA	Code Division Multiple Access, 2G mobile technology standard developed by Qualcomm and TIA
CDMA2000	Code Division Multiple Access, 3G mobile technology standard developed by 3GPP2
CDR	Call Detail Record: Call records for Subscribers whose devices are reported lost and stolen that give call history, including the IMEI

Abbreviation/Term	Definition
CNO	Contributor Network Operator: An Operator authorised by GSMA to retrieve Block List records from the Device Registry for the purpose of blocking devices on its network
Contributor	An organisation authorised by GSMA to use the Device Registry to update the Block List. Eligibility is defined in SG.18.
Device	Cellular telephone or wireless equipment that contains an IMEI
Device Registry	Database maintained by the GSMA to facilitate the sharing of block list information
Duplicate IMEI	A non-unique IMEI contained in two or more different mobile devices
EIR	Equipment Identity Register: Cellular Network Function featuring a database holding common status of devices, plus local status, to enforce the identification, checking and blocking of IMEIs
ESN	Electronic Serial Number: used to identify an individual CDMA device
GSM	Global System for Mobile communications
GSMA	GSM Association
IMEI	International Mobile Station Equipment Identity or International Mobile Equipment Identity: An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer. (3GPP TS 21.905)
LTE	Long Term Evolution: 4G mobile communication standard developed by 3GPP
MEID	Mobile Equipment Identifier: used to identify an individual CDMA device
Mobile Device Crime Data (MDCD)	The status of device identifiers reported to, and recorded in, GSMA's Device Registry Block List
MNO	Mobile Network Operator. A legal entity that is licensed by a competent licensing authority to provide wireless services to the public and that operates a cellular network to provide public services
MVNO	Mobile Virtual Network Operator. Organisation that provides wireless services using the radio access network of one or more MNOs
Operator	MNO or MVNO that provides wireless services

Abbreviation/Term	Definition
Owner	The owner and/or authorised user of the device. Typically, this would be the same individual who purchased the device, but there are many variations on this, and the purchaser may be a spouse, parent or employer where the device is given to a partner, child or employee. The owner also implies the authorised user of the device with the assumption there is only one owner, although there may be variations.
Subscriber	A person or entity that subscribes to and uses the products and services of an Operator, in the context of this document the victim of device crime
UMTS	Universal Mobile Telecommunications System: 3G mobile communication standard developed by 3GPP

2 Overview

The set of best practices in this document were developed based on engagement between GSMA and its members to understand how Operators perform device blocking. The exercise highlighted greater commonality, rather than differences, in terms of approach although some minor variations became apparent. Some of those anomalies are reflected in these best practices, which seek to document the most common approaches to the various aspects covered in the document. Individual Operators may notice where the guidelines differ from their current processes or polices.

It is impossible to create a document that describes the way every Operator combats mobile device crime. Instead, GSMA tries to reflect the most common policies and approaches considering there are a few areas of difference. GSMA believes these to be relatively insignificant and capable of being resolved with some compromise and flexibility on the part of those with variances.

3 Customer Privacy and Data Protection

Some of the practices recommended in this document, particularly in section 6, are related to the sharing of Mobile Device Crime Data between CNOs for the purpose of preventing the re-use of devices that are the subject of device crime. An essential component of the shared data is the device identifier, most commonly the IMEI but could also be an ESN or MEID.

Increasingly a mobile device is used by a single individual and therefore a device identifier such as an IMEI, ESN, or MEID can be used to link to or identify an individual. Although the GSMA is not directly handling personal details of device owners, Operators involved in the device blocking process will use these details in the process as described in section 5 of this document.

With the publication of the EU General Data Protection Regulation[1] (GDPR) regulations in 2018, and the increasingly broad approach to the definition of personal data being taken in a

[1] https://gdpr.eu/

number of jurisdictions, GSMA considers it prudent to treat device identity data in a manner consistent with the treatment of personal data to reduce risk.

4 Blocking Devices

There is a strongly held belief that if devices flagged on the Block List can be rendered useless, they become worthless on the underground market. If the market disappears, thieves will stop targeting mobile devices as desirable consumer goods to be stolen and reused or resold.

