International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(07/2020)

QTR-RLB-IMEI
Reliability of International Mobile station Equipment Identity (IMEI)

Summary

The international mobile station equipment identity (IMEI) is an identifier defined by 3GPP that aims to uniquely identify a mobile device across the globe. The value of the IMEI is compromised if the IMEI is not unique, not allocated by the global decimal administrator and cannot be relied upon. This Technical Report describes the overall concept of IMEI, including its format, allocation procedure and security issues. In addition, the Report provides information about existing vulnerabilities that expose the IMEI to unauthorized reprogramming and proposes preventive measures along with possible solutions to mitigate the issue.

Keywords

Counterfeit, IMEI, reliability, reprogramming.

Change log

This document contains Version 1 of the ITU-T Technical Report QTR-RLB-IMEI on "Reliability of IMEI" approved at the ITU-T Study Group 11 virtual meeting, 22-31 July 2020.

Editors:	Biren Karmakar C-DOT	Tel: +91 11 2659 8474 E-mail: biren@cdot.in
	João Alexandre Moncaio ZANON Brasil	Tel: +55 61 2312 2508 E-mail: zanon@anatel.gov.br

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Page

Technical Report ITU-T QTR-RLB-IMEI

Reliability of International Mobile station Equipment Identity (IMEI)

1 Scope

This Technical Report contains a study on the reliability of IMEI, including information about key vulnerabilities to IMEI reprogramming on mobile devices, challenges to make the IMEI non-reprogrammable, effects of IMEI tampering on mobile users, brand owners, manufacturers, service providers, regulators, governments, law enforcement agencies and on national security.

It addresses key challenges faced by a range of stakeholders that arise from cloned/tampered IMEIs, including concerns about the misuse of IMEI numbers raised by Member States at ITU Council-17 and ITU Council-18.

It also proposes ways to improve IMEI reliability and preventive steps for solving the issues on a national and international level.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Report

This Technical Report defines the following term:

3.2.1 mobile identity triplet: A unique set which consists of an international mobile station equipment identity (IMEI), an international mobile station equipment identity (IMSI) and a mobile station international subscriber directory number (MSISDN).

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
CD	Check Digit
CDMA	Code-Division Multiple Access
EIR	Equipment Identity Register
GSM	Global System for Mobile communications
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LU	Location Update
ME	Mobile Equipment
MME	Mobility Management Entity
MS	Mobile Station

MSISDN	Mobile Station International Subscriber Directory Number
SD	Spare Digit
SIM	Subscriber Identity Module
SNR	Serial Number
SoC	System on a Chip
SVN	Software Version Number
TAC	Type Allocation Code
UE	User Equipment
USB	Universal Serial Bus

5 IMEI overview

5.1 General information

The international mobile station equipment identity (IMEI) is a number to identify devices designed to support mobile technologies defined by 3GPP. The IMEI is used to uniquely identify the mobile device and can be used to prevent a mobile device from accessing the mobile network. The IMEI shall be allocated to each individual mobile station (MS) and shall be unconditionally implemented by the MS manufacturer [b-3GPP TS 22.016].

The IMEI can be used to identify mobile devices and prevent it from accessing the mobile network for defined reasons. Each time a mobile device is switched on, a call is made, or a location update is performed the network provider, if it runs an equipment identity register (EIR) on its network, can check the IMEI number of the device, then cross reference it with the EIR blacklist register. If it is on the blacklist, then the network will refuse to allow the device and its related subscription to access the network.

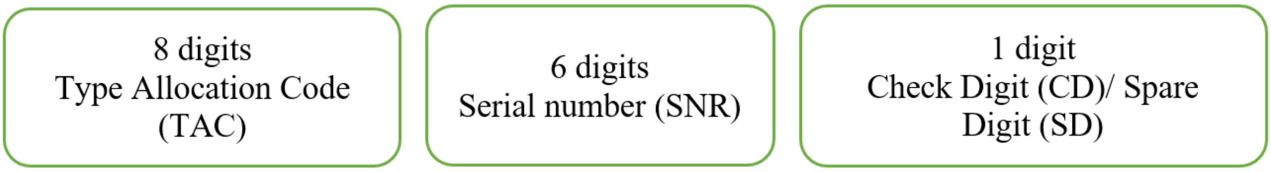
5.2 IMEI structure

The structure and allocation principles of the IMEI and software version number (SVN) are defined in clauses 5.2.1 to 5.3.

The mobile station equipment is uniquely identified by the IMEI or the international mobile station equipment identity and software version number (IMEISV).

5.2.1 IMEI format

The IMEI is a 15-digit number consisting of:



8 digits
Type Allocation Code
(TAC)

6 digits
Serial number (SNR)

1 digit
Check Digit (CD)/ Spare
Digit (SD)

Type allocation code (TAC) – identifies the brand owner, make and model.

The serial number (SNR) is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits.

If the check digit (CD) is implemented, the IMEI (14 digits) is complemented by a CD. The CD is not part of the digits transmitted by the device to the network when the IMEI is checked. The check digit is intended to avoid manual transmission errors, e.g., when customers register a stolen mobile device at the service provider's customer care desk. The check digit is defined according to the Luhn formula.

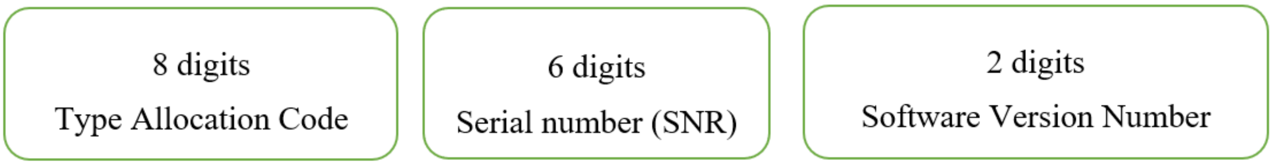
If the spare digit (SD) is implemented, it shall be set to zero, when transmitted by the mobile device.

Example IMEI number:

911347850560031 – where TAC is: 91134785, serial number: 056003, Luhn Checksum: 1

5.2.2 IMEISV format

The international mobile station equipment identity and software version number (IMEISV) is composed as shown below:



TAC identifies the brand owner, make and model, etc., to identify a particular model.

The SNR is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits.

Software version number (SVN) identifies the software version number of the mobile device. Its length is 2 digits.

Example IMEISV:

3568680000414120 – where TAC is: 35686800, serial Number (SNR): 004141, Software Version Number (SVN): 20

5.3 Allocation principles

TAC is issued by the GSM Association (GSMA) in its capacity as the global decimal administrator [b-1].

Manufacturers shall allocate individual serial numbers (SNR) in a sequential order, wherever possible.

For a given mobile device, the combination of TAC and SNR used in the IMEI shall be the same as the TAC and SNR used in the IMEISV.

The SVN is allocated by the manufacturer. SVN value 99 is reserved for future use [b-3GPP TS 23.003].

The GSM Association has defined the requirements that multi-SIM devices should comply with. These requirements are described in [b-TS.37] and should be complied with by the device manufacturers.

5.4 Identifying IMEI on mobile device

The following are some methods to identify the IMEI of a mobile device:

- By dialling *#06#
- By removing the battery cover and looking at the empty battery slot for a label noting the IMEI.
- If the battery is integrated in the mobile device, the IMEI may be etched or printed on a label on the back of the mobile device.
- Through the system menu of the mobile device.

- IMEI is also printed on the mobile device's packaging and may also appear on the invoice/receipt provided by the point of sale.

5.5 Procedure of IMEI checking in mobile network

Whenever an activated SIM is inserted in a mobile device and that device is switched on, the SIM must authenticate itself to the network, independent of the device in which it is used. At the time of SIM registration/authentication (IMSI attach) with the mobile network, the IMEI of the device is provided to the network. If the check IMEI function is supported by the network the status of the IMEI may be checked against the network EIR, if available, which can then check for the presence of the IMEI in its white, grey or blacklists. The EIR gives a response to the core network that contains the status of the mobile device (whether the IMEI is valid and if the device is allowed to connect or not). Based on the response from the EIR, if the IMEI is permitted to access the network, the core network allows the mobile device to continue with the authentication procedure. However, if the IMEI is blacklisted, the core network rejects the mobile device and terminates the authentication procedure.

Optionally, the EIR may check if the IMEI-IMSI pair is the same as the one which corresponds to the IMEI of the mobile device that may be registered elsewhere by the network operator. This correlation of IMSI and IMEI, and the checking of them, is outside the 3GPP defined standards but if the match on IMSI is found by EIR then it may override any blacklist condition found on the IMEI and allow the MS to connect to the network.

Other than the initial power on, the IMEI check can also be performed on the following occasions:

1) When a location update (LU) is performed.

2) Whenever any communication is originated from any subscriber, optionally IMEI checking is performed (for all communications or some pre-defined % of it) – it is dependent on service provider's configuration.

3) Even if there is no event with the subscriber, there is still a periodic location update – which is performed after a regular interval of time – when the IMEI check may be done.

5.6 Different IMEI status

The following are the different status indicators for an IMEI:

1) Valid IMEI – which conforms to all the IMEI checks, allocated by the global decimal administrator [b-3GPP TS 23.003], and is allowed to access network services unless it is blacklisted.

2) Invalid IMEI – format of the IMEI is invalid – like NULL IMEI, all zero IMEI, IMEI with alpha-numeric characters, incomplete digits (less than 14 digits), etc.

3) Blacklisted IMEI – IMEI is not allowed to access network services.

4) Unallocated TAC – TAC of the IMEI was not allocated by global decimal administrator [b-3GPP TS 23.003].

5) Duplicate IMEI – where the same IMEI is programmed in more than one mobile device.

5.7 Limitations of the existing model

The existing model deals with the IMEI status recorded in the EIR database of a particular network to which the subscribers' mobile devices are connected. According to the existing model, if the subscriber loses his or her mobile device, the service provider can block the IMEI of that mobile device in its own network to make the device unusable. In case of multi-SIM/IMEI mobile devices, all IMEIs must be blacklisted separately.

If a criminal changes the SIM card in a stolen device, the mobile device could connect to another network in which the IMEI may not be blocked, thereby giving the device access to the network.

Even within the same network, if the blocked IMEI number is re-programmed, access to the network will be granted to the stolen mobile device if it transmits a different IMEI to the one originally programmed that has not been blacklisted.

A further limitation is that device blocking only applies to mobile networks and because IMEI checking does not exist on other network technologies such as Wi-Fi and Bluetooth, blacklisted mobile devices will continue to work on those networks.

6 IMEI reprogramming

6.1 General information about IMEI reprogramming

IMEI reprogramming refers to unauthorized changing or tampering of the IMEI which was programmed into a particular mobile device at the time of manufacturing. A mobile device's IMEI could be altered to enable illegal re-sale, thus facilitating theft and resale of mobile devices.

6.2 Existing guidelines

The IMEI is incorporated in a mobile station /user equipment (MS/UE) module which is contained within the MS/UE equipment. The 3GPP standards clearly provide that the IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e., manipulation and change, by any means (e.g., physical, electrical and software) [b-3GPP TS 22.016].

This requirement applies to all mobile devices type approved since 1June 2002 and was applicable to all 3GPP system compatible UEs from the start of production.

The manufacturer implementing the IMEI in the mobile device is responsible for ensuring that each IMEI within the allocated range is unique to the mobile device in which it resides, and is also responsible for keeping detailed records of produced and delivered mobile devices.

6.3 Key reasons for IMEI reprogramming

IMEIs of mobile devices are sometimes changed, against the existing guidelines, for a number of reasons:

1) To disassociate the tracking record of a stolen or lost device. This means that, even if the stolen device has been blacklisted by mobile networks via its original IMEI, the new re-programmed IMEI can then bypass network IMEI checks against the blacklist.

2) To disassociate the tracking of the manufacturer and model, including to hide counterfeit devices.

3) For research and analysis purposes.

4) To bypass long distance interconnection charges through the use of SIM boxes to reroute and obfuscate the true origins of traffic.

5) To be able to use the mobile devices that is not registered on a mandatory registration/import list to use the device (for instance, to bypass paying local duties and taxes).

6.4 Key vulnerabilities of IMEI

According to [b-3GPP TS 22.016], IMEIs should not be changeable, but the specification does not indicate any details on implementation characteristics. In order not to stifle innovation, GSMA does not propose mandating a standardized way to achieve secure IMEIs because it recognizes the ability of responsible manufacturers to deliver secure IMEI implementations that are based on pragmatic and attainable technology and engineering approaches [b-2]. Instead, GSMA has published guidelines for device manufacturers on how IMEI implementations should be secured. These are defined as the IMEI security technical design principles and if IMEI implementations satisfy those requirements they can be considered secure and immutable.

6.5 The existing methods for IMEI reprogramming

IMEIs of mobile devices may be implemented in hardware or software. In this regard, there are two methods for changing the IMEIs of mobile devices:

1) Hardware based: by replacing the chipset in a mobile device with one that can work in the target device.

2) Software based: to change IMEI of mobile devices, various tools and hardware flashers are available on the market.

6.5.1 "Flashers" tools

Flashers are a combination of software and hardware. They were originally designed for repair purposes, but they can be illegally used to change the IMEI in some mobile devices.

There are many varieties of flasher boxes covering a wide variety of mobile devices. Therefore, choosing the correct box for a type of mobile device or device model or mobile device manufacturer can be a daunting task. There are two main categories of flasher boxes:

a) Branded boxes

They are more expensive than their proprietary counterparts, have well-known names and model numbers and have unique serial numbers.

Some boxes need activation. Software, updates, and support is provided for these boxes. The level of support varies depending on the manufacturer of the box. They are widely used by service technicians.

They are sold by recognized suppliers and an "approved supplier list" is often found on the manufacturer's website. Thus, it is easier to obtain support for them in forums and on other websites.

Some boxes come with a large amount of cables and can cover both GSM and code-division multiple access (CDMA) devices. They do not usually require an external power supply to function. They rely on the universal serial bus (USB) interface as a power source [b-3].

b) Unbranded (proprietary) boxes

These are much cheaper than branded boxes and sometimes match the original flasher boxes in terms of components and functionality. They sometimes combine the functionality and device support of more than one branded flasher box. They sometimes support the addition of a smartcard from branded flasher boxes.

They do not usually come with any software and/or drivers which puts the onus on the buyer to come up with the software from other Internet sources. Some boxes come with device flashing/servicing cables while others do not. Some require an external power supply that is not usually provided with the purchase.

Flasher dongles are also available and can be used for changing the IMEI in some mobile devices. They often offer less functionality than flasher boxes but may offer additional services.

There are various tools available in the market for IMEI reprogramming.

7 Scale of mobile devices with tampered or cloned IMEI

The following are some facts and figures taken from different news items, reports and statistics which show the scale mobile devices with tampered or cloned IMEI. Itis important to notice that these figures can also be resulted from counterfeit mobile devices:

- "Not less than 50% of the phones readily available on the market are cloned imitation phones," Vodafone said in its comments to the National Communications Authority (NCA) on why there is no need for an Interconnect Clearinghouse (ICH) in Ghana. [b-4]

- The share of mobile device with "zero" or duplicated IMEI in "Rostelecom" network is about 10% [b-5].
- In Colombia, as per the analysis done in 2016, there was almost 13% (see Figure 1) of mobile devices which were linked to more than 3 SIMs in a period of 30 days, showing potential duplication of IMEI [b-6].

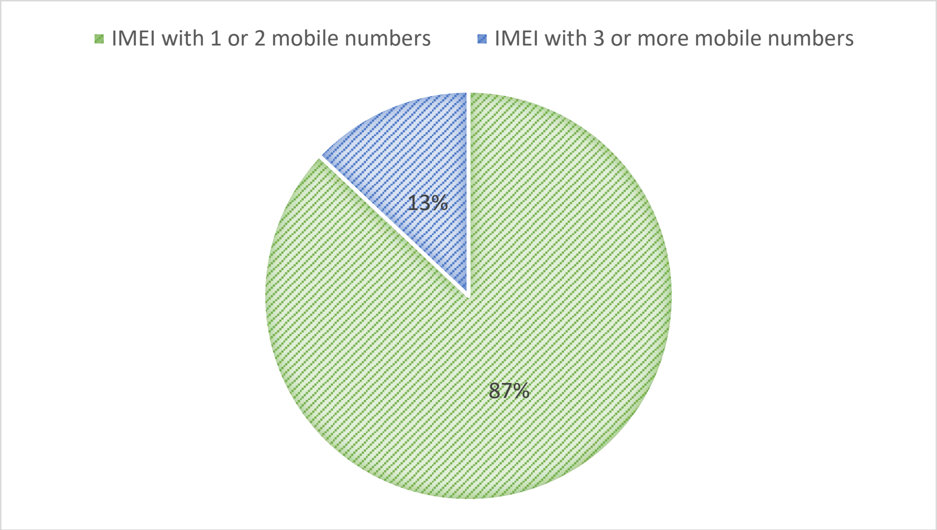


Figure 1 – Duplicate IMEI in Colombia, 2016

Control of duplicate IMEI started in 2017 and after that there is a sharp fall in the number as shown in Figure 2.

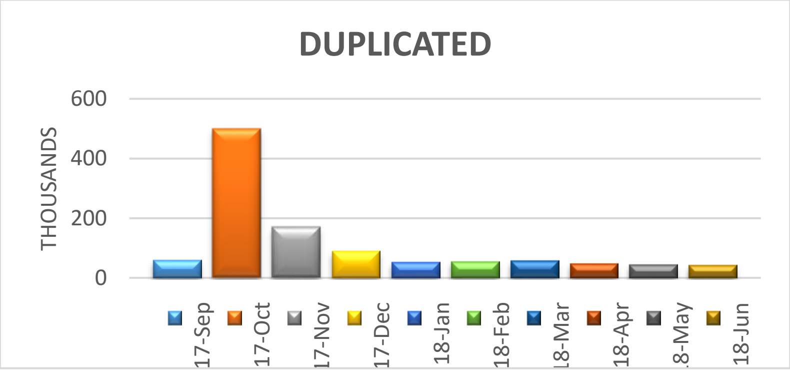
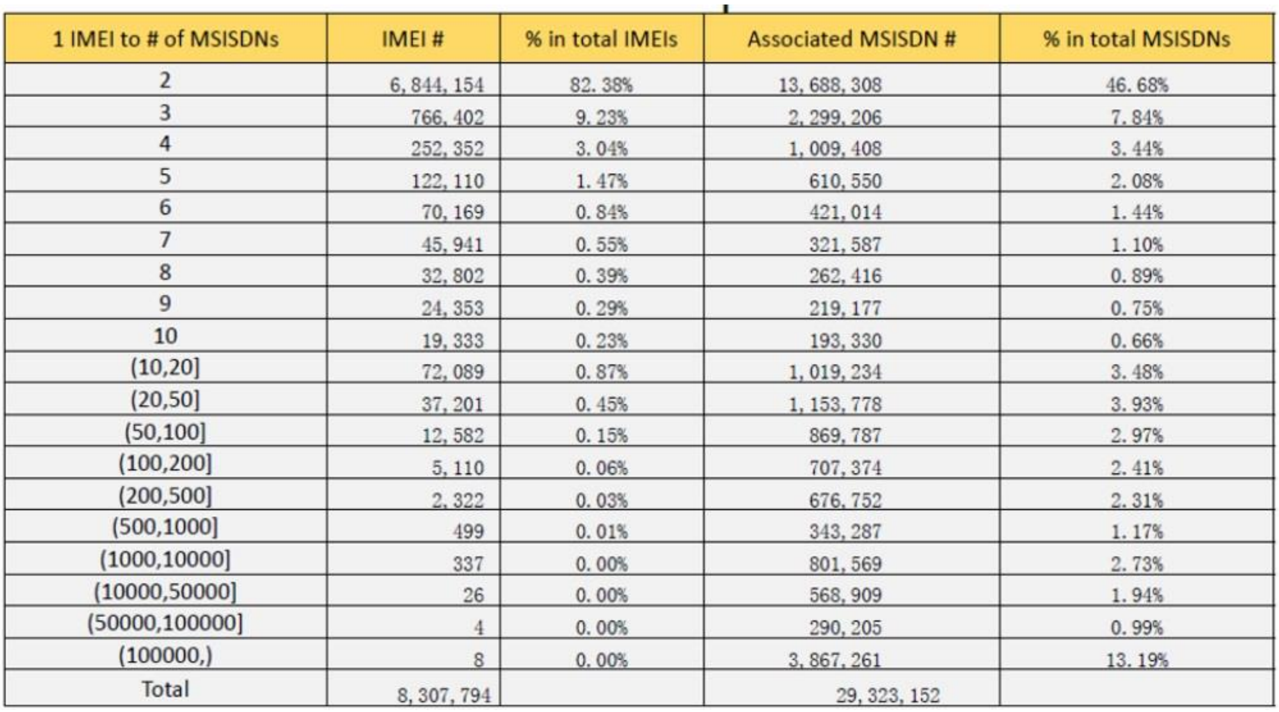


Figure 2 – Trends of duplicate IMEI presence in Colombia

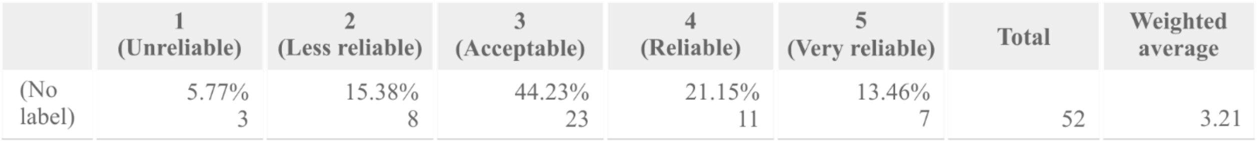
- Figure 3 gives the list of duplicate IMEIs as presented in a report by Qualcomm [b-7]. Based on Qualcomm analysis, the percentage of mobile devices on a given network varies and in general ranges from 10% to 25% (sometimes higher) depending on the geography.



1 IMEI to # of MSISDNs	IMEI #	% in total IMEIs	Associated MSISDN #	% in total MSISDNs
2	6, 844, 154	82. 38%	13, 688, 308	46. 68%
3	766, 402	9. 23%	2, 299, 206	7. 84%
4	252, 352	3. 04%	1, 009, 408	3. 44%
5	122, 110	1. 47%	610, 550	2. 08%
6	70, 169	0. 84%	421, 014	1. 44%
7	45, 941	0. 55%	321, 587	1. 10%
8	32, 802	0. 39%	262, 416	0. 89%
9	24, 353	0. 29%	219, 177	0. 75%
10	19, 333	0. 23%	193, 330	0. 66%
(10,20]	72, 089	0. 87%	1, 019, 234	3. 48%
(20,50]	37, 201	0. 45%	1, 153, 778	3. 93%
(50,100]	12, 582	0. 15%	869, 787	2. 97%
(100,200]	5, 110	0. 06%	707, 374	2. 41%
(200,500]	2, 322	0. 03%	676, 752	2. 31%
(500,1000]	499	0. 01%	343, 287	1. 17%
(1000,10000]	337	0. 00%	801, 569	2. 73%
(10000,50000]	26	0. 00%	568, 909	1. 94%
(50000,100000]	4	0. 00%	290, 205	0. 99%
(100000,)	8	0. 00%	3, 867, 261	13. 19%
Total	8, 307, 794		29, 323, 152	

Figure 3 – IMEI associated with multiple MSISDNs

- Pakistan Telecommunication Authority (PTA) has identified over 20 million non-standard IMEI and blocked them accordingly. As per PTA DIRBS impact case study, around 53 million IMEIs were blocked in 2019 of which 15 million were false IMEIs. Keep in mind that subscribers are more than that as this number only includes unique IMEIs which are duplicated as well [b-8].
- Response to Question 6 – "Do you think IMEI is reliable when identifying a mobile device"? of ITU-T SG11 Questionnaire on Reliability of IMEI [b-8] (see Figure 4 the results).



	1 (Unreliable)	2 (Less reliable)	3 (Acceptable)	4 (Reliable)	5 (Very reliable)	Total	Weighted average
(No label)	5.77% 3	15.38% 8	44.23% 23	21.15% 11	13.46% 7	52	3.21

QTR-RLB-IMEI(20)_F04

8 Impacts of tampered IMEI

- **Non-traceability of stolen handsets**: There is a grey market involved in the provision of IMEI reprogramming of mobile devices. Stolen mobile devices can be reprogrammed with genuine IMEI numbers already existing in the network. Even if a stolen IMEI number is blocked and the IMEI number is present in the blacklist of the EIRs of all telecom operators, it is difficult to identify the cloned devices present in the network and to recover the stolen devices and return them to the legitimate users.
- **Non-traceability of miscreants**: Mobile devices provide valuable intelligence and evidence to law enforcement agencies in preventing and detecting crimes. However, reprogrammed and duplicate IMEIs pose a challenge for law enforcement and security agencies as it is impossible to uniquely identify and trace targeted devices of miscreant users.

- **Restrict option of blocking IMEIs**: Although technically it is possible to block all mobile devices that have the same IMEI numbers present in the network, it also has the potential to block genuine users in possession of mobile devices with genuine original IMEI numbers. Thus, blocking or barring mobile devices that have the same IMEI numbers may invite complaints from genuine owners, including the filing of legal cases. Thus, blocking all devices with the same IMEI is challenging.
- **Lawful interception**: Some authorities decide to identify, and trace miscreants based on the mobile devices they use. In those cases, the IMEI number is used as the basis for lawful interception based on national rules and regulations. When the miscreant is using several new SIMs in the same mobile, interception through the IMEI is assumed to be the only option available. However, a problem arises when multiple instances of the same IMEI exist in the network. Intercepted content floods the lawful agency server. For example, if an IMEI with 1 800 instances is put under interception, it will be really difficult to identify the intended intercept target from the huge number of instances intercepted.
- **Tax evasion**: For countries that have implemented mobile devices control, tampered IMEI may be able to evade detection and impact on tax collection.
- **Conformance issues**: For countries where only compliant mobile devices can connect to the mobile network, mobile device with tampered IMEI may be able to evade detection and being recognize as a complying mobile device and allowed to connect to the mobile network, weakening the implementation of conformance requirements.
- **Mobile device theft** (and the associated violent crime): Combating mobile theft is a major priority for government and law enforcement agencies. To date, resale values of stolen mobile devices are quite lucrative as IMEI number re-programming has the potential to make stolen devices untraceable and free to operate on mobile networks.

9 Key weaknesses of IMEI

Although 3GPP TS 22.016 clearly mandates that IMEIs should not be changeable and resist to tampering, the specification does not indicate any details on implementation characteristics. Industry defined "IMEI Security Technical Design Principles" [b-2] to provide guidance to device manufacturers and to provide operators with a set of high-level criteria against which handset security can be assessed.

The nine principles on secure IMEI storing mechanisms (as detailed in clause 12.6), if implemented, are capable of protecting the IMEI against change. The view has been supported by the European Commission and EU member states, which were originally concerned about IMEI security, for the following reasons:

- Standardizing the technical means to protect the IMEI could expose devices to even greater risk if the prescribed safeguards are compromised as that would expose all devices if one method fits all.
- Currently, device manufacturers and chipset suppliers have different security implementations, some better than others, but mandating a single solution would most likely remove the enhanced level of protection offered by some manufacturers.
- The work to standardize a single solution, or even a small range of solutions, would be very difficult as every manufacturer would want their specific approaches to be adopted and that is unlikely to result in any consensus and could ultimately result in a race to the bottom to satisfy the ability of the less innovative manufacturers.
- By definition, standards are publicly available and describing how the IMEI is secured in mobile devices is likely to be welcomed by the hacker community but not likely to increase the security of the implementations.

- Standardizing IMEI security measures could stifle innovation and would be unlikely to take into account new and evolving attacks to which a standards-based response could be difficult, inflexible and slow.
- The usefulness of standards to deal with security matters is questionable as standards are optional and defining mandatory features in voluntary standards does not constitute a credible solution. This is evidenced by the fact that the standards already mandate that IMEIs must be non-reprogrammable after the point of manufacture, but this has not solved the problem. Adding more detail in terms of how this should be done is unlikely to yield better results.
- Investing in and improving IMEI security should be undertaken in the context of a broader industry effort to secure devices and develop anti-theft measures and these typically sit outside the standardization domain.

Device manufacturers invest different amounts of resources in device security, including IMEI security strength against tampering, with the result that each mobile device is likely to have different protections against IMEI change. Even if all legitimate manufacturers achieve acceptable levels of IMEI security in their products, problems will persist because producers of counterfeit mobile devices are never likely to invest in IMEI security as such investment runs contrary to their business model. Until such time as counterfeit devices are phased out from production, sale, and operation there will always be an issue with IMEI security.

There are four major reasons of IMEI being vulnerable for abuse and avoid detection:

i) **Manufacturer customer service**: Some device manufacturers, for various reasons, may have built capabilities into their products that allow the IMEI to be programmed after leaving the factory. This capability may weaken the security implementation of the IMEI, and generate increased risk pertaining to the storage and transport of relevant tools and security keys. These tools and security keys may, if leaked, enable technically competent users to conveniently reprogram the IMEI in mobile devices.

ii) **Lack of understanding on industry requirements**: As mobile devices became more commoditized and the cost of developing mobile devices decreased, some manufactures emerged that were not fully aware of the industry requirements to develop strong security around IMEI implementations, which may allow hackers to tamper with the IMEI easily. Sometimes, the changing of IMEIs by device users is allowed programmatically through the device's system menu.

iii) **Availability of unauthorized IMEI tampering tools**: Since there are different levels of security among mobile devices concerning IMEI tampering, unauthorized IMEI reprogramming tools inevitably become available for criminals to attack and modify the IMEI that has been implemented in mobile devices.

iv) **Intentional detection evasion**: As counterfeit mobile devices are manufactured and usually smuggled, their goal is to evade detection by consumers, mobile operators, and law enforcement agencies. These counterfeit mobile devices will never comply with legislation, policies and standards defined by governments, regulators, and industry bodies, as it runs contrary to their business model to minimize costs but failing to comply with industry and regulatory norms. Until all counterfeit mobile devices are removed from circulation, there will always be duplicated, malformed, or invalid IMEIs found in mobile networks.

10 Concerns on misuse of IMEI raised by Member States

10.1 Concerns of ITU Council-17

The important issue discussed in ITU Council-17 related to the misuse of IMEI. According to the 3GPP technical specifications and GSMA guidelines it was intended to ensure that the integration of IMEI in mobile devices at the time of manufacture would be done in such a way as to render the mobile devices unusable if their IMEIs were altered. This is a very serious problem, in socio-economic terms and, above all, in terms of security. The problem needed to be tackled through a combination of country programmes and international cooperation initiatives, with the aim of at least ensuring that IMEIs were non-erasable and non-reprogrammable.

As per the ITU Council-17, it was important to involve service providers, equipment manufacturers, national enforcement authorities and other interested parties in moves to resolve these issues. The importance of specific measures to implement regulations was specially discussed. All councillors agreed that the question could be taken on by TSB, to be included as part of the work done by Study Group 11, and that there should be collaboration for that purpose with GSMA.

While ITU-T Study Group 11 could come up with the technical means of preventing an IMEI number from being changed or tampered with, it would still need to be made obligatory for manufacturers at the country, regional or international level to do so. It would be helpful if the Council could adopt a resolution along those lines to ensure that the process was properly implemented.

10.2 Concerns of ITU Council-18

In line with the proposal in clause 10.1, GSMA collected data and took targeted action, but GSMA was also aware that implementation was patchy. ITU had adopted various resolutions dealing with the impact of counterfeit devices, and ITU-T should therefore ask GSMA for more information and for timelines. Noting that Resolution 97 (Hammamet, 2016) gave ITU-T a mandate to address tampering and non-reliability of unique identifiers, it was requested that TSB take action in that regard and report back to Council-19. TSB could draw on the summary record of the present meeting for guidance in that respect.

Tampering with unique telecommunication device identifiers was a challenge faced by all members and an especially critical issue for developing countries. Rather than develop new unique identifiers, steps should be taken to guarantee that existing identifiers could be securely stored on devices and rendered tamper-proof, and to implement means of detecting clones and differentiating them from genuine devices. Moreover, projects to build databases to store the IMEIs of mobile handsets and thereby prevent counterfeiting –would fail if the IMEI numbers changed or were duplicated. ITU-T Study Groups, in particular Study Group 11, should therefore continue to develop Recommendations, Technical Reports and guidelines to address the problems posed by counterfeits, in accordance with Resolutions 96 (Hammamet, 2016) and 97 (Hammamet, 2016).

Resolution 97 resolved that "ITU-T should, in collaboration with the relevant standards organizations, develop solutions to address the problem of duplication of unique identifiers".

10.3 Consolidation of the existing concerns

1) Misuse of IMEI.

2) Tampering with unique telecommunication device identifiers is a challenge faced by all members and an especially critical issue for developing countries.

3) Projects to build databases to store the IMEIs of mobile devices and thereby prevent theft would fail if the IMEIs changed or were duplicated.

4) Steps should be taken to guarantee that existing identifiers could be securely stored on devices and rendered tamper proof, and to implement means of detecting clones and differentiating them from genuine devices.

5) The problem needs to be tackled through a combination of country programmes and international cooperation initiatives, with the aim of at least ensuring that IMEIs were non-erasable and non-reprogrammable.

6) Resolution 97 (Hammamet, 2016) gave ITU-T a mandate to address tampering and non-reliability of unique identifiers.

Study Group 11 should therefore continue to develop Recommendations, Technical Reports and guidelines to address the problems posed by counterfeits, in accordance with Resolution 96 and Resolution 97 (Hammamet, 2016).

11 Issues with IMEIs

Storage of IMEIs in a non-editable area is the ideal solution to make IMEI implementations secure, but practical feasibility on mandating this to all the mobile manufacturers globally needs to be considered.

11.1 Stolen/lost mobiles

To remove the traceability and blacklisted status of lost/stolen mobile devices the IMEI is re-programmed. The solution is to encourage reporting of stolen mobile devices through accessible and readily available channels.

11.2 Lack of effective implementation/enforcement of law and regulation

In some countries, there are national legislations or policies specifically criminalizing the unauthorized reprogramming of IMEIs in mobile devices. IMEI re-programming is an illegal activity and punishment for this unlawful activity is also defined. IMEI security is becoming more serious and critical day by day and due priority is to be given to the enforcement of these regulations in all countries.

11.3 IMEI re-programming with same TAC code

It is a challenge to detect IMEI re-programming if the mobile device IMEI is modified with a TAC of the same make and model. If the IMEI is not already in use, then it is very difficult to identify the reprogrammed device as duplicate or counterfeit.

12 Approaches to improve IMEI reliability

To overcome the IMEI reliability issues discussed above, the following options have been identified, which could be implemented nationally and internationally.

12.1 Public awareness

Consumers may not be aware if the mobile device they are purchasing contains an IMEI that has been changed. Performing a check against an IMEI checking service may indicate a problem if the response from the service, on entry of the IMEI, displays that IMEI is invalid or belongs to a different device make and model from the one the consumer believes he/she is purchasing.

Public awareness campaigns mainly through TV, newspaper, social media, SMS and radio announcements to promote public awareness of the existence and dangers of mobile devices with modified IMEIs could be helpful.

12.2 Conformity assessment process for market entry

If feasible, a conformity assessment process for mobile devices, that includes a declaration on compliance levels with the industry defined IMEI Security Technical Design Principles, may increase the reliability of IMEIs as additional efforts may be made by manufacturers to increase IMEI security levels.

12.3 Criminalize IMEI tampering

Legislation and policy may be enacted to criminalize the unauthorized reprogramming of IMEIs or the development, distribution and possession of tools that facilitate IMEI reprogramming. This could help reduce the chance that IMEI tampering tools are publicly available.

12.4 Rating of mobile device or manufacturer

Security is not generally a consumer's priority when choosing mobile devices, and the general public may not have the understanding required to evaluate and differentiate between the security implementations across mobile devices. A mobile device IMEI reliability index may facilitate customers to understand how reliable the mobile device is. If the IMEI reliability index for individual mobile device models could be established and publicized, it could incentivize consumers to purchase mobile devices with higher IMEI reliability index, thus incentivizing manufacturers to invest in IMEI security.

The IMEI reliability index could also be used for conformity assessment and compliance.

12.5 Increasing the reliability of IMEI implementations to make reprogramming harder

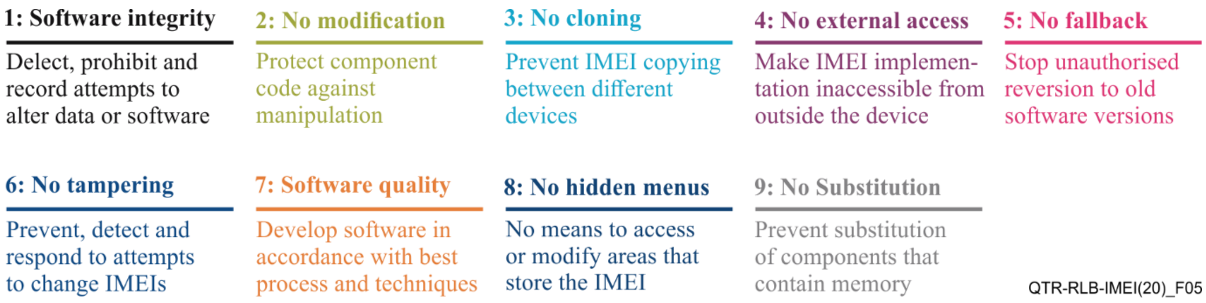
Device manufacturers are required to make the IMEI tamper proof by adopting different techniques such as storing the IMEI in different hardware components, preferably in trusted execution environments, using best in class encryption, and other security enhancing techniques. In case of any change to the IMEI, the change information can be sent to the device manufacturer for tracking purposes.

12.6 Adopting and improving IMEI security principles

GSMA, with the support of the world's leading device manufacturers, has been working on IMEI security for many years as it recognizes that the effectiveness of device blocking on mobile networks is dependent on the secure implementation of device identities. Although the mobile standards require that device identities should not be capable of being changed after the point of manufacture, it became apparent over a number of years that identities were being changed with relative ease. This had the effect of jeopardizing industry efforts to combat device theft as identities could be changed on stolen devices from the original identities that had been blocked thereby bypassing the action taken by network operators. That necessitated a concerted industry effort to consider what could be done to improve the mobile device security landscape. Significant efforts were made to improve the situation with real commitment and engagement by the device manufacturing community and these led to a series of initiatives that have been central to improved device identity security levels.

Although the standards clearly provide that IMEIs should not be reprogrammable, there is no strict rule for mobile manufacturers to secure IMEIs when supplying devices to individual countries. As a result, some manufacturers do not take effective precautions to make the IMEI reliable. To resolve the reliability of IMEIs permanently, in cooperation with the mobile device manufacturers, there is a need to establish globally applicable requirements in that manufacturers can follow them to make IMEI non-reprogrammable in all future mobile devices.

Mobile device manufacturers have made some effort to reduce reprogramming. The mobile industry's trade association, GSMA published "9 principles", as illustrated in Figure 5, to encourage manufacturers' security concerns.



1: Software integrity
Delect, prohibit and record attempts to alter data or software

2: No modification
Protect component code against manipulation

3: No cloning
Prevent IMEI copying between different devices

4: No external access
Make IMEI implementation inaccessible from outside the device

5: No fallback
Stop unauthorised reversion to old software versions

6: No tampering
Prevent, detect and respond to attempts to change IMEIs

7: Software quality
Develop software in accordance with best process and techniques

8: No hidden menus
No means to access or modify areas that store the IMEI

9: No Substitution
Prevent substitution of components that contain memory

QTR-RLB-IMEI(20)_F05

Figure 5 – Principles for IMEI security

Changes in IMEI security are monitored via an "IMEI Security Weakness Reporting and Correction Process", which involves confidential bilateral engagement between GSMA and the manufacturers of devices in which the security of IMEI implementations has been compromised. The confidential and trusted nature of the engagement ensures that the reported security issues can be comprehensively discussed and addressed without sensitive product security details being unnecessarily disclosed.

13 Approaches to improve IMEI reliability

To resolve and minimize the impact of the issues related to IMEI weaknesses, a system can be deployed to help detect reprogrammed mobile devices and restrict their use in mobile networks.

13.1 IMEI authentication

Typically, during the manufacture of devices a device key is imprinted that can later provide attestation towards a remote entity. As part of this device personalization, the IMEI is typically recorded (with other applicable device identifiers, such as a SoC unique identifier). This means when a device signs a statement a remote entity can later use a device certificate (typically ITU-T X.509) to verify the device's assertion and also reference the device's IMEI. This means a network can cryptographically ensure that the IMEI has not changed on a device since it was manufactured.

This could be coupled to device registration when the device attempts to connect to a network and the network EIR could perform the following actions:

- Check if the IMEI is blacklisted.
- Pass down a cryptographic nonce to the device that it signs with the key personalized during manufacturing and provide this to the network for proof of ownership. The EIR then obtains the device certificate corresponding to the IMEI the mobile device used for network registration and verifies it. If it matches, the network knows the IMEI presented by the device matches what was originally implemented during manufacturing. This means that the IMEI has not changed and the device claiming this IMEI cannot be subverted as the imposter device lacks the corresponding key used to assert this.

This suggested approach is yet to be implemented and would require additional work to be done by industry to mandate that devices must pass asserted IMEI binding before being granted network access. This is an example of how pairing between a device and a network could happen to ensure the IMEI has not been changed since manufacturing and other approaches could also be considered.

Coupling IMSI or MSISDN data with the IMEI is already happening but it is preferable that an attestation should be used to verify a device as it provides a cryptographic binding (which thus makes it harder to duplicate). This also means only one device can own an IMEI as it was recorded and stored during manufacturing and that assurance that no other device can correctly claim the same handset identifier confers many benefits.

13.2 Responses to ITU-T SG11 Questionnaire on the reliability of IMEI

Some different approaches are quoted on the responses received to the ITU-T SG11 Questionnaire on the reliability of IMEI, that was circulated to all ITU Members in November 2019 [b-8].

Bibliography

[b-3GPP TS 22.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 version 3.1.0 Release 1999).*

[b-3GPP TS 23.003] ETSI TS 123 003 V15.7.0 (2019-07), *Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 15.7.0 Release 15).*

[b-TS.37] GSMA TS.37 Requirements for Multi SIM Devices <https://www.gsma.com/newsroom/resources/ts-37-prd-requirements-multi-sim-devices/>

[b-1] GSMAI MEI Allocation and Approval Process <https://www.gsma.com/newsroom/wp-content/uploads//TS.06-v17.0.pdf>

[b-2] GSMA IMEI Security Technical Design Principles <https://www.gsma.com/publicpolicy/wp-content/uploads/2017/06/IMEI_Security_Technical_Design_Principles_v4.0.pdf>

[b-3] Al-Zarouni, M. (2007), *Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics*.

[b-4] Vodafone Article: <http://m.ghheadlines.com/agency/myjoyonline/20150305/39216420/50-of-phones-have-been-cloned-vodafone>

[b-5] ITU Workshop on global approaches on combating counterfeiting and stolen ICT devices (2018) <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/6_Rustam%20Pirmagomedov.pdf>

[b-6] ITU-D SG 2 Workshop on Combating Counterfeit ICT devices, control system in Colombia <https://www.itu.int/dms_pub/itu-d/oth/07/12/D07120000060001PDFE.pdf>

[b-7] ITU-T Technical solutions to address falsification of uninque indentifiers to combat device counterfeiting and theft <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/Raheel_Kamal_Ne.pdf>

[b-8] ITU-T SG11 Questionnaire on Reliability of IMEI document –
TSB Circular 207.

[b-9] https://security.stackexchange.com/questions/84542/is-there-a-reason-why-imei-is-stored-in-eeprom

[b-10] https://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Final%20Report/Summary-of-Discussions-18Dec2014.docx

[b-11] http://spotafakephone.com//docs/eng/MWF%5FCounterfeit%5FInfographic %2Epdf

[b-12] https://www.thenewsminute.com/article/imei-cloning-karnataka-watch-out-your-phone-may-not-be-unique-32570

[b-13] https://www.firstpost.com/tech/news-analysis/1300-cases-of-imei-cloning-found-in-india-between-2009-2012-3616085.html

[b-14] https://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Final%20Report/Summary-of-Discussions-18Dec2014.docx

[b-15] https://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Final%20Report/Summary-of-Discussions-18Dec2014.docx

[b-16] https://www.thehindubusinessline.com/2002/10/17/stories/20021017023103 00.htm

[b-17] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Documents/PPT/S1P3_D_Protsenko.pdf

[b-18] http://www.techsmart.co.za/business/New-tricks-needed-to-stop-the-45-Billion-counterfeit-smartphone-Market

[b-19] https://guardian.ng/technology/counterfeiters-threaten-n612-billion-yearly-revenue-from-ict/

[b-20] https://www.ficcicascade.in/wp-content/uploads/2018/07/Mobile-final.pdf

[b-21] Survey report on counterfeit ICT devices in Africa region – T-TUT-CCICT-2017-MSW-E

[b-22] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/Presentation%20LAST.pdf

[b-22] https://www.gsma.com/publicpolicy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf

[b-23] http://dot.gov.in/sites/default/files/2018_09_13%20Sec%20IMEI%20Certificate.pdf

[b-24] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20170405/Documents/S1_6.%20SG11_AF_Workshop_Counterfeit_Zanon_v01.pdf

[b-25] https://www.gsma.com/services/gsma-imei/imei-blacklisting/

[b-26] https://link.springer.com/article/10.1057/palgrave.cpcs.8150060