Device Blocking and Data Sharing Recommended Practice

Version 1.0

19 January 2021

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, Network Operators and mobile device manufacturers in order to find solutions to combat device theft. The GSMA's contribution to the global fight against mobile device theft 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 stolen 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 theft as being a major public policy concern for Network Operators and national authorities. The GSMA has developed a number of mobile device theft initiatives in order to find solutions to address this problem and these are centred on the blocking of lost and stolen devices across mobile networks in a consistent, efficient and effective manner.

1.1 Purpose

The purpose of this document is to recommend practices to be observed by Network Operators pertaining to the blocking of lost and stolen mobile devices on their networks and to the sharing of data relating to those devices via 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 Network Operators that block devices and share information via the Device Registry.

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 loss and theft 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 Network Operators.

1.2 Scope

The GSMA recognises there are a number of technology and solution options open to Network Operators when it comes to blocking devices and sharing data. Consequently, the 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 practices put forward as being the best, and therefore superior, but they are considered to be capable of delivering desired improvements in terms of increased consistency and efficiency. As such, they are classified as recommended practices.

This document is written for Network Operators and it is recognised that 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 theft
- Section 5 sets out the recommended practice on local device blocking policy and process
- Section 6 outlines the recommended practice on connectivity to, and device data sharing via, the Device Registry
- 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
Block List	List of the IMEI numbers for mobile devices that have been blocked on a specific wireless operator's network and uploaded to the GSMA Device Registry or as circulated to other wireless operators
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

Abbreviation/Term	Definition
CDR	Call Detail Record: Call records for subscribers whose devices are reported lost and stolen that give call history, including the IMEI
CNO	Connected Network Operator: a GSMA member Network Operator or a Mobile Virtual Network Operator that is connected to and exchanges data with the GSMA Device Registry
Data	The information to be shared between the CNOs being the information on IMEI numbers belonging to lost and stolen devices
Device	Lost or stolen cellular telephone or equipment that contains an IMEI
Device Registry	Database maintained by the GSMA to facilitate the sharing of lost and stolen mobile device data between stakeholders
DB	Database
Duplicate IMEI	A non-unique IMEI contained in two or more different mobile devices
EIR	Equipment Identity Register: software and hardware deployed by CNOs 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)
MEID	Mobile Equipment Identifier: used to identify an individual CDMA device
LTE	Long Term Evolution: 4G mobile communication standard developed by 3GPP
Network	The cellular network operated by a licensed wireless service provider, not limited to the type of technology used
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 do provide 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.
Recommended Best Practice	This document upon which the cooperation and common agreement between the Network Operators is based
Subscriber	A person or entity that subscribes to and uses the products and services of a Network Operator, in the context of this document the victim of a loss or theft
UMTS	Universal Mobile Telecommunications System: 3G mobile communication standard developed by 3GPP

2 Overview

The set of recommended practices in this document were developed based on engagement between GSMA and its members to understand how Network 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 recommended practices, which seek to document what the most commonly taken approaches are to the various aspects covered in the document. Individual operators may notice where the guidelines differ from their current processes or polices.

In conducting consultation exercises with Network Operators it is recognised from the outset that it is impossible to come up with a document that describes the way every operator does things. Instead, GSMA tries to reflect the most commonly adopted policies and approaches in the knowledge 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 that may be out of kilter, depending on the specific aspect.

3 Customer Privacy and Data Protection

Some of the practices recommended in this document, particularly in section 6, are related to the sharing of device data between Network Operators for the purpose of preventing the re-use of lost and stolen devices to help combat device theft. 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, Network 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 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 lost or stolen mobile devices 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 increasingly used to block network access to devices that have been reported as lost or stolen 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 Network Operators and the recommended 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 participating Network Operators taking a consistent approach, in terms of policy and process, and adhering to that approach. The GSMA proposes the following recommended practice and pragmatic steps for the blocking of devices by Network Operators that are reported lost or stolen by its customers:

- Each Network Operator participating in the programme to combat device theft shall deploy a technical solution that is capable of identifying and blocking mobile devices based on their unique identifiers
- 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 recommended practice

[1] https://gdpr.eu/

- 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
- Facilities shall be provided 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
- Devices reported lost or stolen shall be blocked.
- Devices stolen from the retail and distribution channels shall also be blocked by Network Operators if the identifiers are known and are considered reliable
- The originator that reports the loss or theft of a mobile device shall be verified by the Network Operator following its normal customer authentication procedures and only when the party making the report has satisfactorily proven its identity to the Network Operator shall the report be acted upon
- Police reports are not required from customers that report devices stolen to have those devices blocked as theft reports shall be taken and acted on in good faith
- IMEIs of the lost or stolen devices that are to be blocked shall be established by the Network Operator obtaining the correct IMEIs from call detail records for legitimate traffic known to have been generated by the users when in control of the device
- Network Operators shall carry out checks for duplicate IMEIs before putting devices on the block list and shall not block IMEIs that they know to have been duplicated to avoid other innocent users being denied service
- Lost and stolen devices shall be populated into the local block list within one hour of the report having been initially received from the customer
- Network 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
- Blocked device identifiers shall remain on the Network Operator’s block list for a minimum period of three years, unless the devices to which they relate are otherwise reported found or recovered
- Emergency calls shall be permitted from otherwise blocked devices in accordance with regulatory obligations to support such traffic
- IMEI/device checks shall be carried out for home network customers but not for inbound roamers
- Devices shall only be unblocked in the home network in the event of a follow up and 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 that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost or stolen.

Network Operators who deploy EIRs or other device blocking capabilities in their networks can connect to the Device Registry to share their latest lists of blocked devices with other operators. The Device Registry takes the block lists from the various operators around the world that are connected to the system and compiles the data into one global block list. When a Network Operator connects to the Device Registry it can download the latest block

list that contains device identifiers from the operators it has chosen to take data from for its own use. By loading the GSMA Device Registry block list into its local device blocking system all devices reported as stolen on other connected networks are now also capable of being blocked on that network.

The Device Registry solution is available to operators to use free of charge and all Network Operators are encouraged to use the platform to submit and share stolen device data. The following recommended practice should be adhered to:

- Each Network Operator shall establish its own connection to the GSMA Device Registry and shall upload data from its local block list to the Device Registry on an hourly basis
- Each network connected to the Device Registry shall ensure the data exchanged with the platform is in accordance with the requirements specified by GSMA
- Where access to the Device Registry is established, the exchange of information shall be performed electronically by internet connection as defined in GSMA's GSMA Device Registry Specification and Access Policy (SG.18)
- All devices reported lost or stolen to each Network Operator and contained in the local block list shall be uploaded to the Device Registry to ensure the widest possible sharing of data and blocking of devices
- Each connected Network Operator is responsible to ensure that the reason for blocking the device is valid and in accordance with local laws
- The decision to block a device shall not be to gain commercial advantage or inflict damage to any other party and should not be used to withhold service or to resolve commercial disputes
- The uploading Network Operator shall ensure that all mandatory data format fields are completed before forwarding records to the Device Registry
- Records uploaded to the Device Registry shall appropriately and accurately use the reason codes defined by GSMA i.e. devices shall only be uploaded to the Device Registry Block List for reasons approved by GSMA that use the correct reason code as defined in the Device Registry Specification and Access Policy (SG.18)
- The originating operator will remove any entry which it made in the block list as soon as there is no longer a valid reason for it to remain and shall notify the Device Registry of that action to reflect the removal in other networks' block lists
- Each operator shall download data from the Device Registry to its local block list on an hourly basis
- Parties agree to block all IMEIs downloaded from the Device Registry block list directory unless there is evidence that an error has been made, that IMEIs were entered with malicious intent, or duplication is suspected.
- The connected operators shall block, within one hour of being notified of IMEIs that have been placed in the Device Registry block list, to minimise the risk of resale and reuse of lost and stolen devices
- The Parties shall remove IMEIs from their local block lists within one hour of being notified by the Device Registry of an IMEI's removal from the Device Registry
- CDMA and CDMA2000 carriers shall upload to the Device Registry ESN and MEID data as data sharing is not restricted to IMEI data from GSM/UMTS/LTE carriers

- It is recognised that only the originating Network Operator can remove a record from the Device Registry block list and it will only do so if convinced a lost or stolen device has been found or recovered. Otherwise, block list records will remain in the Device Registry
- If a connected Network Operator believes an error may have been made regarding the inclusion of a device identifier in the Device Registry block list that is impacting one of its own customers it may escalate a request to review the specific block list record to confirm the device was blocked as a result of a lost/theft report. An escalation should be raised only in exceptional circumstances as the default position is for the Network Operator to request its customer to revert to the source from which it acquired the blocked device for an explanation and resolution
- In the event of having difficulties in accessing the Device Registry the Network Operators may transmit their block lists to the other operators directly by email once the necessary information is captured in the appropriate format
- All Network Operators 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:

- The Network Operators shall provide an operational point of contact on the Device Registry to deal with operations and maintenance enquiries which may be raised within the group of participating operators and resolved within a reasonable time frame to maintain the efficacy of the system for all participants
- The networks shall review, at least once annually, the substance, content and implementation of these recommended practices and to address any challenges that may be encountered in meeting the objectives of this document
- The Network Operators shall report on devices that are blocked by other operators that they observe on their networks when attempts are made by their own customers to register or use those blocked devices to help aid understanding of the movement of stolen devices
- The Network Operators that host and provide network access for Mobile Virtual Network Operators (MVNOs) shall act as a conduit for their MVNOs by uploading to the Device Registry, on behalf of the MVNOs, IMEIs pertaining to devices that are blocked following reports to the MVNOs by their customers. It is expected that the MVNOs take full responsibility for customer engagement and just provide to their host networks, by API or batch file exchange, the IMEIs to be blocked.

Annex A Document Management

A.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

A.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.