Operators can block specific devices from accessing their networks by using the standards defined Equipment Identity Register (EIR), which was originally created to allow operators to disable devices that were not type approved or could cause interference on mobile networks. The mechanism relies on each device having a unique electronic identity. This is known within the standards as the International Mobile Equipment Identifier (IMEI), in the case of 3GPP compliant technologies, or the ESN and MEID for 3GPP2 defined technologies.

To control network access, operators can create a database within their networks – technically known as the EIR - in which the electronic identities of devices can be stored. Devices to be denied network access can then be registered on a “block list”. During the registration and authentication process that occurs whenever a device attempts to connect to a mobile network the IMEI is checked against the database and if the IMEI is contained in the block list, access will be denied.

EIRs are used to block network access to devices flagged as stolen or subject to device crime and, although these tend to be the most efficient, other proprietary solutions that use CDR analysis and/or transaction triggering capabilities can also be used. The precise approach and method of device blocking is entirely a matter for individual Operators and the best practices outlined in this document are solution agnostic and can apply to whatever approach is preferred.

5 Local Network Device Blocking

The success of device blocking initiatives is largely dependent on all Operators taking a consistent approach, in terms of policy and process, and adhering to that approach. The GSMA sets out the following best practice and pragmatic steps for Operator blocking of devices that are the subject of device crime:

5.1 Operators shall deploy a technical solution that is capable of identifying and blocking mobile devices based on their unique identifiers.

5.2 All mobile devices that have unique identifiers, such as feature phones, tablets, etc. and not just smartphones, are capable of being blocked and are subject to this best practice.

5.3 Due to the difficulty in differentiating between lost and stolen devices, and the fact that unreturned lost devices often end up the hands of others, no such distinction will be made for the purposes of blocking devices.

5.4 Operators shall provide facilities for Subscribers to report loss and theft of devices on a 24-hour basis by accessing web based service portals or by calling and notifying customer service.

5.5 Devices reported lost or stolen shall be blocked.
5.6 Devices stolen from the retail and distribution channels shall be blocked if the identifiers are known and are considered reliable.
5.7 Operators shall authenticate and verify the identity of Subscribers reporting a lost or stolen device using its normal customer authentication procedures prior to taking any block list action.
5.8 Operators shall accept and act upon Subscriber reports of lost or stolen devices in good faith without requiring a police report.
5.9 Operators shall verify the IMEIs of devices reported by Subscribers as lost or stolen by using call detail records to identify legitimate traffic known to have been generated by the Subscriber within 30 days of the report.
5.10 Operators shall carry out checks for duplicate IMEIs on their own network before adding to their local block list and shall not block IMEIs known to have been duplicated to avoid denying service to other innocent Subscribers.
5.11 Operators shall populate their local block list within one hour of receiving a Subscriber's report of a lost or stolen device.
5.12 Operators shall check device identifiers transmitted to the network against a block list on the occasion of every subscription attach and location update on the network.
5.13 Operators shall maintain device identifiers on their block list for a minimum period of three years unless the devices to which they relate are otherwise reported found or recovered.
5.14 Operators shall permit emergency calls from otherwise blocked devices in accordance with regulatory obligations to support such traffic.
5.15 Operators shall perform IMEI/device checks for home network Subscribers.
5.16 Operators shall only unblock devices in the home network upon receipt of an authenticated report from the legitimate user of the device confirming it has been found or recovered.

6 Device Data Sharing

The GSMA Device Registry supports a global Block List of device identifiers associated with devices that are subject to device crime that should be blocked from sale or use on mobile networks.

Operators who deploy EIRs or other device blocking capabilities in their networks are eligible to use the GSMA Device Registry as a CNO to share their latest lists of blocked devices with other CNOs and industry stakeholders according to the GSMA Mobile Device Crime Data User Access Policy (FS.44). The Device Registry takes the block lists from the various Contributors around the world and compiles the data into one global Block List. When a CNO connects to the Device Registry it can download the latest device Block List information from other contributors. By loading the GSMA Block List data into its local device blocking system, devices flagged by other contributors are now also capable of being blocked on that network.

