International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5052

(09/2020)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Combating counterfeiting and stolen ICT devices

Addressing mobile devices with a duplicate unique identifier

Recommendation ITU-T Q.5052

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR P2P COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	**Q.5050–Q.5069**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.5052

Addressing mobile devices with a duplicate unique identifier

Summary

The detection mechanisms for duplicate unique identifiers (UIDs) discussed in Recommendation ITU-T Q.5052 are based on post-processing mobile network data to identify devices for blocking purposes based on criteria defined by individual national regulatory bodies. Through incorporation of one or more of these mechanisms, systems can identify and address the problems that duplicate or cloned devices present to governments, operators and consumers. A combination of one or more methodologies described in Recommendation ITU-T Q.5052 can be employed at any given time. The decision regarding the methodology or methodologies to employ will determine the level of effectiveness of a country's detection mechanism. The presence and detection of duplicate UIDs on mobile networks and identification of the authenticity of a device are two key problems to which stakeholders are looking to find solutions.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5052	2020-09-29	11	11.1002/1000/14392

Keywords

Counterfeit mobile devices, duplicate device detection, eUICC authentication, genuine device detection.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.5052

Addressing mobile devices with a duplicate unique identifier

1 Scope

This Recommendation identifies challenges and proposes mechanisms to enable the detection of mobile devices with duplicate identifiers present on operator networks, as well as recommending mechanisms for validating the legitimacy of such devices.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 charging data record (CDR) [b-ETSI TR 121 905]: A formatted collection of information about a chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR shall be generated, i.e., more than one CDR may be generated for a single chargeable event, e.g., because of its long duration, or because more than one charged party is to be charged.

3.1.2 cloned identifier [b-ITU-T Q.5051]: Is a valid device identifier properly assigned by the responsible management entity to one device but is being used by other different devices.

3.1.3 device user [b-ITU-T X.1127]: The authorized user of the mobile device.

3.1.4 invalid identifier [b-ITU-T Q.5051]: Is a unique identifier that does not comply with the format defined in the technical standards or that is not included in the device identifier reference database distributed by responsible management entity.

3.1.5 mobile device [b-ITU-T X-Suppl.19]: An electronic device used for making phone calls and sending text messages across a wide geographic area through radio access to public mobile networks, while allowing the user to be mobile.

3.1.6 reliable unique identifiers [b-ITU-T Q.5051]: Shall be unique for each equipment it aims to identify, can only be assigned by a responsible management entity and should not be changed by unauthorized parties.

3.1.7 smartphone [b-ITU-T X-Suppl.19]: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

3.1.8 tampered ICT device [b-ITU-T Q.5050]: An information and communication technology (ICT) device that had components, software, unique identifier, items protected by intellectual-

protected rights or trademarks tentatively or effectively altered without the explicit consent of the manufacturer or its legal representative.

3.1.9 unique identifier [b-ITU-T Q.5050]: An identifier associated with a single device that aims to uniquely identify it.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 equipment identity register (EIR): A register that can be used to terminate an access attempt or ongoing call when performing an international mobile equipment identity (IMEI) check procedure depending on the status of the IMEI in one of its registers: blacklist, white list, or grey list.

NOTE – Paraphrased from [b-ETSI TS 122 016].

3.2.2 mobile device identifier database (MDID): A database containing aggregated information about mobile device unique identifiers.

3.2.3 non-access stratum (NAS): A set of protocols in the evolved packet system that is used to convey non-radio signalling between user equipment and the mobility management entity for local terminal emulator or evolved universal terrestrial radio access network access.

NOTE – Paraphrased from [b-3GPP].

3.2.4 radio access technology (RAT) type: Type that indicates which RAT is currently serving the user equipment.

NOTE – Paraphrased from [b-ETSI TS 129 060].

3.2.5 subscription manager data preparation (SM-DP): Functionality that creates, encrypts, packages and installs operator profiles in the embedded universal integrated circuit card.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CDR	Charging Data Record
DDCDS	Device Duplication and Clone Detection System
EID	eUICC Identity
EIR	Equipment Identity Register
eSIM	embedded SIM
eUICC	embedded Universal Integrated Circuit Card
ICCID	Integrated Circuit Card Identifier
ICT	Information and Communication Technology
ID	Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
iSIM	integrated SIM
MDID	Mobile Device Identifier Database
MSISDN	Mobile Subscriber Integrated Services Digital Network
NAS	Non-Access Stratum

NID National Identifier

OEM Original Equipment Manufacturer

UID Unique Identifier

RAT Radio Access Technology

SIM Subscriber Identification Module

SM-DP Subscription Manager Data Preparation

TAC Type Allocation Code

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

a) The phrase "is required to" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

b) The keyword "should" indicates a requirement that is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

c) The keyword "may" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 General aspects

The detection mechanisms discussed in this Recommendation are assumed to be within the context of a device duplication and clone detection system (DDCDS) that post-processes operator data to identify devices for blocking purposes based on criteria defined by regulatory bodies governing operator networks.

Through incorporation of one or more of these mechanisms, such systems can identify and address the ever-growing problem that duplicate or cloned devices present to governments, operators and consumers in every country.

Implementation of a sub-regional or regional central equipment identity register as an exchange point among countries can address the duplication issue across national borders.

The methodologies described in clauses 7 to 10 can make use of either voice only or voice and data CDRs.

7 Detecting Duplicate IMEIs

This clause describes various methodologies for identifying duplicated or cloned devices on a network. Each methodology relies on collection and availability of specific data for analysis.

A combination of one or more methodologies can be employed at any given time. The choice of methodology or methodologies to employ determines the level of effectiveness of a country's detection mechanism.

Use of simpler methodologies identifies egregious abuse, while that of more advanced or multiple methodologies simultaneously deployed identifies more subtle abuse.

7.1 Excessive subscriptions

Excessive subscriptions analysis identifies duplication when the number of international mobile subscriber identities (IMSIs) (subscription IDs) observed using the same international mobile equipment identity (IMEI) exceeds specified thresholds. Such thresholds are most effectively determined based on country-specific factors and user behaviour. For example, a country in which users rarely change subscriber identification module (SIM) cards may use low thresholds, while a country predominated by pre-paid SIM card use and users that are accustomed to regularly swapping SIM cards to take advantage of promotional of rates, may use higher thresholds. Countries can use the results of the analysis to determine the right values for their specific country environment. Over time, this threshold value can be adjusted to ensure device identifier (ID) duplication is detected at finer granularity.

Regardless of the specific threshold values used, there are a couple different algorithms that can be used in such analysis. Example algorithms are described in clauses 7.1.1 to 7.1.2.

7.1.1 Simple subscription threshold

The most basic form of excessive subscription analysis is to evaluate whether an IMEI has been observed with more than a maximum number of IMSI values during any aggregation period. For example:

Logic:

IF ($IMEI_x$ observed with $\geq$ IMSI_threshold over aggregation_period)
    treat $IMEI_x$ as duplicate

IMSI_threshold	number of unique IMSIs per IMEI to be considered a duplicate
aggregation_period	granularity to which observed IMEI-IMSI data is aggregated for analysis purposes (e.g., all observations aggregated daily)

The simple duplicate threshold approach is effective at identifying obvious cases of duplication. For example, if an IMEI is observed with dozens of IMSIs on the same day, that IMEI has most likely been duplicated and is being used by many people.

However, a simple duplicate threshold set too low can erroneously identify legitimate use cases as duplication in addition to real ones. For example, if an IMEI is observed with five IMSIs on a given day, it could be a case of duplication or a subscriber that uses several SIM cards on a regular basis. Likewise, if a person that regularly swaps between three SIM cards sells their device to another person who also regularly swaps between three SIM cards, then on the day of sale for that device, the associated IMEI may be seen with six SIM cards and appear to be a duplicate on that day.

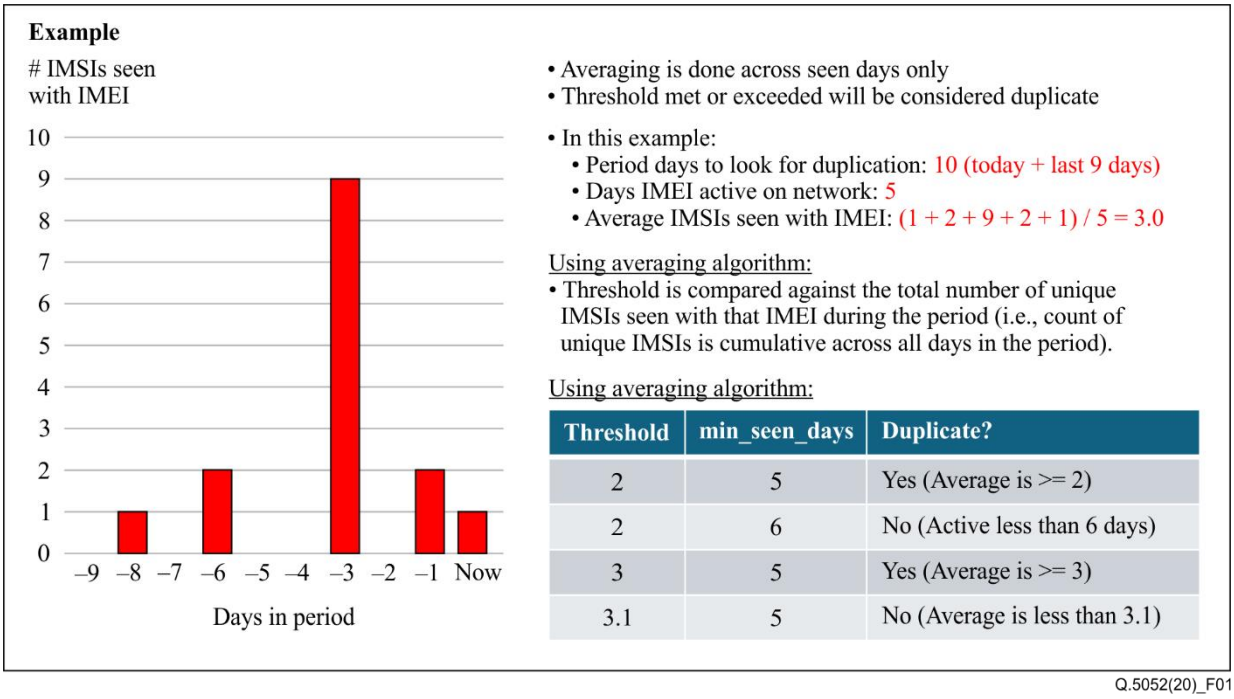
7.1.2 Average subscription threshold

A more advanced version of excessive subscription analysis replaces the simple duplicate threshold with an average threshold. This approach seeks to prevent false positive indications of duplication by looking at the subscriptions seen with an IMEI per aggregation period averaged over an analysis duration for IMEIs observed during a minimum number of aggregation periods. The goal is to identify consistent abuse, rather than transient spikes in IMSI usage. An example follows. See Figure 1.

Logic:

IF ($IMEI_x$ present for < **min_aggregation_periods**)
    could be transient so ignore
ELSEIF ($IMEI_x$ observed with ≥ **avg_IMSI_threshold** over **analysis_duration**)
    treat $IMEI_x$ as duplicate

avg_IMSI_threshold	number of unique IMSIs per IMEI averaged across aggregation periods in which IMEI is observed to be considered a duplicate
aggregation_period	granularity to which observed IMEI-IMSI data is aggregated for analysis purposes (e.g., all observations aggregated daily)
min_aggregation_periods	minimum number of aggregation periods where IMEI must be observed
analysis_duration	number of aggregation periods over which to perform average threshold analysis



Threshold	min_seen_days	Duplicate?
2	5	Yes (Average is >= 2)
2	6	No (Active less than 6 days)
3	5	Yes (Average is >= 3)
3.1	5	No (Average is less than 3.1)

Q.5052(20)_F01

Figure 1 – Example of an averaging algorithm

7.2 Excessive users

In addition to excessive subscription analysis, additional duplicate detection analysis can be performed by leveraging a unique identifier (UID) that is associated with either the IMSI or the IMEI.

In many countries, purchasing a SIM card (IMSI) from an operator requires evidence of an identification (national identifier (NID), driving licence, etc.). UID-IMSI pairings could, subject to local privacy laws, be expected to be maintained by the operator or national authority and provided to the DDCDS system on a frequent basis. Depending on the deployment, the UID might be the actual ID or simply another UID that is mapped to the NID.

Example algorithms are described in clauses 7.2.1 to 7.2.2.

7.2.1 Average excessive user threshold

The average excessive user threshold helps further distinguish between cases such as one person swapping personal SIM cards (IMSI) or different people who are all using the same IMEI.

The algorithm allows IMEIs to be blocked if the average number of UID-IMSI pairings associated with an IMEI exceeds a configured threshold. In this scenario, the UID-IMSI pairings are joined by IMSI with the DDCDS (IMEI, IMSI, mobile subscriber integrated services digital network (MSISDN)) triplet information to create a (UID, IMEI, IMSI, MSISDN) list.

This approach identifies how many different people are using an IMEI and seeks to prevent false positive indications of excessive users by looking at the UIDs seen with an IMEI per aggregation period averaged over an analysis duration for IMEIs observed during a minimum number of aggregation periods. An example follows.

Logic:

IF ($IMEI_x$ present for < **min_aggregation_periods**)
    could be transient so ignore
ELSEIF ($IMEI_x$ observed with ≥ **avg_UID_threshold** over **analysis_duration**)
    treat $IMEI_x$ as a duplicate

avg_UID_threshold	number of unique IMSI UIDs per IMEI averaged across aggregation periods in which IMEI is observed to be considered a duplicate
aggregation_period	granularity to which observed IMEI-IMSI data is aggregated for analysis purposes (e.g., all observations aggregated daily)
min_aggregation_periods	minimum number of aggregation periods where IMEI must be observed
analysis_duration	number of aggregation periods over which to perform average threshold analysis

7.2.2 IMSI UID enforcement

Since presence of a known IMSI-UID relationship is key to the effectiveness of excessive user algorithms, regulators may want a mechanism to identify observed IMSI values that lack such associated UID information for the purposes of ensuring operators collect this missing information or potentially block any IMEIs observed with these UID-unregistered IMSI values.

Key to such enforcement efforts is compliance with local privacy laws and notification campaigns to ensure that any existing user with a UID-unregistered IMSI is notified of the need to provide personal UID information by a specified date. This date would mark the end of the UID grace period and start of enforcement.

Logic:

Before UID grace period ends:
    IF ($IMSI_x$ observed without UID)
        Notify user to provide personal UID before end of grace period

After UID grace period ends:
    IF ($IMSI_x$ observed without UID)
        treat $IMSI_x$ as UID-unregistered *(e.g., block associated IMEI or report $IMSI_x$ to regulator)*

7.3 Device not registered to UID

In countries where registration procedures may be in place or envisioned, regulators can consider the use of UIDs, if local privacy laws permit, which would enable them to identify any use of an IMEI that has not been registered.

Accurate identification requires all users to register their devices with their UIDs. When users sell or transfer their device to another party, they would unregister that device so that the new party can register it. Associations between UID and IMEI can be provided through self-service channels or supported by operators or point of sales channels and updated in the post-processing analysis system automatically.

