International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Q

Supplement 75

(12/2021)

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

Use cases on the combat of counterfeit ICT and stolen mobile devices

ITU-T Q-series Recommendations – Supplement 75

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 PEER-TO-PEER 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.

Supplement 75 to ITU-T Q-series Recommendations

Use cases on the combat of counterfeit ICT and stolen mobile devices

Summary

This Supplement 75 to the Q-series Recommendations collects use cases provided by ITU members that reflect the challenges, opportunities and results in combating counterfeit information and communications technology (ICT) and stolen mobile devices and aims to assist new members in engaging better with this problem.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q Suppl. 75	2021-12-10	11	11.1002/1000/14885

Keywords

Challenges, counterfeit, duplicate IMEI, stolen mobile devices, tampering, use cases.

* 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

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.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 75 to ITU-T Q-series Recommendations

Use cases on the combat of counterfeit ICT and stolen mobile devices

1 Scope

This Supplement collects use cases provided by ITU Members that reflects challenges, opportunities and results on the combat of counterfeit ICT and stolen mobile devices.

2 References

The following ITU-T and other references contain provisions which, through reference in this text, constitute provisions of this Supplement. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Supplement 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 Supplement does not give it, as a stand-alone document, the status of a Recommendation.

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

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

[ITU-T TR-Counterfeit] ITU-T Technical Report (2014), *Counterfeit ICT Equipment*. http://www.itu.int/pub/T-TUT-CCICT

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloned identifier [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.

3.1.2 counterfeit ICT device [ITU-T Q.5050]: An information and communication technology (ICT) device that explicitly infringes the trademark, copies hardware or software designs, or infringes brand or packaging rights of an original or authentic product and, in general, infringes applicable national and/or international technical standards, regulatory requirements or conformity processes, manufacturing licensing agreements, or other applicable legal requirements.

3.1.3 invalid identifier [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 a responsible management entity.

3.1.4 reliable unique identifiers [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.

3.1.5 tampered ICT device [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.

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

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

EIR Equipment Identity Register

ICT Information and Communications Technology

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

SIM Subscriber Identification Module

TAC Type Allocation Code

5 Conventions

None.

6 Introduction

Appendix I collects use cases of different countries, and Appendix II lists use cases provided by private sector and NGO initiatives.

Appendix I

Use Cases

I.I Africa

I.I.I Congo

1 Introduction

Combating counterfeit goods has become a global necessity and priority in order to protect innovations, intellectual property and inventions.

Several strategies for combating counterfeiting have been highlighted in Recommendations [ITU-T Q.5050] and [ITU-T Q.5051].

As research continues into ways to stem the scourge of counterfeit devices affecting the Member States, we propose using a central equipment identity register (CEIR) system to notify mobile network operators and consumers about counterfeit devices.

2 Common statistics for a country's use case

The Democratic Republic of the Congo is situated at the heart of the central sub-Saharan region of Africa and is bordered by nine other countries: the Central African Republic and Republic of the Sudan to the north, Uganda, Republic of Rwanda, Republic of Burundi and United Republic of Tanzania to the east, Republic of Zambia and Republic of Angola to the south and the Republic of the Congo to the west.

– Surface area: 2 345 000 km

– Population: more than 81 000 000 inhabitants, of whom nearly 70 per cent live in large urban areas, such as Kinshasa, Lubumbashi, Mbuji-Mayi and Kisangani.

3 Analysis

The implementation of the recommendations contained in the framework for solutions to combat counterfeit ICT devices ([ITU-T Q.5050]) and the framework for combating the use of stolen mobile devices ([ITU-T Q.5051]) poses serious problems, particularly as interpretation differs from country to country.

All Member States are unanimous on the need to combat ICT counterfeit goods. It is, however, important to establish a mechanism that combats such goods without inconveniencing consumers, who are a significant market for mobile network operators and sellers of ICT equipment.

By blocking counterfeit mobile devices, network operators make it difficult for consumers themselves to recognize counterfeit devices. This procedure also does more harm than good as it leads to a greater number of legal complaints.

In that regard, we have chosen to have mobile network operators send a message or notification to consumers to inform them of the status of their device as part of the efforts to combat counterfeiting.

4 CEIR system and consumer notifications

Recommendations [ITU-T Q.5050] and [ITU-T Q.5051] provide several approaches for combating counterfeit ICT products, including the blocking of counterfeit telephones.

As the international mobile equipment identity (IMEI) codes serve as the reference database for mobile devices and provide the white, grey and blacklists for the CEIR system, it is important that all Member States work to provide automatic SMS notifications for counterfeit devices that are in circulation.

The use of automatic notifications enables consumers to remain up to date about the type of mobile device owned.

By notifying consumers of the status of their mobile devices via the CEIR system, mobile network operators enable consumers to prepare to switch to a genuine device following a moratorium, i.e., to be established by the competent authorities.

Mobile telephone blocking should be used only where consumers refuse to comply with the decisions taken or with any moratorium put in place by the competent authorities following an awareness-raising campaign.

The use of notifications also alerts consumers to the existence of counterfeit devices and allows everyone to help combat this economically destructive practice.

5 Experience of the Democratic Republic of the Congo

To combat counterfeit ICT products, the Ministry of post, telecommunications and new information and communication technologies of the Democratic Republic of the Congo issued a ministerial order for the establishment of a CEIR system in 2020.

This system aims to limit the market for counterfeit mobile devices. Its introduction was accompanied by the creation of a central database of IMEI numbers.

6 Roadmap of the future planned evolution of a use case

Mobile network operators should send automatic messages to consumers to notify them of the status of their devices.

7 Conclusion

Counterfeiting is a practice that destroys the benefits of research and undermines the protection of innovations, intellectual property and inventions.

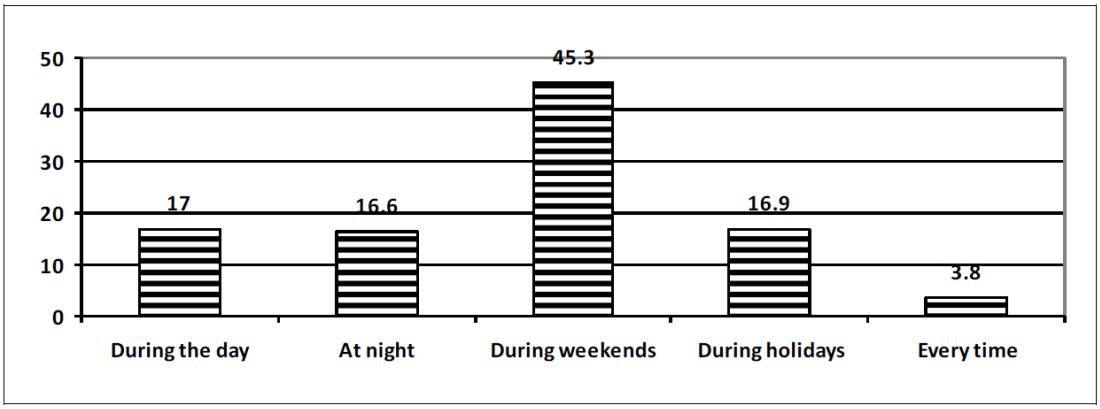
We all have a duty to combat this scourge by using new information and technology techniques to achieve a noticeable reduction in the production of counterfeit goods worldwide.

I.I.II Republic of Botswana

Overview of the situation

Botswana has a population of just above 2 million and there are three (3) mobile operators, however, the regulator continues to receive an influx of complaints on the poor quality of service provision (some of which emanate from the networks and some from the gadgets used by the users to access the services). In 2013, ITU reported that the Republic of Botswana had the highest mobile penetration rates in the southern African region; with the mobile cellular networks combined and covered more than 90 % of the population and the mobile subscriber identification module (SIM) penetration standing at 162 % by September 2016.

In 2015, BOCRA commissioned the Botswana institute for development policy analysis (BIDPA) to carry out the first customer satisfaction survey for the services it regulates. The survey results for mobile network performance for different times throughout the day were as follows: 71 % of the users of mobile services indicated that they had a problem connecting to the network while 29 % said that they did not. Refer to the Figure I.1 for the summary of the results. The survey however, did not cover the network key performance indicators.



Source: Author computed from survey

Figure I.1 – Times of having problems connecting to the network[1]

Measures taken

The Communications Regulatory Authority Act of 2012, (CRA Act of 2012) is an act that provides all licensees manufacturers, distributors and suppliers shall type approve all their electronic communicating devices connecting to the public network. Awareness was raised to all the relevant stakeholders and consumers and regular enforcements are being conducted throughout the years. However, the country and/or the region do not have a testing laboratory to test the mobile devices and other devices during the type approval process. The regulator, however, relies on the documentation provided by the manufacturers and distributors/suppliers. The absence of the testing equipment is a clear indication that there are plenty of these devices in the country, evidenced by the reports that are received on a daily basis concerning the gadgets themselves and the complaints on the poor quality experienced. BOCRA in the quest to address issues of poor QoS/QoE procured a QoE emulation monitoring system.