The Device Registry is available to Operators who are encouraged to use the platform to submit and use Block List information for the widest possible sharing of Mobile Device Crime Data.

The following best practice should be adhered to:

6.1 Each CNO shall establish its own connection to the Device Registry.
6.2 CNOs shall ensure their use of the Device Registry adheres to the GSMA connectivity and format requirements for data exchange.
6.3 CNOs shall upload data from their local Block List to the Device Registry on an hourly basis.
6.4 CNOs shall upload to the Device Registry all identifiers reported lost or stolen from their local block list to ensure the widest possible sharing and blocking of flagged devices.
6.5 CNOs shall upload to the Device Registry identifiers that are known to be duplicated using the Duplicated IMEI reason code 0016.
6.6 CNOs must ensure the reason for blocking a device is in accordance with local laws.
6.7 CNOs shall select the correct reason code when updating the GSMA Block List.
6.8 CNOs shall not block a device to gain commercial advantage or inflict damage to any other party and should not block a device to withhold service or to resolve commercial disputes.
6.9 CNOs shall remove any entry which they made in the Block List as soon as there is no longer a valid reason for it to remain.
6.10 CNOs shall download data from the Device Registry to their local block list on an hourly basis.
6.11 CNOs shall download and block lost or stolen Block List information from all Contributors using the Device Registry. Device identifiers flagged on the Block List using other reason codes (e.g. fraudulently obtained) should also be blocked locally as they are also often associated with device crime.
6.12 CNOs shall block all IMEIs downloaded from the GSMA Block List unless there is evidence that an error has been made, that IMEIs were entered with malicious intent, or duplication is suspected.
6.13 CNOs shall remove IMEIs from their local block list within one hour of being notified by the Device Registry of its removal from the Block List.
6.14 CNO that operate a CDMA or CDMA2000 network shall upload ESN and MEID data to the Device Registry as data sharing is not restricted to IMEI data from GSM/UMTS/LTE networks.
6.15 It is recognised that when a CNO inserts an IMEI in the Block List only that CNO can remove that entry, and will do so only if convinced the device status has changed according to the relevant paired reason codes (e.g. lost or stolen -> recovered, fraudulently obtained → validly obtained, etc.). Otherwise, the IMEI will remain flagged in Block List until such time as all Contributors have removed their respective Block List records.
6.16 If a CNO believes its own customer is impacted due to an error made by another Contributor, it may escalate a request to review the specific Block List record to confirm the device was flagged as a result of a valid report. An escalation should be raised only in exceptional circumstances; the default position is the CNO should advise its customer to revert to the source from which it acquired the blocked device for an explanation and resolution.
6.17 CNOs having difficulties connecting to the Device Registry may use e-mail or other file exchange methods to transmit their block lists records to other CNOs in the appropriate format.
6.18 CNOs shall synchronise their local block lists with the Device Registry semi-annually to ensure dataset consistency.

7 General Principles

In addition to the detailed recommended practices outlined in Sections 5 and 6 the following shall apply:

7.1 CNOs shall provide an operational point of contact for the Device Registry to deal with operations and maintenance enquiries from GSMA and other Contributors in a timely manner. CNOs should consider establishing an e-mail alias/distribution list to ensure timely receipt and response to inquiries from other Contributors.

7.2 CNOs shall review, at least once annually, the substance, content and implementation of these recommended practices and address any challenges that may be encountered in meeting the objectives of these best practices.

7.3 CNOs shall, at least once annually, submit to GSMA the Self Declaration of Conformance to these best practices.

7.4 To help aid understanding of the movement of devices that are the subject of device crime, CNOs shall report on devices observed on their networks which have been flagged by other Contributors. Such reports should at a minimum contain the TAC, Contributor name and date of the Block List action.