It is recommended to have a procedure to allow users to prove their device is legitimate, for cases where the IMEI may have been already registered associated with a different UID.

Optionally, to lessen the burden on existing users that have been using their devices prior to a UID registration requirement, pre-existing users could be provided with a grace period during which they can continue using their devices without registering their UID. This list of pre-existing users would include IMEI and associated IMSI values (i.e., the device and SIM cards the user has been observed using with that device prior to the UID requirement).

Logic:

Before grace period ends:

IF ($IMEI_x$ observed with a UID not registered to it)
IF ($IMEI_x$ on pre-existing list with observed $IMSI_x$)
notify user to provide their UID before end of grace period
ELSE
treat $IMEI_x$ as duplicate
IF ($IMEI_x$ on pre-existing list with different IMSI(s))
add these specific pre-existing IMEIx-IMSI pairs to an exceptions
list enabling them to continue working even if $IMEI_x$ is blocked

After grace period ends:

Remove any IMEI-IMSI pairs that were added to the exceptions list to support grace period

IF ($IMEI_x$ observed with a UID not registered to it)
treat $IMEI_x$ as duplicate

7.4 Detection of duplicated IMEI based on time and distance conflicts between CDRs

This type of detection is based on the analysis of time and distance conditions in which CDRs are made with the same device ID using different IMSI, in one or different mobile networks.

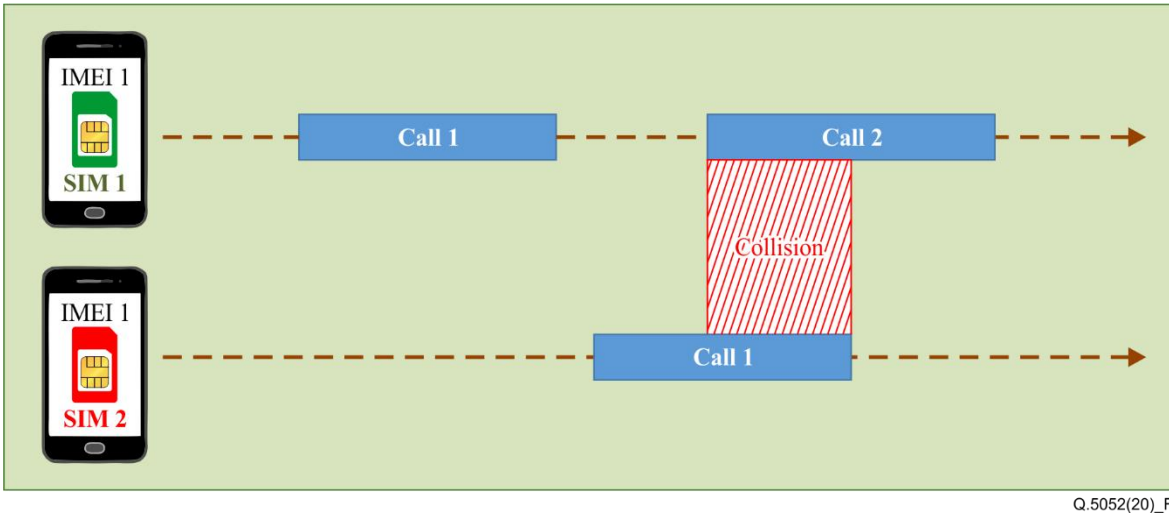
In normal cases, a UID that is programmed on a single device (not duplicated), and that could be used with several SIM cards, will generate CDRs in a sequential order in time, from the cells associated with the locations to which the user has moved.

However, when two or more devices use the same ID, each will have activity at different times and locations, and will generate different CDRs with the same IMEI, with diverse time and location conditions on one or different networks.

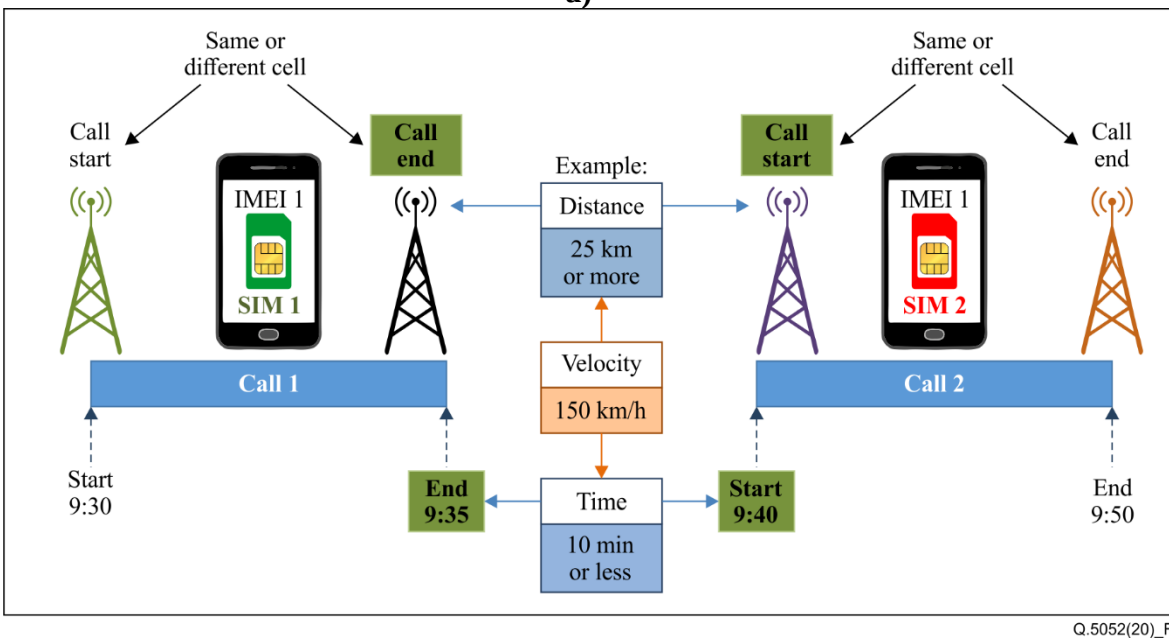
Using algorithms to analyse consecutive CDRs with the same device ID, taking in to account the cell in which the call was originated or terminated, the call duration and the time elapsed between the termination and next origination, two conditions of ID duplication could be detected as follows.

a) Two or more calls overlap in time. See Figure 2 a).

b) Activity from two distant locations occurs in a period of time in which it is impossible to move between them. See Figure 2 b).



a)



b)

Figure 2 – a) Example of two or more calls overlapping in time,
b) example of activity from two distant locations

The advantages of this detection method are that it:

a) can detect cases in which no alarm is detected associated with a number of SIMs used with the same ID (e.g., the same ID is used only with two SIMs that is potentially normal, but is used in the same hour in two distant cities);

b) can detect both intra- and internetwork identifier duplication;

c) relies on network information, regardless of the user information (MSISDN, personal data);

d) offers a high level of confidence concerning duplication conditions.

The disadvantages of this method are that it:

a) is intensive in data processing, especially when voice and data CDRs are considered;

b) is intensive in configuration and fine tuning – all cell site information from different networks must be populated in one instance and updated as network changes occur;

c) has effectiveness that depends on the algorithm to be used: i) a set of parameters of time or distance for urban, semi urban and rural areas, or ii) any time or distance scenario calculated for all CDRs;

d) has limited effectiveness when one of the devices with the same identifier has no activity or activity in different time windows

7.5 Duplicate IMEI detection across countries

As of now, a manufacturer of counterfeit mobile devices may produce multiple devices with the same IMEI. These devices may be distributed/sold in different countries. A robust MDID sharing information with national MDIDs among countries (bilateral, regional or global) will aid in detecting counterfeit mobile devices distributed or sold in such a manner. The objective is to detect instances of IMEIs that are duplicate across countries. Duplicate detection of IMEIs within a country should leverage other methodologies described in this Recommendation. An MDID will be established in such a manner that after connection it is seamlessly interoperable with other national MDIDs of individual countries in a region or sub-region by sharing a list of IMEIs.

In order to detect duplication across countries, an analytics function is required. Analysis can be performed either at the macro- (sub-regional, regional, global) or at the national level. Regardless of where the duplicate detection analysis is carried out, the movement of devices, e.g., sale of used devices from one country to another, as well as the time element, must be considered for this analysis as the same IMEI may appear in two different countries on different (or the same) dates, even though it is the same single device with a unique IMEI.

National MDIDs should contain IMEI lists containing valid, unique and duplicate IMEI instances within their own countries at the national level before sharing their lists with the sub-regional or regional MDIDs.

The regional or sub-regional MDID must be very efficient in the processing of data received.

Figure 3 depicts the layout of this arrangement.