I.I.III Chad

Overview of the situation

In Chad, ARCEP does not yet have control over the equipment importation especially the mobile devices so as not to be able to identify their origin.

Moreover, despite the issue of a decree N°036/MPNTIC/SG/11 dated the 10/11/2011 related to the equipment type approval procedures, the country still does not have a testing laboratory and is similar to Botswana, the regulator relies on the documentation provided by the manufacturers and distributors/suppliers.

Due to the lack of this procedure between the customs and the regulator, the counterfeit mobile devices used in their market is increasing exponentially and the proliferation of mobile phone black markets is also being observed.

In this context, the existence of those devices in the mobile networks and the markets impacts the users in terms of health and the quality of experiences, the government in terms of taxes not collected, the mobile networks in terms of quality of services and network performances.

Measures taken

To identify the origins of the mobile phones and to find the proportion of counterfeit devices in the market and evaluate their impacts on the QoS/QoE, ARCEP conducted a survey in N'Djamena.

The concerned entities were: authorized (25) or non-authorized (30) vendors, customs agents (20), mobile users (50), type approval agents (5).

---

1 http://www.bocra.org.bw/sites/default/files/documents/Final_Report_BOCRA_Cust_Satisfaction.pdf

The adopted method of survey was face-to-face questionnaires, and it included the three existing mobile operators: Airtel, Tigo, Salam.

The results are as follows:

Subjects of the survey	Interviewed	Results
Importation rate of mobile handsets:	Authorized and non-authorized vendors	100 % of mobile handsets were authorized and non-authorized vendors that were imported, that they interviewed.
The need for import entitlements	Authorized and non-authorized vendors	100 % of authorized vendors require this entitlement 0 % of non-authorized vendors require this entitlement
Customs clearance costs for mobile handsets	Authorized vendors Non-authorized vendors	32 % find it expensive, 44 % have a problem with the costs and 24 % find it affordable 10 % find it very expensive; 73, 3 % find it expensive; 16, 7 % find it affordable.
The place to buy the mobile handsets	Mobile users	50 % buy it through authorized sellers 26 % buy it through non-authorized and the 24 % don't care where to buy it as long as the prices suit them.
The criteria of choice of the handsets	Mobile users	44 % choose to buy a handset as long as it is not a Chinese handset 30 % choose to buy a handset according to its quality 22 % choose brand products 8 % choose the cheapest handsets
Type of chosen mobile phones	Mobile users	56 % = Android phones 30 % = 2G only phones 14 % = choose the simplest ones (to be used for voice call and messaging)
Usual purchased brands	Mobile users	Samsung = 34 %; Techno = 30 % iPhone = 18 %; Apple = 12 % Others = 6 %
Negative impacts of mobile terminals	Authorized vendors Non-authorized vendors	– Impact on health because of the electromagnetic fields – Impact on environment – Injuries when they explode – Network degradation (e.g., multiple sims) – 42 % confirm that mobile handsets can have bad effects on users but without giving any details – The remaining percentage did not offer any opinion

I.I.IV Republic of Ghana

The Ghanaian regulator i.e., the national communication authority (NCA) is mandated by law to certify and ensure the testing of the communications equipment for compliance with international standards and environmental health and safety standards including electromagnetic radiation and emissions. As a result, the NCA has established the device type approval testing laboratories (RF and signalling for performance and protocol testing) and SAR (for safety) and aims at checking conformance and combating ICT device counterfeiting. Any ICT device manufactured or imported into Ghana must be tested and type approved either in the NCA laboratories or at any other laboratories recognized by the authority.

In order to efficiently operate the labs and curb the influx of counterfeit devices, the NCA has also teamed up with the Ghana standards authority and the Ghana customs to conduct both physical port inspection and market surveillance. Port inspection involves the random picking of samples of electronic communications equipment at any of Ghana's ports of entry to test and certify at the laboratory before the consignment is released to the importer.

In the case of market surveillance, the regulator enters the market at any time and picks samples of the electronic communications equipment that has been type approved for testing. This is to ensure that samples tested and approved are of the same quality as the ones placed on the market.

The regulator will also be requiring labelling for equipment that has been type approved. The equipment will have unique identifiers on the label and other security features.

Ghana is in the process of gaining access to the GSMA IMEI database to help combat counterfeit ICT devices.

I.I.V Guinea

The Ministry of posts, telecommunications and the digital economy, acting through the *Direction Nationale des Télécommunications*, initiated a study/survey to gather information on the difficulties encountered, different utilizations and the efforts that are in place for remedying the problem of counterfeit ICT devices.

Survey report

All the information gathered in the survey made it clear that, despite the existence of Law L 018/2015/AN on 13 August 2015 and its Article 64 on the **type approval and homologation of telecommunication/ICT devices** (53.79 per cent of those surveyed were unaware of its existence) and a consumers association in the telecommunication/ICT sector (unknown to 71.69 per cent of those surveyed), an enormous amount of work still remains regarding the oversight of markets, as the aforementioned law has neither been widely disseminated nor applied effectively.

The report also indicates that the counterfeit products sold most on Guinean markets are the mobile phones (66.70 per cent according to those surveyed), chargers (67.36 per cent according to those surveyed) and earphone devices (66.91 per cent according to those surveyed). With the low incomes earned by Guineans – around USD 2 per inhabitant – most of the population prefer these counterfeit products as they can afford them.

Lastly, the report indicates that virtually all these counterfeit products flooding the Guinean markets come from Asia (92.76 per cent according to those surveyed).

I.I.VI Republic of Kenya

a) Background

Kenya's robust mobile industry has had a positive and significant impact on the socioeconomic indicators of the country leading to the emergence of new innovative businesses such as mobile agents and deepening of the financial sector with notable innovations such as mobile money transfers and accounts.

This growth has also had its fair number of challenges, one of which is the complex matter of illegal mobile devices. In an effort to tackle this menace, the communications authority (CA) of Kenya, through engagement and partnership with stakeholders, has developed and implemented several regulatory interventions.

It is important to note that the concern initially began with stolen mobile devices, but the matter has progressively become more complex with the cloning of the international mobile equipment identity (IMEI) becoming more rampant and the rising cases of SIM swap fraud and SIM box.

As of September 2018, Kenya has had 45 million mobile subscribers against an estimated population of 48 million inhabitants.

b) Regional initiative – interconnected equipment identity registers (EIRs)

In 2005, CA together with the other regulators within east Africa initiated a project to install equipment identification registers (EIR) through the east African regulatory, posts and telecommunications organization (EARPTO), the precursor of the east African communications organization (EACO). Each mobile operator operating in the east African region was required to install an EIR and its blacklist reported the number of stolen devices, and the information was shared with the other operators within the region. The aim was to ensure that no stolen device would have access to mobile services within east Africa. The challenge of this initiative, which still exists today, is that the authority cannot enforce denial of services outside its jurisdiction.

c) 1555 IMEI verification service

By 2012, the mobile industry was facing a new challenge in the proliferation of counterfeit and substandard devices. The authority, thus, engaged industry stakeholders and relevant government agencies in an effort to manage the proliferation of illegal mobile communications devices. The providers of mobile services involved in the project included mobile operators and mobile equipment vendors.

This particular effort led to the denial of services to all mobile devices, which had non-standard international mobile station equipment identity (IMEI) as defined in the GSMA IMEI type allocation code (TAC) database. More than 1.5 million devices were switched off at this stage. It is to be recalled that consumer organizations were up in arms with the authority due to the switch-off. The consumer organizations argued that consumers had no way of knowing if a device was genuine or not. To this end, an SMS based solution for verifying genuine mobile devices dubbed, "1555" was setup to assist consumers in the identification of genuine devices. However, this initiative was quickly defeated as unscrupulous backstreet vendors began cloning genuine IMEIs.

The 1555 initiative had anticipated the possibility of cloning of devices and recommended a phase II on the management of illegal mobile devices where a system was to be setup to detect cloned devices.

As of September 2017, the service recorded 16 644 802 IMEI verification requests out of which, 11 261 843 were traceable to the GSMA IMEI TAC database. An additional task in the 2nd phase was to tame the proliferation of SIM boxes.

d) National IMEI whitelist solution

In 2015, CA began the second phase of the management of illegal mobile devices based on a national IMEI whitelist solution to detect illegal mobile communications devices and isolate them into a blacklist.

All mobile operators will be required to connect to the national IMEI whitelist and ensure devices on the blacklist do not access mobile services.

The targeted illegal communications devices include:

i) Sim boxes;

ii) Counterfeit devices;

iii) Substandard devices; and

iv) Stolen/lost devices.

CA is cognizant that many Kenyans either knowingly or unknowingly are utilizing illegal devices to access mobile services. Therefore, devices falling under ii) and iii) above, which are in use before the implementation of the solution, shall continue to access mobile network services until their natural life-cycle comes to an end. This decision also offers multiple advantages such as avoiding disconnection of many innocent consumers, mitigating potential opposition by consumer organizations on account of consumer rights, and reduction on the potential negative impacts on mobile operator revenues. Furthermore, the decision does not derail the long-time objective of the project to manage mobile devices going forward.

This is also in line with the Technical Report on counterfeit ICT equipment dated 21 November 2014 on page 23 [ITU-T TR-Counterfeit].

"…if regulators and governments choose to put in force terminal blocking actions, it is important to adopt transition policies, such as starting by blocking only new terminals and allowing devices that are already on the network to continue to operate but, ultimately, users will have to move to genuine terminals since the estimated life cycle of a mobile terminal is…".

e) Identification of illegal devices

The solution shall utilize three (3) unique features to identify a user and the mobile communications device that is used:

i) the international mobile station equipment identity (IMEI);

ii) the international mobile subscriber identity (IMSI); and

iii) the mobile station-ISDN number (MSISDN).

I.I.VII Republic of Madagascar

Overview of the situation

Having experienced technical problems affecting QoS caused by counterfeit terminals, mobile telephone operators in Madagascar recently brought the matter to the attention of the regulator during the QoS/QoE workshop organized in October 2017 by ARTEC and ITU.

According to the data, over 25 per cent of mobile phones used in the existing mobile telecommunication networks of Madagascar are either counterfeit or non-compliant.

It is, thus, clear that the use of such terminals in networks has a negative impact on QoS/QoE parameters and forces operators to over-invest in the optimization measures. As a result, appropriate action needs to be taken to reduce the percentage to zero. This step must not, moreover, be overlooked, given the objective of improving network service quality and obtaining reliable, uncorrupted, and consistent data for QoS and QoE indicators.

Apart from the complaints received from the operators and from users, ARTEC does not have the technical skills to identify and clearly manage the issues linked to counterfeit devices in the QoS/QoE among all the other network issues.

Measures taken

Madagascar has taken a step in this direction with the publication of its ministerial decree 890/2018 of 17 January 2018, defining the restrictive measures relating to mobile phones that are counterfeit, stolen or non-compliant with international norms.

In the long term, this measure aims to ban the import and use of terminals with invalid IMEI numbers on Malagasy territory. The deadline set by the decree was 30 June 2019.

I.I.VIII Federal Republic of Nigeria

The Nigerian communications commission (NCC) was established by the Acts of parliament which mandates the NCC to ensure that all CIT devices to be shipped into Nigeria; to be sold in Nigeria and or deployed on the network must go through the process of equipment authorisation based on the NCC type approval guidelines.

The type approval procedure is based on the submission of type approval application based on the test reports listed below:

The test reports listed below have been identified as generally acceptable for type approval of mobile devices in Nigeria:

- EMC test report from an accredited laboratory
- Safety test reports from an accredited laboratory
- SAR test reports from an accredited laboratory
- RF test reports from an accredited laboratory

Currently, the RF conformance test system is in the process of being established in order to validate and support the type approval process in Nigeria. However, tests conducted based on the categories of the above enumerated tests are acceptable for type approval of genuine mobile devices and any mobile device that fails to go through successfully can be defined as either a non-conforming or counterfeit mobile device.

The final output of the type approval process is the type approval certificate/grant with a unique NCC identifier which can be used as a label to tag type approved mobile devices. The commission is currently working on a directive to ensure that all type approved mobile devices are labelled with the NCC identifier.

NCC also conducts surveillance, compliance monitoring and enforcement activities with the main objective of combatting the influx of counterfeit mobile devices into Nigeria. During the type approval process, test reports verification is also carried out when in doubt of such test reports. Equipment audits at the operator's centre to identify genuine products are also being carried out, also when there is a doubt about the quality assurance (QA) of mobile devices, a factory/laboratory audit is also conducted.

The above activity has solved the challenge of counterfeiting but not holistically and hence the search for other solutions continues in addition to the above highlighted equipment authorisation procedure. The NCC organises sensitisation workshops for identified stakeholders in order to collaborate with them on combatting counterfeiting and to ensure that only type approved mobile devices are imported into Nigeria. The identified stakeholders are the Nigerian customs, standards organisation of Nigeria, original equipment manufacturers, equipment vendors and licensed operators in Nigeria and type approval consultants among others.

With the increasing number of counterfeit ICT devices especially in mobile phones, regulators and operators globally are faced with the challenge of finding a full proof solution to prevent the deployment of such devices on the network which if/when allowed can lead to the degradation in the network quality of services and subscribers quality of experience. More so, higher dropped calls have been observed as a result of the deployment of counterfeit mobile devices. Some of them if fully charged have very short battery talk time and standby time and can even get extremely hot with risk of explosion if care is not taken. Hence the issue of safety arises. Based on the foregoing, the NCC is currently seeking a solution that will be based on the IMEI. The issue of cloned IMEI numbers and stolen mobile phones that can lead to tampering with the IMEI number, with the aim of changing the identity of the stolen mobile device has brought to the fore the need for the NCC to seek a solution that will block such mobile devices from latching onto the network. Also, duplication of IMEI numbers portends a serious security challenge which throws up the challenge of the original mobile

device user or owner. All these have motivated the NCC to search for a mobile device management system.

I.I.IX Republic of Senegal

In addition to effectively combating piracy, counterfeiting and the theft of telecommunication/ICT devices, and taking steps to adapt to changes in the legal environment, the Government of Senegal has undertaken important initiatives in collaboration with continental and intercontinental communities, multinationals, telecommunication and ICT regulators and Internet service providers (ISPs) to fight against this modern scourge, which is an obstacle to technological innovation, job and wealth creation and foreign direct investment.[2]

Senegal has put in place measures of a legislative and regulatory nature and taken other steps to improve the protection of individual property, including:

– a legislative framework based on a series of laws;
– a regulatory framework based on a series of decrees;
– a national brigade for combating piracy and counterfeiting;
– the Senegalese agency for industrial property and technological innovation;
– the regulatory authority for telecommunications and posts (ARTP);
– the national customs authority;
– the involvement of national and multinational manufacturers and distributors of telephones, tablets, smartphones and decoders.

I.I.X United Republic of Tanzania

Introduction

The Tanzania communications regulatory authority (TCRA) is a government body responsible for regulating the communications and broadcasting sectors in Tanzania. It was established under the Tanzania Communications Regulatory Act No.12 of 2003 to regulate the electronic communications, and postal services, and management of the national frequency spectrum in the United Republic of Tanzania.

Section 83 of the Electronic and Postal Communications Act, 2010 (EPOCA 2010) mandates TCRA to conduct type approval of all electronic communication equipment before being used for connection to any electronic communications network to receive and, or transmit electronic communication signals.

In conducting type approval of communication equipment, TCRA is guided by either technical standards formulated and published by the national, regional or the adopted international standards. In conducting type approval, TCRA is also guided by the electronic and postal communications (electronic communications equipment standards) regulations, 2018 and type approval guidelines. TCRA is responsible for formulating technical standards related to electronic communications services and maintaining the database of all communications equipment authorized for use in the United Republic of Tanzania.

The equipment manufacturers, for every electronic communication equipment or device, need to declare that the equipment conforms to international and national standards before the equipment is approved for use in the country.

In order to curb substandard and counterfeit electronic communication devices, TCRA does conduct periodical surveillance in the market. Any person who uses any non-type approved electronic

[2] ITU-D SG2 Document SG2RGQ/66 from Senegal [in French]

communications equipment commits an offence, and upon conviction is liable to a fine not less than five million Tanzanian shillings or an imprisonment term not less than six months or both.

Central equipment identification register (CEIR)

TCRA also established a central equipment identification register (CEIR) as per Section 84, of the EPOCA 2010 and the electronic and postal communications (central equipment identification registers) regulations, 2018. There are eight (8) mobile network operators (MNO) in the country and their equipment identification register (EIR) is connected to CEIR and any changes to any of the MNO EIR are sent to CEIR and broadcasted to all the MNOs EIR.

The central equipment identification register (CEIR) maintains the whitelist, blacklist and greylist. The whitelist holds information on any mobile telephone used in any networks, the blacklist holds information of all reported lost or stolen or destroyed mobile telephones and the greylist holds information of any pair that does not fit in the white or blacklist. White, black and grey lists contain all unique mobile telephone numbers and IMEI number pairs.