7.5 CNOs shall facilitate use of the Device Registry by Mobile Virtual Network Operators (MVNOs) which they host on their networks by one of the following means:

- 7.5.1 Upload Block List reports to the Device Registry on behalf of the MVNO. The CNO shall provide a technical means (API, batch file exchange, etc.) by which the MVNO can report IMEIs to the Block List.
- 7.5.2 Direct the MVNO to become an authorised Contributor and user of the Device Registry to directly flag IMEIs on the Block List. CNOs shall use the Device Registry to download and act upon the MVNO block list information according to these best practices.

Annex A Self-Declaration of Conformance

A.1 CNO Information

	Organisation Information
Organisation ID	
Organisation Name	
Main Contact Name	
Main Contact Email	
Date of Report	

A.2 Conformance to Best Practices

#	Description	Y/N	Explanation / notes
	Local Network Device Blocking		
5.1	Ability to locally block IMEIs		
5.2	Block all device types with IMEIs		
5.3	No distinction between lost or stolen		
5.4	Subscribers can report lost/stolen 24x7		
5.5	Lost or stolen devices are blocked on local network		
5.6	Block devices stolen from retail and distribution channels		
5.7	Authenticate Subscriber account / identify prior to blocking		
5.8	Do not require police report to validate Subscriber report of lost or stolen device		
5.9	Before blocking, verify IMEI activity by Subscriber with the reported lost or stolen device within 30 days of the report		
5.10	Check for duplicate IMEIs on local network before adding to local block list		
5.11	Add to local block list within one hour of receiving Subscriber report		
5.12	Check IMEIs on local network per every subscription attach and location update		
5.13	Maintain and use active block list data for a minimum of three years		
5.14	Permit emergency calls regardless of block list status		
5.15	Check IMEIs for home network Subscribers?		
	Check IMEIs for inbound roamers?		

5.16	Require authenticated report from legitimate user of the device before unblocking on local network? What type?		

	Device Data Sharing		
6.1	Only support Subscribers within a single country for a given Device Registry account?		
6.2	Adhere to GSMA technical and format requirements for data exchange with Device Registry?		
6.3	Upload data to Device Registry on an hourly basis?		
6.4	Upload all lost or stolen data from local block list to Device Registry?		
6.5	Report known duplicates to Device Registry using reason code 0016?		
6.6	Comply with local laws for device blocking?		
6.7	Use correct reason codes when uploading to Device Registry? E.g. do not use lost or stolen if broken or faulty		
6.8	Do not report devices to Device Registry as a collections tool?		
6.9	Submit Block List removal record when reason for reporting is no longer valid?		
6.10	Download Block List data from Device Registry to local block list on an hourly basis?		
6.11	Download and block lost or stolen Block List info from all Contributors to Device Registry?		
6.12	Locally block all Block List data obtained from Device Registry within one hour?		
6.13	Remove IMEIs from local block list within one hour of retrieving applicable records from Device Registry to remove an IMEI from the Block List?		
6.14	If operating CDMA networks, submit ESN and MEID block list data to Device Registry?		
6.15 6.16	Respect Block List action by others, only remove or override from local block list after consultation and escalation with other Contributors to resolve disputes.		

6.17	Since prior report, have you submitted data directly to other CNOs? If so, due to connectivity issues with the Device Registry?		
6.18	Synchronise local block list with the Device Registry at least semi-annually?		

	General Principles		
7.1	Maintain a valid operational point of contact in the Device Registry? Use of individual e-mail address or alias/distribution list?		
7.2	Review best practices annually?		
7.3	Date last report submitted?		
7.4	Report devices flagged on Block List by other Contributors when visible on local network?		
7.5.1	Report to Device Registry on behalf of MVNOs using local network?		
7.5.2	Use Device Registry to exchange block list information from MVNOs using local network?		

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	20th Jan 2021	New document that recommends good practice for lost/stolen device blocking and data sharing	GSMA TG	James Moran, GSMA
2.0	28th Jan 2022	Terminology and language have been updated to better align with the Device Registry Specification and Access Policy document. A number of recommended practices have been added or changed to enhance the effectiveness of device blocking and data sharing and a self-declaration of conformance has been added.	FASG	James Moran, GSMA

B.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions.