Mobile Device Crime Data User Access Policy

Version 1.0

20 January 2021

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

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Contents

1 Introduction 3
1.1 Background 3
1.2 Scope 3
1.3 Definitions 3
2 Holistic Approach to Combatting Device Crime 4
3 Access to Mobile Device Crime Data 4
4 Policy to Provide Access to Mobile Device Crime Data 5
4.1 Data Protection 5
4.2 Liability 5
4.3 Classification of Access to Mobile Device Crime Data 6
4.4 MDCD User Approval 7
4.5 IMEI Checking Service Provider Access 9
5 Funding of MDCD User Access to Mobile Device Crime Data 9
6 Conclusions 9
Annex A Document Management 10
A.1 Document History 10
A.2 Other Information 10

1 Introduction

1.1 Background

The GSMA fully recognises that mobile device crime is a major issue of public policy concern for network operators, consumers and regulatory authorities. GSMA is committed to support and enhance the provision of device data sharing services and to collaborate with stakeholders to demonstrate the industry's ability to work together to combat device crime.

In parallel with working with device manufacturers to improve IMEI integrity, GSMA offers the functionality needed to allow parties other than Contributors and Contributor Network Operators (CNOs) to access mobile device crime data exchanged using the GSMA Device Registry service pursuant to SG.18 Device Registry Specification and Access Policy ("MDCD" or "Mobile Device Crime Data"). GSMA provides such access as set out in the GSMA Device Registry Services Description, which is available at http://devicecheck.gsma.com/deviceregistryservices

1.2 Scope

This document defines the policy determined by GSMA members that permits eligible organisations, other than Contributors and Contributor Network Operators (CNOs) that provide data to the Device Registry, to have look-up access to the Block List data. The policy describes how organisations qualify to become Mobile Device Crime Data (MDCD) Users and what data they receive from the Device Registry in response to checks performed on individual IMEIs. The document also deals with administrative aspects such as approval and funding of access.

1.3 Definitions

The following terms are used in this document:

Term	Explanation
Block List	A Device Status List that holds IMEI numbers of MEs that may be blocked from use on cellular networks, including the reason for being inserted or removed, that are represented by the letter 'B' in Device Status List Records. Access to this information is subject to this policy.
Contributor	An organisation authorised by GSMA to use the Device Registry to update the Block List.
Contributor Network Operator	A Contributor, either a mobile network operator or mobile virtual network operator, authorised by GSMA to retrieve Device Status List Records from the Device Registry for the purpose of blocking devices on its network.
Device Registry	Database that maintains a list of authorised TAC and a list of TAC allocation records and Device Status List records of flagged devices.
Device Status List	List in the Device Registry indicating the status of a ME: Block List ('B'), Authorised TAC List ('W').
IMEI	International Mobile station Equipment Identity: electronic serial number of a 3GPP compliant mobile device.
Mobile Device Crime Data (MDCD)	The status of device identifiers reported to, and recorded in, GSMA's Device Registry Block List

TAC	Type Allocation Code. 8-digit part of IMEI that is assigned by a Reporting Body.

2 Holistic Approach to Combatting Device Crime

The GSMA's activities to combat device crime are grounded in a commitment to initiate and implement a range of solutions that contribute to fighting this problem.

One such solution is the GSMA Device Registry, which allows elibible Contributors and Contributor Network Operators to connect device blocking systems (e.g. EIR) to the Device Registry to exchange MDCD. This approach facilitates pan-network device blocking and is preferable to isolated and fragmented solutions that are of less value. Additionally, it is critical that other parties that have an interest in combating device crime can engage fully to implement appropriate crime prevention measures. Specifically, the GSMA seeks to encourage the following:

- Implementation, by device manufacturers, of the industry agreed technical principles to prevent the changing of device IMEIs
- Use of the industry initiated IMEI reporting and correction process by device manufacturers and operators to report and correct identified IMEI security weaknesses
- Introduction and enforcement of specific legislation by national regulators/governments to criminalise the unauthorised reprogramming of IMEIs
- Tools and services that identify devices with IMEI changes in cases where device design and legislation attempts to prevent this, have failed

It is hoped that a holistic range of measures, please see above, will complement use of the GSMA Device Registry, and greatly enhance the value of each of the other measures in an effort to reduce device theft and fraud related crime.

3 Access to Mobile Device Crime Data

Whilst network operators, manufacturers, enterprise customers and consumers are the most obvious stakeholders in the fight against device crime, there are a number of additional sectors that have a role to play and these include the following:

- Law enforcement agencies are in the front line of combating street crime and other aspects of criminal activity related to device crime Increased access to, and use of, MDCD helps to deter and devalue device crime.
- Service repair centres that could be used, willingly or unknowingly, as clearing houses to launder devices by facilitating unauthorised IMEI re-programming
- Authorised dealers and retail outlets that exchange devices that have been purposely damaged to claim replacement devices under warranty programmes
- Insurance providers that underwrite device theft insurance policies provided to consumers
- Recyclers that could be used to launder criminally obtained devices by paying money to have the devices reused in other markets or have them broken up for parts
- Data aggregators that compile device data from a variety of sources to provide IMEI checking services to a range of stakeholders

- Industry organisations engaged in anti-fraud and anti-theft initiatives where the information would be of statistical interest
- Providers of solutions to help identify or prevent use of lost/stolen devices

This policy enables read only access to MDCD for parties other than network operators and it supports the holistic approach required to combat device crime.

4 Policy to Provide Access to Mobile Device Crime Data

Responsibility for formulation of the policy pertaining to MDCD User access rests with the GSMA's members and compliance with that policy is enforced by the GSMA support staff. Granting MDCD User access by GSMA is only permitted in accordance with recommendations and procedures set down by GSMA members and approved by GSMA's Fraud and Security Group.

The policy set out in this document defines how best, and in what circumstances, MDCD can be made available to parties other than network operators. The GSMA Device Check service supports multiple tiers of read only access to MDCD.

4.1 Data Protection

Although there is no globally applicable data protection law as such, legislation has been enacted by individual countries based on similar high-level objectives. Therefore, different legislative requirements may apply across individual countries and legal jurisdictions.

Different national requirements have to be considered and the priority of GSMA is to maximise operator use of the GSMA Device Registry. Contributors compelled by local regulation to limit sharing of MDCD should inform GSMA which will work with those Contributors to facilitate participation consistent with local legal requirements.

Increasingly a mobile phone 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. In light of increasingly broad approaches to defining "personal data" or "personally identifiable information" globally, GSMA considers it prudent to treat device identity data including MDCD in a manner consistent with personal data.

This approach generally ensures the removal of any regulatory obstacles to operators intending to use the GSMA Device Registry.

4.2 Liability

The GSMA, although the custodian of MDCD, is merely a provider of a centralised hosting and exchange service for the MDCD. Therefore, the GSMA cannot claim any responsibility for the accuracy or currency of the MDCD data it maintains. Disclaimers are in place to protect GSMA, and authorised contributors of MDCD, to mitigate against any potential claims that may arise as a direct result of action taken by any party because of information received from the GSMA Device Registry Services.

All content of the MDCD is provided "as is", without any warranty of any kind and at user's own risk. The content is for general information only, without into account the particular objectives, situation or needs of any individual users. GSMA does not guarantee that such content will be current, accurate or complete when you access it or that the goals of the MDCD will be achieved.

The GSMA shall not be liable for any user or third party reliance on or claim against the MDCD and its content and any matter provided or undertaken by the GSMA associated with it. In the case of any alleged third-party reliance on or claim against the GSMA in relation to the MDCD and its content the user will fully and finally settle such matter (irrespective if brought against the GSMA) from its own funds without any recourse to the GSMA.

4.3 Classification of Access to Mobile Device Crime Data

A number of parties require read only access to MDCD. Access rights for each category of user, and the nature of the data to be accessible to each, is clearly defined. Five tiers, or levels, of user govern access to MDCD. These can be summarised as follows:

MDCD User Classification	User Description
MDCD User A	Law enforcement and customs agencies Regulatory bodies
MDCD User B	National / Regional Interest groups
MDCD User C	Commercial entities • Authorised Dealers • Repair and refurbishment centres • Providers of device insurance, warranty and financing services • Recyclers and traders of used devices • Providers of reverse logistics services and solutions • Device manufacturers • Mobile Virtual Network Operator (MVNO) • Providers of solutions to help identify or prevent use of lost/stolen devices
MDCD User D	General Public
MDCD User E	IMEI Checking Service Providers. Entities that provide IMEI checking services to eligible end-users, as defined in in this document as MDCD User A, B C or D, including through another IMEI Checking Service Provider.

Table 1: Nature of Data to be Disclosed

GSMA members have clearly defined the type of data to which MDCD Users have read only access. In all cases, the input is a single IMEI number, via the GSMA Device Check service, and the following table sets out the nature of data that may be returned in response to queries originated by types of MDCD Users;

MDCD User Classification	User Description	Response to MDCD User Query
MDCD User A, B and C	Law enforcement and customs agencies Regulatory bodies National / Regional Industry Interest groups Commercial entities	• Whether or not the input IMEI is present on the Block List • Date of each Block List entry for that IMEI • The Contributor name, and corresponding country, responsible for each Block List entry for that IMEI • If TAC information exists for that IMEI, the manufacturer and marketing name of the device • Reason for Block List entry (based upon reason codes) •
MDCD User D	General Public	• Whether or not the input IMEI is present on the Block List • If TAC information exists for that IMEI, the manufacturer and marketing name of the device
MDCD User E	IMEI Checking Service Providers	• Whether or not the input IMEI is present on the Block List • Date of each Block List entry for that IMEI • The Contributor name, and corresponding country, responsible for each Block List entry for that IMEI • If TAC information exists for that IMEI, the manufacturer and marketing name of the device • Reason for Block List entry (based upon reason codes) The above information is available to IMEI checking service providers in so far as the data may only be provided to others according to the applicable MDCD User classification.

Notes:

1. The Type Allocation Code (TAC) agreement between GSMA and device manufacturers provides GSMA the ability to disclose device detail information as appropriate and to be of benefit to the industry. Such information is not classified as Mobile Device Crime Data but is useful in providing clarity and authenticity of mobile devices. Examples of such information include manufacturer, make/model, device type, and networking capabilities.

4.4 MDCD User Approval

MDCD User access is controlled and monitored and each organisation accessing MDCD has a named GSMA Device Check account established to which unique user credentials are allocated after completion of appropriate registration procedures. An end user agreement must be signed and submitted to GSMA before access is approved.

GSMA vets the bona fides of each applicant and its eligibility to access data as an eligible MDCD User as defined in Section 4.3. All checks are thoroughly undertaken by GSMA staff, which take and retain the applicant's details and the evidence supporting its application for review by any GSMA member that may wish to do so.

If GSMA staff are unable to fully satisfy themselves as to the eligibility or bona fides of an applicant they may seek the assistance of any CNO. In the event that such CNO assistance is necessary, the following table sets out the support and sponsorship criteria that must be satisfied for each category of user that applies from a jurisdiction in which there are one or more CNOs.

MDCD User Classification	User Description	Sponsorship Requiredif not Approved by GSMA Staff
MDCD User A	Law enforcement agencies Regulatory bodies	• Sponsorship letters from at least two[1] CNOs in the jurisdiction where the applicant law enforcement agency has authority • Sponsorship letter from all of the CNOs in the relevant jurisdiction in the case of a regulatory body
MDCD User B	National / Regional Interest groups	• Sponsorship letters from at least two CNOs in the case of national /regional interest groups
MDCD User C	Commercial entities	• Sponsorship letter from a CNO, except for a GSMA member device manufacturer in which case approval may be obtained from the GSMA Head of Fraud and Security.
MDCD User D	General Public	• Not applicable
MDCD User E	IMEI Checking Service Provider	• Sponsorship letters from at least two CNOs

Appropriate application forms and sponsorship letters will be provided by GSMA to support the processing of applications for MDCD User access.

In the case where a request is received from an applicant MDCD User in a jurisdiction in which there are no CNOs, GSMA staff will seek to vet the bona fides of the applicant and assess its eligibility to access data as it would do for an applicant from a jurisdiction in which there is at least one CNO. If GSMA staff are unable to fully satisfy themselves as to the eligibility or bona fides of an applicant they may seek the assistance of any local operator(s), regardless of their status as a CNO.

A list of approved MDCD Users (organisation name and country) is available to authorised contributors of MDCD.

[1] Where there is only one operator in that jurisdiction, or where there is only one CNO, the authority of that single operator will be sufficient. In cases where there are no CNOs from that jurisdiction, access can be granted following consultation with any local operator(s) that can assist the vetting process.

4.5 IMEI Checking Service Provider Access

Similar to other MDCD Users, IMEI Checking Service Providers are permitted read-only access to the MDCD using both web and API interfaces.

5 Funding of MDCD User Access to Mobile Device Crime Data

It is not the intention of GSMA to profit from the problem of device crime but it is necessary to levy some charges in order to recoup development, operational and associated costs. Therefore, fees apply for use of the GSMA Device Check service to access MDCD, except for law enforcement agencies and regulatory bodies that are provided with free web access, strictly as end-users.

6 Conclusions

MDCD User access constitutes a significant initiative on the part of GSMA and its members to enable other organisations, and consumers, to combat device fraud and theft related crime. GSMA is pleased to offer the facility to qualified parties and it is willing to provide eligible applicants with the support necessary to obtain access to MDCD in accordance with the GSMA approved policy.

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 describes policy governing access to mobile device crime data	GSMA TG	James Moran, GSMA

A.2 Other Information

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