All MNOs capture any pair of subscriber numbers and the IMEI numbers attach to the network. Each MNO maintains a sub register (EIR) containing all the entries submitted to the CEIR and updates the blacklist. When a subscriber reports loss of his mobile telephone to the serving MNO, the respective MNO needs to effect such changes to the register. Every subscriber's information is kept in the CEIR. MNOs are required to blacklist reported stolen, lost or damaged mobile telephones.

The procedure to blacklist reported stolen, lost or damaged mobile telephone is as follows:

a) A consumer whose mobile telephone has been stolen, lost or damaged, reports to the police station (damaged, lost and found desk at the designated police stations) and notifies the relevant MNO for blocking the SIM card from any further use.

b) The MNO bloc the SIM card and deactivates the stolen mobile telephone so that it cannot be used on any network in Tanzania. Upon receipt of the lost report, the respective MNO blacklist's the reported stolen or lost equipment through its own EIR and automatically shares the updated list to the CEIR.

c) The CEIR synchronises with all MNO EIRs twice per day to collect all IMEI activity (i.e., blacklist, greylist or whitelist) and updates all the MNO EIRs accordingly to ensure that the changes are affected end-to-end.

All MNOs have created a procedure for blacklisting mobile telephones and publishing them for consumer information. They have also established and implemented a user verification mechanism to ensure that correct mobile devices are blacklisted to avoid fraudulent blacklisting of other mobile devices. Any blacklisted equipment shall remain unusable to any network service licensee that uses CEIR unless reported otherwise by the police.

If a mobile device is lost, damaged or lost and recovered it is reported to the police and upon receipt of a report, the police immediately issue a written proof to the person reporting the lost, damaged or lost and found mobile device. The person will then inform their service provider on the recovery of the mobile device, who shall then whitelist it and automatically update the CEIR for whitelisting. The CEIR automatically broadcasts the IMEI or ESN of the lost and found mobile device to all the network service licensees that are connected to the CEIR for whitelisting.

MNOs and the police do not charge subscribers on reporting stolen, damaged or lost mobile telephones nor to the owner on collecting recovered mobile telephones.

No person is allowed to reprogram IMEI numbers of mobile devices. TCRA is carrying out regular inspections and audits the relevant records and systems of the relevant network service licensees from time to time to ensure compliance with CEIR regulations. Any MNO who contravenes any of the provisions of the CEIR regulations commits an offence and is liable on conviction to a fine not less

than five (5) million Tanzania shillings or imprisonment for a period not less than twelve months or to both.

TCRA is also in the initial stages of finding means of setting up a type approval laboratory and it will start by establishing a mini type approval laboratory for mobile phones and set-top boxes.

Blacklisting of invalid and duplicate IMEI

Through the electronic and postal communications (central equipment identification registers) regulations, 2018 all the MNOs are required to auto reject any invalid IMEI that tries to attach to their networks. Once a subscriber tries to attach to a network, the EIR will validate among other things the IMEI against the approved GSMA TAC. If the IMEI passes the validation it will then be allowed to attach to the network and use the services. All non-conformity IMEIs are automatically rejected and blocked by MNOs once after trying to attach to the network.

Taking into consideration the problem of duplicate IMEIs across the networks, TCRA coordinates a blacklisting of all duplicate IMEIs on a monthly basis for all the MNOs. Each MNO scans their networks and establishes a list of duplicate IMEs that need to be blacklisted. Once the blacklist of duplicate IMEIs is done for each of the MNO EIR, the CEIR will then be automatically updated of the changes to ensure end-to-end blocking. Since the first blacklist in July 2016 a total of 417 489 IMEIs have been blacklisted in all the MNO networks.

I.I.XI Republic of Zimbabwe

All mobile network operators in Zimbabwe have the capability to detect counterfeit devices with duplicate IMEI codes on their networks and to disconnect them. However, given the importance of counterfeit devices for operator revenues – these devices account for the majority of network users – actual disconnection is rare.[3] Nevertheless, the following measures have been taken in Zimbabwe to combat the proliferation of counterfeit devices and the theft of mobile devices:

– prohibition on the use of any device not meeting type-approval requirements;

– obligation for mobile network subscribers to register newly purchased SIM cards with the MNO before the card can be activated on the network;

– acquisition of a subscriber registration database to ensure that all SIM cards activated in the country are correctly registered, which also facilitates the detection of counterfeit devices and fake mobile phones;

– testing and certification of all new ICT devices at the regional level by an independent testing laboratory operated by the independent communications authority of South Africa (ICASA).

I.II South America

I.III.I Federative Republic of Brazil

1 Brazilian approach on combating counterfeit ICT and stolen devices

1.1 Location where the use case is implemented

Brazilian mobile networks. Initially the solution was focused on addressing stolen and lost devices (*Cadastro de Estações Móveis Impedidas – CEMI*) and by 2014 a second part of the solution (*Sistema Integrado de Gestão de Aparelhos – SIGA*) responsible for detecting and blocking tampered and non-certified devices was initiated. This second part implementation was planned in three phases. In this phase, irregular devices were blocked in different regions of the country. The solution is now active in the whole territory.

[3] ITU-D SG2 Document SG2RGQ/85 from Zimbabwe

1.2 Dates of implementation

- CEMI solution: 2005;
- Approval of the action plan by Anatel for deploying SIGA: 2012;
- SIGA trial activation: 2014;
- Construction of a database of the uncompliant (SIGA) devices: 2015;
- Anti-piracy public campaign: 2016;
- Launch of "Celular Legal" website: 2017;
- Start of SMS warnings and blocking of tampered and non-certified (including counterfeit) devices: 2018.

2 Scope

Besides the initial approach focused on blocking stolen or lost devices in mobile networks (CEMI), the Brazilian mobile service regulation[4] determines that operators should only allow on their network devices that have been certified by the national telecommunications agency – Anatel. Besides, the normative also dictates[5] that users should only use equipment certified by Anatel. Based on these two directives, Anatel enforced that the Brazilian mobile operators should implement jointly a technological solution to curb the use of mobile devices that are not certified (including counterfeit) or have been tampered (SIGA).

The established action plan submitted by the operators to fulfil this obligation defined the outline of technological solution to be implemented, possible criteria based on real users cases in order to minimize the impacts on the population, the criteria to be implemented for new users after the solution goes live, so that only devices that comply with Anatel's regulation can access the network, the criteria to be implemented for mobile users in order to avoid inconvenience to users or foreign users, awareness campaigns on the mobile network users, among other things.

The action plan was approved by Anatel in 2012, considering the technical and regulatory aspects, and a joint workgroup, called SIGA – devices management integrated system, was created to coordinate the activities on the implementation of the solution. This workgroup is led by Anatel and has members from mobile operators, manufactures and associations such as GSMA and Abinee (Brazilian manufactures association).

3 Common statistic for country's use case

- **Mobile accesses**: 249 4 million[6]
- **Population**: 213 million
- **Gross domestic product (GDP)**: 1.45 trillion USD (2020).

4 Description of use case's solution

The main objective of the CEMI solution is to provide for the mobile device owner a mechanism to block their device in situations in which the device is stolen or lost (see Figure I.2). Currently, mobile device owners can request the device block at police enforcement authorities or directly at their mobile operator company as shown in the picture below:

---

4 Article 156 of Law N.º 9.472, of 16 July 1997 (http://www.anatel.gov.br/legislacao/en/laws/608-law-9472) combined with Article 10, V of Resolution N.º 477, of 7 august 2007 (http://www.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477)

5 Article 4º, V of Resolution N.º 632, of 7 march 2014 (http://www.anatel.gov.br/legislacao/resolucoes/2014/750-resolucao-632)

6 https://informacoes.anatel.gov.br/paineis/acessos/telefonia-movel

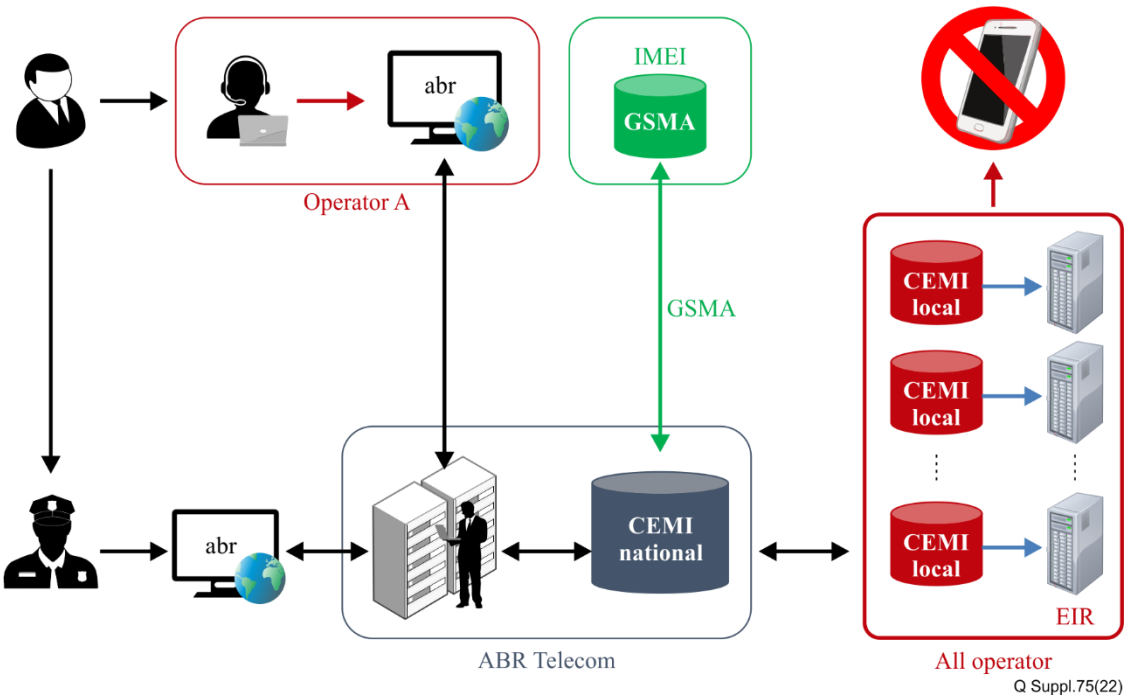


Figure I.2 – Mechanism to block mobile device

The SIGA solution, implemented since 2014, works in a way to complement CEMI's achieved goals, so that it can be possible to block tampered and uncertified devices. Unlike CEMI, SIGA's blockage is not done by request. The blockage occurs automatically after the user is informed about the irregularity several days before. Along with the IMEI, the system combines other information such as MSISDN and IMSI contained in CDRs/SDRs to ultimately identify cases of tampered or uncertified devices. Users using those devices will receive SMSs a few days before informing about the irregularity and the consequent block in the mobile networks.

Figure I.3 depicts the SIGA common workflow.

After the irregular device is identified by the system, a "case" is generated at the central system and all the relevant information is forward to the involved operators so that they can notify the owner of the device, following the script below:

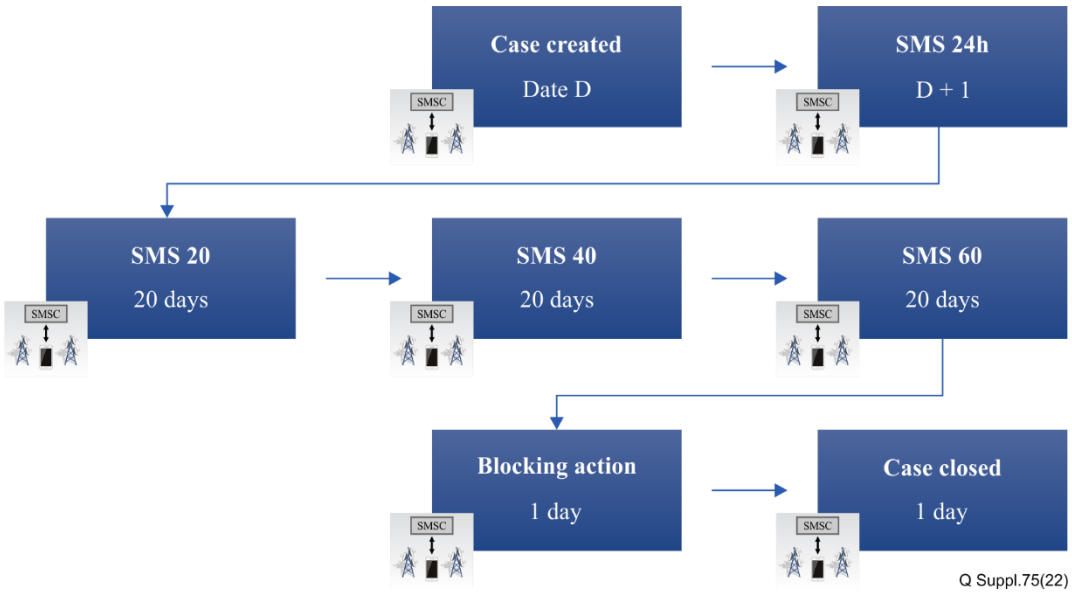


Figure I.3 – Image x – SIGA common workflow (time lapse between SMS was reduced by May/2021 from 25 to 20 days)

– 24h – SLA for the SIGA central system collects the relevant information at the operator network, identifies the irregular device, generates the "case", forward the relevant information to the operator where the irregular device is identified, and notifies the user.

– 1st SMS – As soon the operator is notified, it sends the first SMS to the user informing that their device is irregular and provides the link to the "Celular Legal" [7] website.

– 2nd SMS – 20 days after the first SMS is sent, if the irregular device is still active on the network, another SMS is forwarded to the user reiterating the need to regularize his device.

– 3rd SMS – 40 days after the first SMS, if the irregular device is still active on the network, another SMS is forwarded to the user reiterating the need to regularize his device.

– 4th SMS – 60 days after the first SMS, the user is notified that his device will be blocked on the operator's network.

– The irregular device is blocked at the operator network (including at their EIR the IMEI and MSISDN related to the irregular device) one day after the last SMS is sent.

– Currently, it develops alternative workflows to block irregular devices that have been tampered after the blockage. In those cases, it's desirable to have a different approach so that the offender does not game the system so as to remain unblocked indefinitely.

5 Overview of challenges and countermeasures regarding implementation of use case

The SIGA solution was activated, on a trial basis, in April 2014 and since the end of 2015 it is active on all Brazilian network operators identifying and building a database of the uncompliant devices that currently are active on the mobile network.

Additionally, in 2016, under the discussion of the SIGA group, a public campaign was launched by Abinee (a major manufacturers' association), with the name "Celular pirata não", with the aim to raise awareness for the Brazilian population of the importance and benefits in using certified equipment. The campaign produced publicity material[8] that were used on social networks, broadcast TV and radio, internet video websites and on street media (such as bus stops and outdoors).

---

7 https://www.gov.br/anatel/pt-br/assuntos/celular-legal

8 https://www.youtube.com/channel/UCdAapZdKU0BMJR8De8phg1Q

In January 2017, Anatel has launched the website "Celular Legal"[9] that informed the user on the importance of using only certified devices and that it also aims to assist the consumer in fulfilling this obligation by providing an interface where one can verify (based on a consultation on SIGA's database with the device IMEI), if the mobile terminal the user would like to obtain is a regular device. Besides, since mobile device theft is also a major problem in Brazil, the same interface is also verified at the IMEI that has been included on the Brazilian stolen devices blacklist (CEMI).

In April of 2017, Anatel's board of directors decided to proceed to the next phase of the actual project, which consists in commencing irregular devices blockage. At the moment, it covers non-certified equipment and tampered IMEIs that resulted in an invalid IMEI or an IMEI that is not on a "whitelist" from GSMA.

Today, the SIGA group has just implemented a decrease of the time lapse between SMS to 20 days (from May of 2021 the time lapse changed from 25 to 20 days, resulting in blockage after 60 days instead of 75 days). Next improvements include adding more information to the "type" of blocking (invalid, tampered, stolen, lost, etc.) and developing strategies to address cloned devices which are not being blocked yet. The main concern with this matter is developing a procedure that will impose minimum impact on the legitimate user. Also, there is the intention to integrate CEMI's database with GSMA's blacklist database globally (nowadays, it's integrated with Americas database).

Also, even though in 2015 Brazil started to include in the national blacklist database all the IMEIs of all the mobile terminals stolen in the Americas that were blocked on GSMA blacklist (including the IMEIs not active on the national networks), this process had a high impact on the operators EIR.

To address this, since June 2021, Brazil started to consider all the stolen mobile terminals worldwide that were blocked on GSMA blacklist, but only the IMEIs active on the Brazilian operators' networks are now included on the national blacklist database.

6 Statistic on the effects of implementation of the use case

CEMI – number of blocked devices

	2005-2014	2015	2016	2017	2018	2019	2020	2021*	Total
Brazil	5.074.594	1.118.865	1.337.511	1.473.756	1.468.836	1.393.223	1.010.886	721.818	13.132.642
GSMA	15.427.620	8.212.697	11.641.571	4.446.453	8.254.214	10.299.236	7.335.586	23.928**	68.823.552

* Until October, 2021

** In June 2021, Brazil started to consider all the stolen mobile terminals worldwide that were blocked on GSMA blacklist, but only the IMEIs active on the Brazilian operators are now included in the national blacklist database, justifying the relevant decrease seen in the table above

SIGA – number of blocked devices

2018	2019	2020	2021*
154.689	1.203.152	735.327	675.363

* Until October, 2021

9 https://www.gov.br/anatel/pt-br/assuntos/celular-legal

7 Roadmap of future planned evolution of the use case

- Consider new reduction of time in-between consumer SMS warning and blockage (SIGA);
- Improvement of database information about the blockage (CEMI and SIGA);
- Addressing cloned devices (SIGA).

8 Final remarks and conclusion

In the last years, Brazil has been strengthening its framework to combat theft and counterfeit devices. The national agency of telecommunications – Anatel – acts as a coordinator of the project, being constantly in touch with mobile operators and the ABR Telecom, which is the entity responsible for administrating these centralized databases. For the future, as pointed out in clause 7, Brazil has several challenges ahead and shall pursue improvements of the already deployed solutions.

I.II.II Republic of Colombia

1 Common information about use case

1.1 Title of the use case

The Colombian case study to combat stolen, fraudulent, and counterfeit mobile phones.

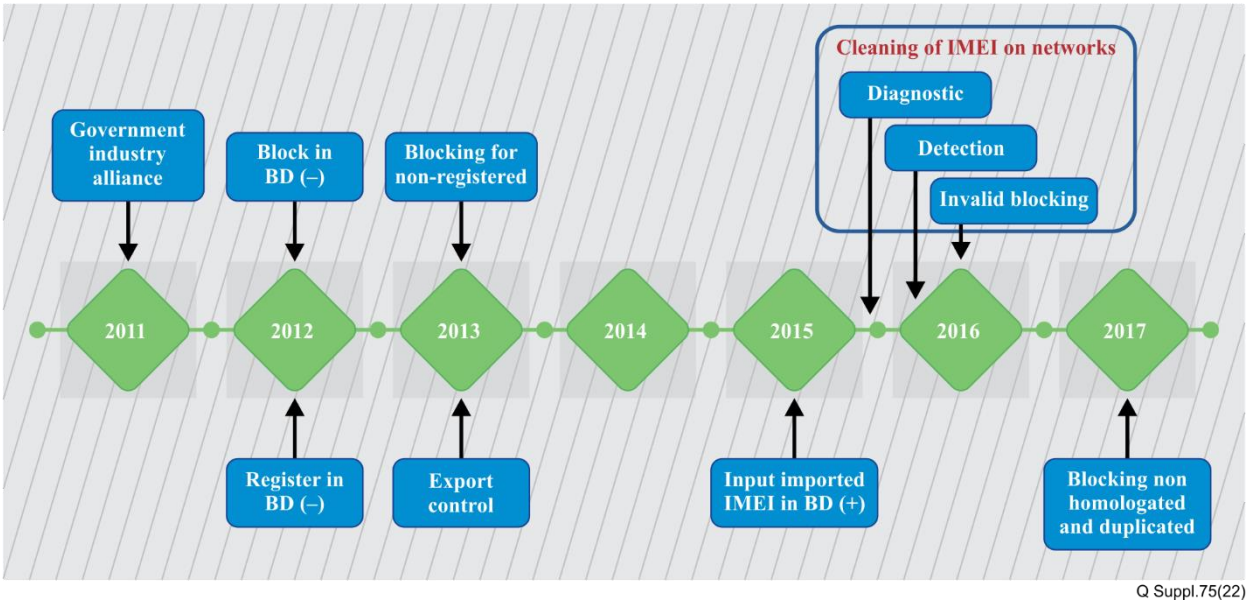
1.2 Location where the use case is implemented (country and/or private use case)

The Colombian national territory.

1.3 Dates of implementation of the use case (month/year)

As seen in Figure I.4, the main implementation dates of the current system are listed below:

- 2012: The IMEI blocking system is implemented for stolen and lost phones.
- 2013 – April: Blocking of non-registered phones are initiated.
- 2016 – October: Blocking of devices with invalid IMEI (not allocated by the GSMA).
- 2017 – January: Blocking of counterfeit IMEIs.
- 2017 – May: Blocking of non-homologated IMEIs.
- 2017 – June: Blocking of duplicated IMEIs.



Source: CRC.

Figure I.4 – Timeline of the adoption of the different IMEI control phases

1.4 Source (ITU Member)

- Communications regulation commission (CRC)
- "Using IMEI control systems to combat stolen, fraudulent, and counterfeit mobile phones: A Colombia case study". April, 2018 by Jay Gumbiner – IDC Latin America.

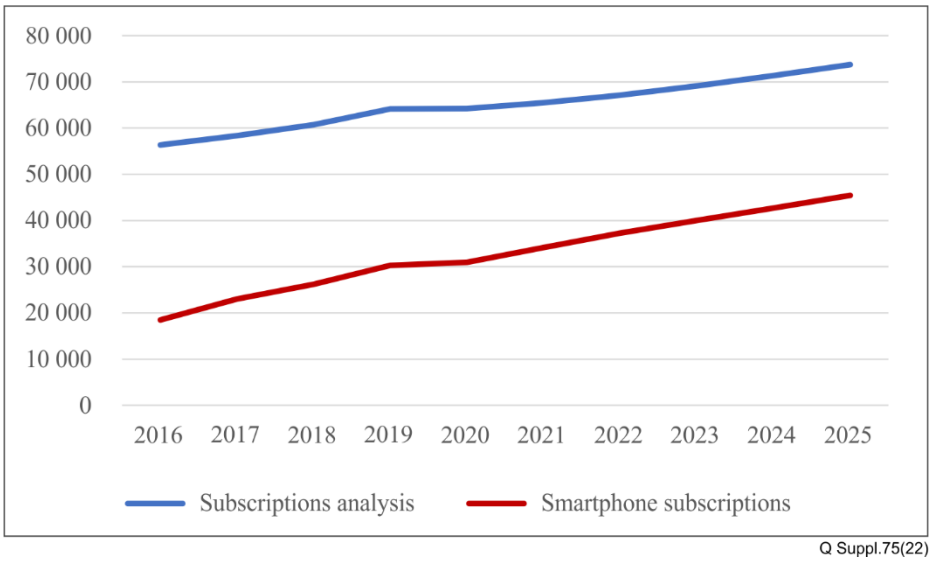
2 Scope

Initially designed to help combat the growth of stolen phones within the country, in 2011 Colombia's government, in collaboration with different sectors such as defense, ICT, retail, and customs, among others, through the national telecommunications regulator CRC (Comisión de Regulación de Comunicaciones – Communications Regulatory Commission) and MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones – Ministry of Information Technology and Communications) developed and implemented a technology-based system to enable identification, registration, and network access management of devices connecting to the nation's cellular networks.

3 Common statistic for country's use case

3.1 Telecommunication statistic (e.g., number of users of mobile devices, operators, etc.)

Figure I.5 shows the related statistics about the projections made for the next five (5) years for mobile line subscriptions and the comparison with the growth in the use of smartphone-type devices.



Source: Projections – Global Data.

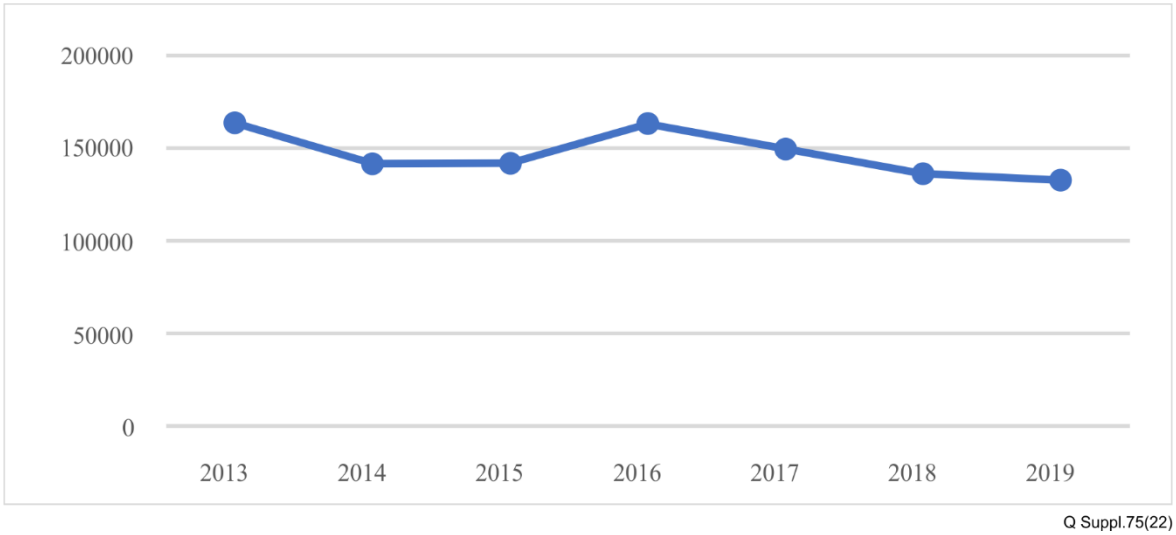
Figure I.5 – Mobile and smartphone subscriptions. [x 1000]

This figure presents the adaptation of smartphone devices and the growth of the total number of users with active lines in the country in recent years; as shown, this behaviour is projected to remain in the upcoming years, closing the gap between these two variables.

This information is relevant, considering that these types of devices are commonly associated with the highest crime rates in Colombia.

3.2 Statistic of the problem (e.g., number of counterfeit devices, stolen devices, etc.)

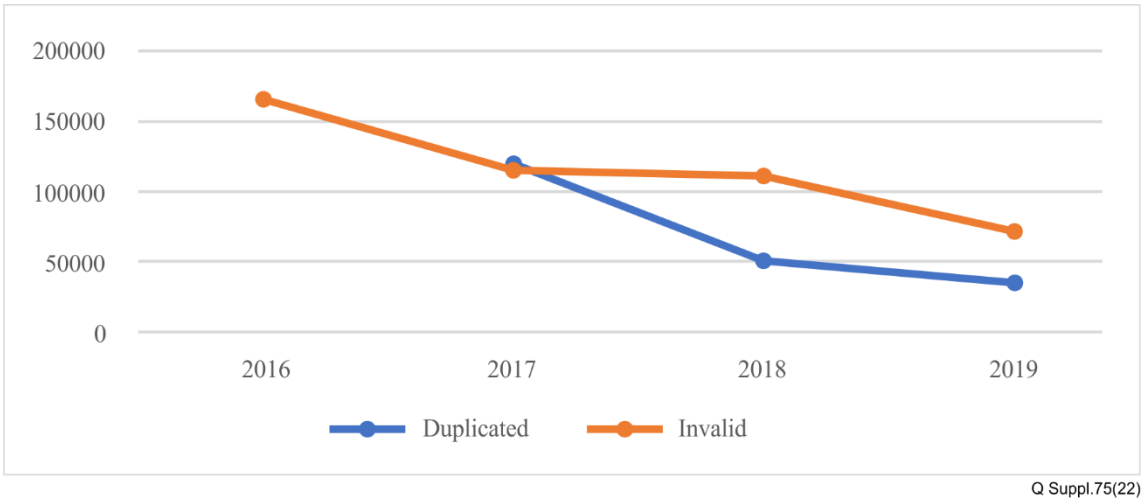
Figure I.6 shows the statistics of the devices reported for the "stolen" and "lost" typologies from 2013 to 2019; it should be emphasized that approximately 100 thousand devices are reported and blocked under the typology "stolen" every month.



Source: CRC.

Figure I.6 – Monthly average of reported stolen and lost devices

Figure I.7 shows the statistics of the monthly average of blocked IMEIs because of IMEI duplication or because the IMEI is identified as invalid; as seen, these types of blocking methods have been implemented in recent years and represent an important number of devices.

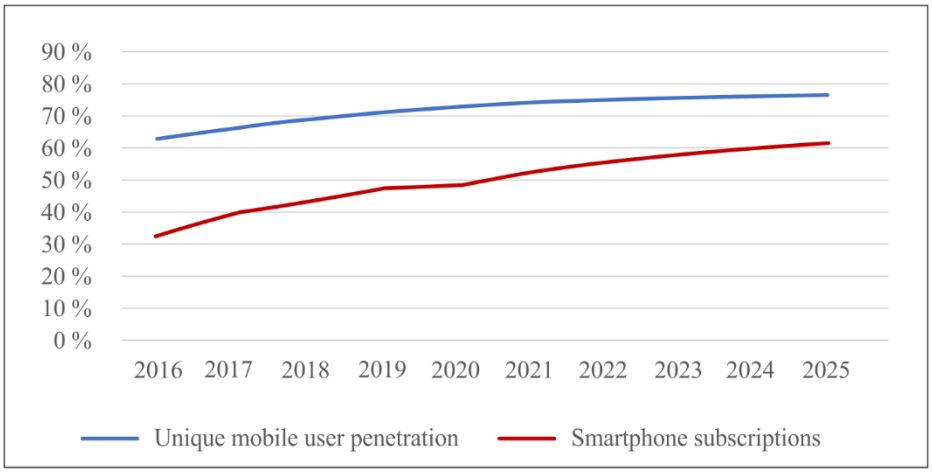


Source: CRC.

Figure I.7 – Monthly average of reported devices with duplicated or invalid IMEI

3.3 General statistic with regard to use case (e.g., size of the economy, population, etc.)

Figure I.8 contains the percentage of unique mobile user penetration, and it is compared with the smartphone penetration from 2016 to the projection of 2025.



Source: Projections – Global data.

Figure I.8 – Unique mobile user penetration and smartphone subscriptions

This graph shows the growth in the penetration of unique mobile users with a projected percentage in the next five years of close to 80 % in Colombia, this growth could be associated with the evolution of technology worldwide and with the new users acquired by mobile operators every year. Many of the users use smartphones to authenticate themselves on the network so they can enjoy the actual services offered by the network; in addition, payment and financing facilities offered by national operators are factors that enhance the adoption of smartphones.

However, citizens are still using low specification devices that have access to 2G technology due to the simplicity of the operation and since it is not quite attractive for the common crime.

4 Description of use case's solution

4.1 Overview of the solution

This IMEI-monitoring system allows the continuous monitoring of mobile phones as they connect to the nation's networks, ensuring that only legal and legitimate devices can be used. Irregular devices are either immediately blocked from the system in the case of a reported stolen/lost phone, or in some cases the user is informed of the potential blocking of the phone with invalid identifying information and the eventual blocking of the phone if certain procedures to 'validate' the phone is not completed.

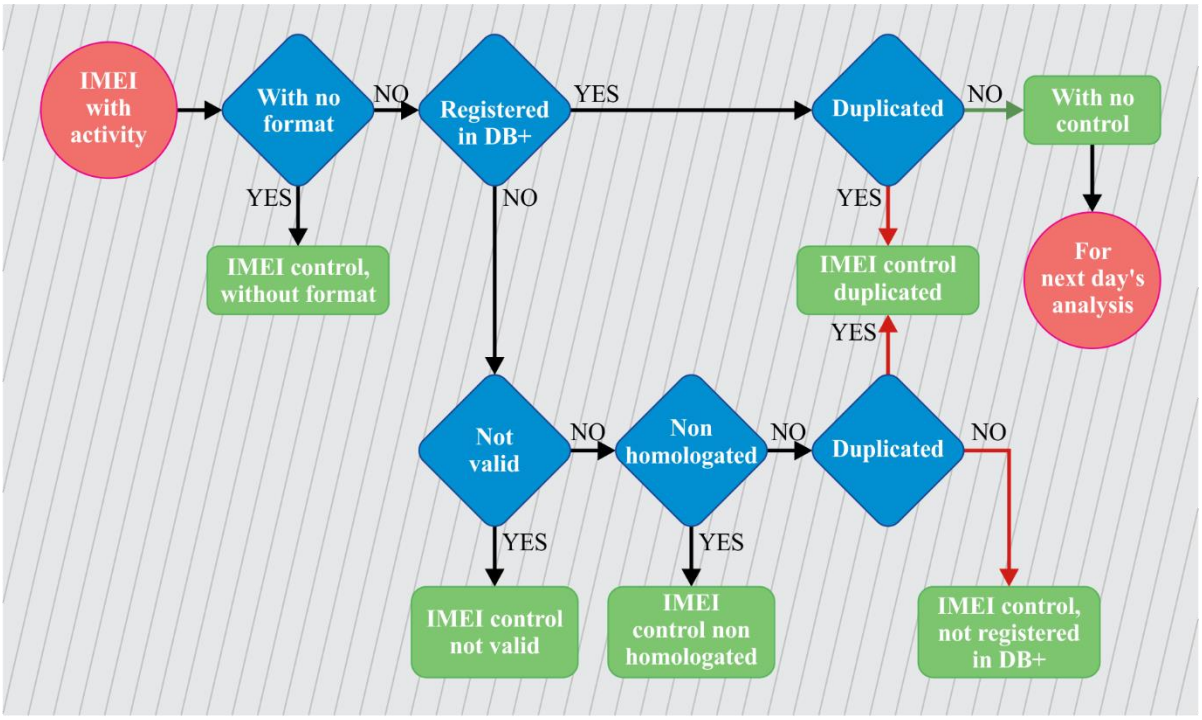
4.2 Framework of the solution including diagrams and detailed description

The current system is based on the functionalities provided by the implementation of two databases, named the positive and negative database. The positive database contains a list with the IMEI of every legally imported terminal into the country. Once the device is acquired by the user, the database is complemented with the personal information of the very same owner such as an ID number.