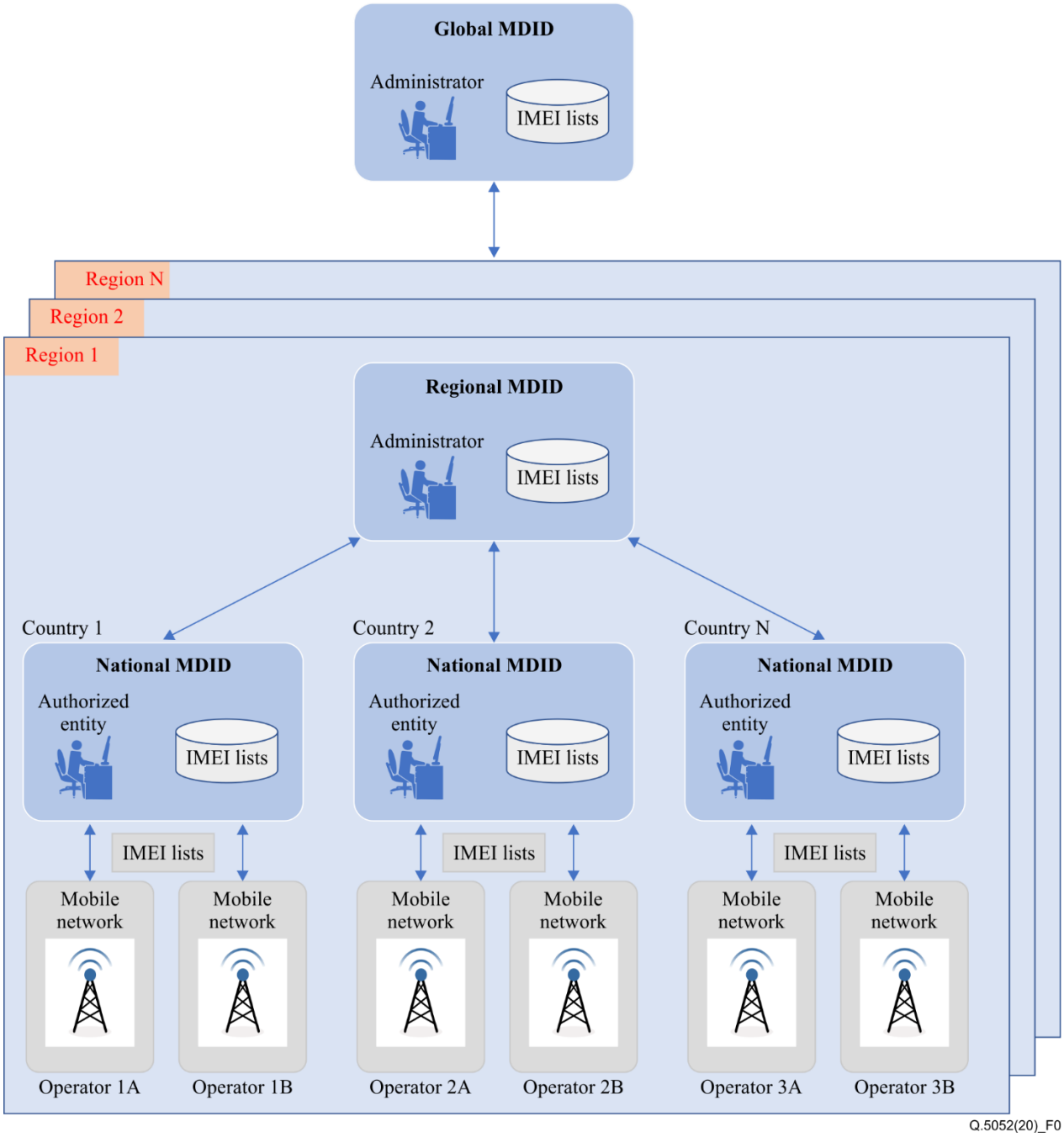


Figure 3 – IMEI list sharing among national, regional, and global MDIDs

8 Determining genuine devices among duplicated IMEIs

As discussed in clause 7, multiple methodologies can be adapted to identify duplicate IMEIs on operator networks. Once duplicate IMEIs are detected, identification of a genuine device from all other duplicates may require multiple techniques, including manual inspection of the device. However, a case of two genuine devices with the IMEI of one device changed or reprogrammed to match the other can still pose a challenge in terms of identifying the legitimate device. In such instances, examining and matching device serial numbers, if available with the support of device manufacturers, to their IMEIs may help validate the legitimacy of the original genuine device.

In addition to physical inspection of the device, another potential approach to device validation is to check key device characteristics and compare them with the official device specifications. These key characteristics may include the following:

– central processing unit type and cores;
– graphics processing unit;
– screen capability;
– sensor types;
– media access control address;
– Bluetooth address;
– serial numbers associated with each device.

The official device capabilities can be maintained by the original equipment manufacturer (OEM) or other central authority that aggregates device specification information from several OEMs. Such central repositories of device characteristics could be used manually during device inspection or through a website or a mobile application on the device.

By providing options such as automatic comparison through a website or mobile application, device characteristics can be compared with the characteristics maintained in the central repository with results provided to an analysis system for providing the information for resolution of duplication. For example, if an IMEI is determined to be a duplicate, all users observed with that IMEI could be instructed to download a validation mobile app to identify the IMEI-IMSI of the authentic device. In such a scenario, the authentic IMEI-IMSI pairing(s) could be added to an exceptions list to enable them to continue receiving service while the IMEI is blocked from use by any other users.

9 Detecting fraudulent use of IMEIs

9.1 Unexpected technology

The RAT type indicates the capability of a device to communicate with certain types of cellular networks. For example, older devices may only be capable of accessing 2G cellular networks, while newer devices may be capable of accessing those of 2G, 3G, 4G or 5G. Because the RAT type of a device can be derived from the type allocation code (TAC) portion of the device IMEI, it is possible to compare the RAT type of any observed IMEI with the capabilities of the network on which it was observed. For example, if a 2G-only device is observed on a 4G network, it could be an indication of a fraudulent device and could be further investigated.

In other words, this algorithm seeks to identify fraudulent devices based on checking consistency between the device capabilities and the type of network on which it is seen.

Logic:

```
Derive RAT type from TAC portion of IMEI

IF (device RAT type < network RAT on which IMEI was seen)
    treat IMEI as a suspected fraudulent device
```

10 Preventing duplication using eUICC authentication mechanisms

For most commercial devices today, it is difficult to leverage the security mechanisms embedded in SIM cards to combat counterfeiting because SIM cards can be easily moved from one phone to another. Therefore, there is no link between a subscription identity and a device identity, which is entirely consistent with the global standards that distinguish between, and separate, the device from the subscription. However, some trends in the industry are changing this basic assumption and open up possibilities to help combat counterfeiting of devices connected to a mobile network.

The trend referred to here is the advent of devices with an embedded SIM (eSIM); also known under the following names: embedded universal integrated circuit card (eUICC), soldered down SIM, integrated SIM (iSIM), non-removable SIM. All these names refer to the case where the SIM card, which holds the subscription credentials to access the cellular network, is either soldered within a

device or even integrated within another component in the device, typically the cellular connectivity modem or a system-on-chip.

In either case (soldered or integrated), the assumption that the subscription identity is independent from the device identity may no longer hold true. Contrary to the device identity (IMEI), it is now possible to verify the authenticity of a connected device's subscription through advanced authentication mechanisms. This authentication is very important for operators to ensure a minimum level of fraud in mobile networks. These two aspects combined in an eSIM-enabled device can be used to combat counterfeiting as described in clauses 10.1 and 10.2.

Prior to describing a possible mechanism leveraging eSIMs to combat counterfeiting, here is some additional background information.

a) eSIMs have been mostly targeted at Internet of things (IoT) devices where providing access to a removable SIM card is either difficult, not required or even not wanted due to size constraints (e.g., connected watches or trackers). Other impediments include difficulty in reaching the device (if it is embedded within another connected device such as a car), costs to change the subscription manually (in the case of a fleet of connected devices), or concerns with subscription theft (if the connected device is in an isolated location).
    i) In practice however, the cell phone industry has started to adopt the same eSIM technology for different reasons (e.g., waterproofing mobile phones) hence eSIMs can apply beyond IoT.

b) With eSIMs, users still have the possibility to change subscriptions electronically. The set of technology features that enables the change of subscription is called remote SIM provisioning.
    i) The fact that the subscription in an eSIM device can still change is not a contradiction to the fact that subscription identity is now linked to device identity. Indeed, the hardware of the eSIM has an identity (called eUICC identity (EID)) that is allocated by the hardware manufacturer and does not change, regardless of the subscription being used.
    ii) EID is similar to an integrated circuit card identifier (ICCID), which is printed on the physical SIM card in human readable form, only that it is used for an eSIM.

10.1 Detection mechanism

The main steps for the detection mechanism are illustrated in Figure 4 and described as follows.

First, during the manufacturing process, the device manufacturer should take the following steps relevant to the detection mechanism:

a) allocate a unique IMEI to each device:
    i) this is typically done as part of the software package that is loaded on to the device;

b) solder-down an eSIM card:
    i) eSIM cards are typically sourced from SIM card manufacturers and may or may not already contain subscription credentials – however, all eSIMs contain an EID;

c) register all EIDs and IMEIs that have been allocated;
    i) mobile device manufacturers need to retain this information as it is required to be printed in a human readable format [b-GSMA eSIM] on device packages.

These steps are part of the existing manufacturing process and mobile device manufacturers already need to retain this information.

Second, when devices are connected to the mobile network, an authorized entity (e.g., the national telecommunication regulator, mobile network operator or an entity acting on behalf of a regulatory authority or mobile network operators) can perform an audit of applicable mobile devices in a

particular country by triggering two network procedures that are standardized and supported in all devices with eSIM:

a) A NAS identity request is triggered from the cellular core network and queries the IMEI of the terminal [b-ETSI TS 124 301].

   i) This procedure is required to be supported on all commercially deployed cellular devices as it is needed to support law enforcement agencies, for example.

b) A common mutual authentication procedure is triggered from the SM-DP+ entity [b-ETSI TS 129 060].

   i) This procedure is required to be supported by all commercially deployed cellular devices that support eSIM. It is required and utilized by operators to verify the authenticity of the subscription.

With the result of these two procedures, the requesting entity needs to store the pair of identities in a repository alongside any other relevant information required to identify the device.

Third, the requesting entity, which has stored the pair of identities, can query each device manufacturer to verify that the devices connected to the mobile network are genuine. The manufacturer does not need to share its entire set of identity pairs (which could expose sensitive information regarding the number of devices sold). However, the manufacturer can verify that the identity pair collected in the field by the requesting entity is indeed a genuine one and it can flag each pair where a fake, malformed or otherwise non-genuine IMEI has been used.

With that information, the requesting entity has the information required to take action depending on the regulatory regime in that country.

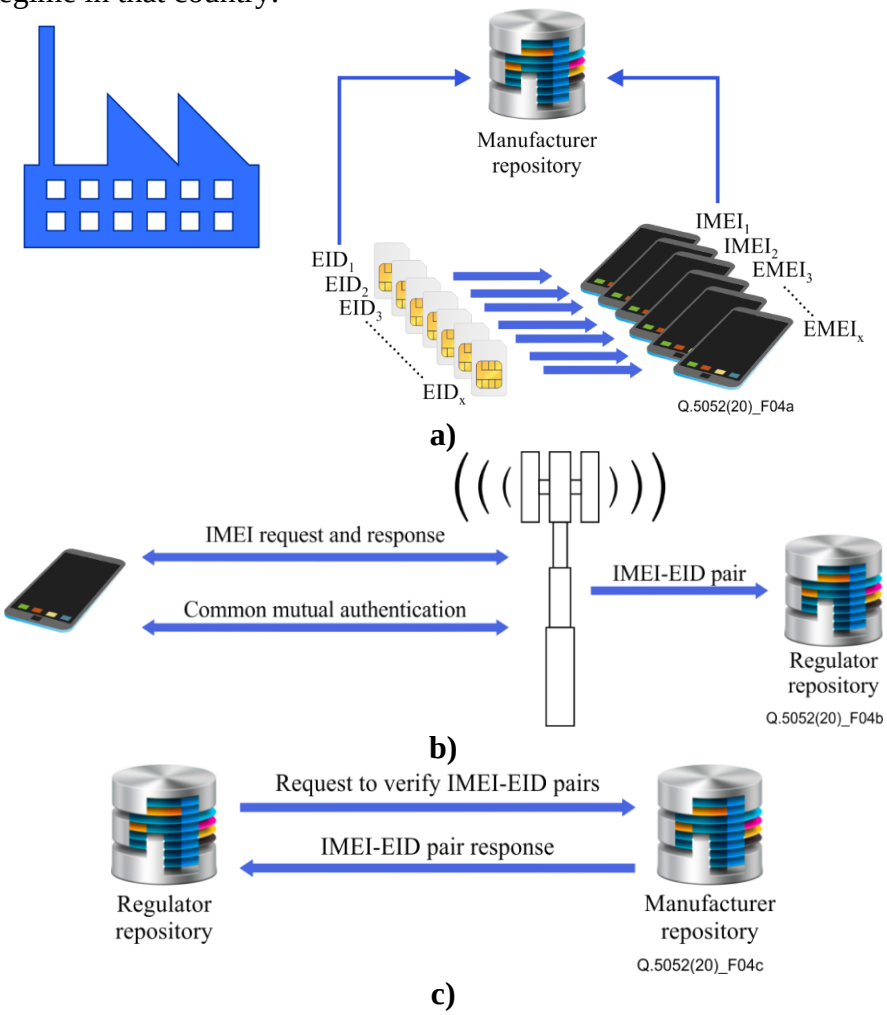


Figure 4 – a) During device manufacture; b) in the field; c) identification verification

10.2 Analysis

Scenarios in which the proposal can be useful include:

– A counterfeit manufacturer includes a genuine eSIM and a fake IMEI.

In this case, the requesting entity will be able to verify by common mutual authentication that the eSIM is genuine and will store the fake IMEI alongside it. Through the IMEI, the manufacturer identity and address can be found and asked whether the IMEI-EID pairing is genuine. If the fake IMEI points to a genuine manufacturer, it will indicate the IMEI-EID pairing is not genuine, and the requesting entity can then list this user as having a fake IMEI.

Bibliography

[b-ITU-T Q.5050] Recommendation ITU-T Q.5050 (2019), *Framework for solutions to combat counterfeit ICT devices*.

[b-ITU-T Q.5051] Recommendation ITU-T Q.5051 (2020), *Framework for combating the use of stolen mobile devices.*

[b-ITU-T X.1127] Recommendation ITU-T X.1127 (2017), *Functional security requirements and architecture for mobile phone anti-theft measures*.

[b-ITU-T X-Suppl.19] ITU-T X-series Recommendations – Supplement 19 (2013), *ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones*.

[b-3GPP] Firmin, F. (2020), *NAS*. Sophia Antipolis: 3GPP. Available [viewed 2020-11-30] at: https://www.3gpp.org/technologies/keywords-acronyms/96-nas

[b-GSMA eSIM] GSMA (2020). *SGP.01-embedded SIM remote provisioning architecture*. London: GSM Association. Available [viewed 2020-12-01] at: https://www.gsma.com/newsroom/resources/sgp-01-embedded-sim-remote-provisioning-architecture/

[b-ETSI TR 121 905] Technical Report ETSI TR 121 905 V16.0.0 (2020), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal mobile telecommunications system (UMTS); LTE; 5G; Vocabulary for 3GPP specifications (3GPP TR 21.905 version 16.0.0 Release 16)*.

[b-ETSI TS 122 016] Technical Specification ETSI TS 122 016 V16.0.0 (2020), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal mobile telecommunications system (UMTS); International mobile station equipment identities (IMEI) (3G TS 22.016 version 16.0.0 Release 16).*

[b-ETSI TS 124 301] Technical Specification ETSI TS 124.301 V15.4.0 (2018), *Universal mobile telecommunications system (UMTS); LTE; 5G; Non-access-stratum (NAS) protocol for evolved packet system (EPS); Stage 3. (3GPP TS 24.301 version 15.4.0 Release 15)*

[b-ETSI TS 129 060] Technical Specification ETSI TS 129 060 V16.0.0 (2020), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal mobile telecommunications system (UMTS); General packet radio service (GPRS); GPRS tunnelling protocol (GTP) across the Gn and Gp interface (3GPP TS 29.060 version 16.0.0 Release 16).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020