The negative database contains the list of the IMEIs that are not allowed to operate in the national networks, specifically the ones that have been classified by the blocking typologies as:

- Lost or stolen
- Having an invalid IMEI (neither in GSMA nor CRC TAC list)
- Non-homologated
- Duplicated
- Non-registered.

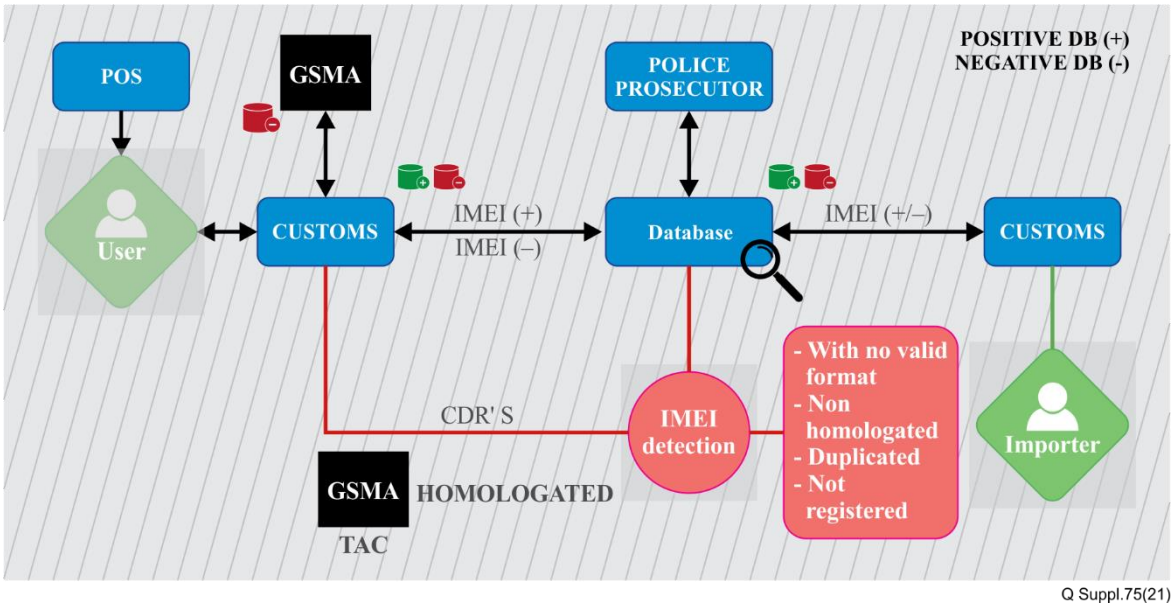
Figure I.9 contains the flow diagram with the control measures recently listed, it includes the control of not valid IMEIs (they have not been able to operate since February 2017).



Source: CRC, 2016; Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: Etapa de control, Relaciones de Gobierno y Asesoría.

Figure I.9 – Flow diagram with the adopted control measures

According to the previous information, Figure I.10 shows the IMEI control system and its interaction with the different agents that take part in this implementation, like the customers, the importers, the police authorities, the GSMA and the CRC itself.



Source: CRC.

Figure I.10 – Deployed IMEI control mechanism

The following specifications of the deployed control mechanism are taken from the work of Jay Gumbiner.[10]

- Control and handling of a phone with a duplicated IMEI

On a daily basis each mobile operator, based on the voice CDRs, can detect duplicated IMEIs using algorithms to identify collisions or time/distance conflicts between the calls placed from different IMSIs with the same IMEI. In the same manner with the same kind of algorithms, a centralized monthly system detects duplicated IMEIs showing activity in different networks at a national level. Once detected, they identify the IMSIs that have been using the duplicated IMEI and its users are alerted and given 30 calendar days to present (physically or virtually) the purchase documents related to the phone, in addition, information about the point of sale and other personal information. This information is delivered to law enforcements to investigate the crime of IMEI tampering.

At the end of the grace period where the users of phones with duplicated IMEI supply the required information and supporting materials, the mobile operator in which the phone is being used must apply the criteria set in the regulation to define which of the users can continue to use the equipment.

There are two criteria for the operators to define which user can continue to use a phone with a duplicated IMEI:

1) The user that has registered the IMEI under his ID, or
2) The user whose supporting materials or phone provides the operator with enough evidence that the phone is the genuine one.

Once the user of the legitimate device, with the above criteria, has been identified, the mobile operator will associate the correct IMEI-IMSI coupling in its EIR to only allow access to the phone that attempts to use the IMEI with that IMSI to the network. In this way the duplicates are blocked. The (single) IMEI is placed in the centralized negative database for identification purposes to users, other operators and authorities.

- Stolen phone handling

In the case of a phone being reported as stolen, the process is much simpler. The user is required to immediately report the theft to their mobile operator and should formally report it to the police or legal authorities. However, only a very small percentage (no more than 2 %) of the phones stolen in Colombia are reported to local police authorities. In most cases the person will call the mobile operator themselves to report the phone as being stolen, at which point the details on the phone, IMEI (taken from the network activity by the date and hour of the theft), and customer details will be placed into the system to have the IMEI blocked in less than half an hour.

The stolen/lost reported IMEIs received by the mobile operator is shared on-line to the centralized negative database and the IMEI is broadcast to the rest of the mobile network operators to be blocked in a maximum time of 25 minutes. By regulation, information about the theft must be populated in the negative database, such as the address / location of the event, if there was violence involved, if there were weapons involved, if the victim is a minor and their contact information. With this information, law enforcements and judicial authorities can start investigations in the absence of a formal report from users, perform geospatial analysis of the hot spots of criminal activity involving stolen phones to reinforce the surveillance in those areas, and arrest thieves or people receiving stolen phones.

- Homologation process

The process for homologating a new phone model for the Colombian networks is a straight-forward process that is submitted to the CRC for both individuals and manufacturers or importers. The approval can be completed in less than two weeks. Since Colombia's mobile networks use the same

[10] Gumbiner, Jay; "Using IMEI control systems to combat stolen, fraudulent, and counterfeit mobile phones: A Colombia case study". April 2018. IDC Latin America.

850 and 1900 MHz bands that the majority of the countries in North, Central, and South America use, most phones that are coming to Colombia already have regulatory approval from the federal communications commission (FCC) in the United States of America (USA). This helps to speed up the process immensely since the network compliance issues have already been confirmed. Since August 2016, MinTIC has waived the fee for this approval process in Colombia.

In the process of homologation, the applicant must present the TAC allocation certification for the CRC to validate the integrity and validity of the new model identification accordingly with the industry standards through access to the GSMA database. Once homologated, the trademark and model are publicized on the CRC web page for the public to see the homologated phones that can be sold and used in the country. At the same time, all TACs related to the model are pulled out from the GSMA database and placed in a confidential list of trademark-model-TAC, which allows the mobile operators to daily detect which of the IMEI with activity in the networks belongs to a non-homologated model and informs the user and gives them a grace period to homologate the phone with the CRC. As a result of this control initiated in October 2016, approximately 22 % of the handsets presented to the CRC by users for the homologation review resulted in identifying lost/stolen phones that were tampered with to alter the original IMEI with IMEIs that were not sold in the country or region.

- Personal imports

As a transition in the beginning of the control of non-homologated phones in October 2016, there was a process in place for individuals who had phones before the regulation was enacted where their phones may have been purchased overseas or in a questionable sales channel. To make sure that these phones were homologated, users were directed to the wwww.notequedesinmovil.gov.co website via social media campaigns of #notequedesinmovil (#don'tbeleftimmobile as a translation to English). A detailed video also helped the applicants to find the required information and explained the process for submitting it to the CRC.

4.3 Description of additional measures taken to engage the problem

As seen in Figure I.10 and in the previous clauses, there is an important role that must be played by the users in the implemented system, it starts with the acquisition of the terminal, where the user at first must verify the legal constitution of the mobile phone seller; additionally, the user is also responsible for the execution of the registration process, using the different platforms provided by the mobile operators.

If the customers acquire or use a terminal with an irregular source, or which IMEI has been duplicated, they must be contacted or notified about the possible blocking situation via SMS, phone calls or emails with the information of the procedure and the requirements in case they need to regularize the IMEI operation.

5 Overview of challenges and countermeasures with regard to the implementation of use case

The CRC has identified in a recently published document, that there are some issues that affect the effectiveness of the mechanism described in the present document, they are listed below:

- Device reprogramming: According to some investigations, there are hardware and software based methods that allow criminal organizations to modify the IMEI of specific devices or chipsets; even if some mobile phone manufacturers have been introducing methods for avoiding software access to the chipset, this practice is still very common within criminal organizations.
- Parts market: Even if the implemented mechanism would reduce the index of IMEI alteration to zero, there would still be a great demand for parts; hence, to satisfy this demand, criminal organizations would continue operating.

Based on the previous aspects, among others, the CRC has defined a problem related to the high complexity that the mechanism to combat stolen and counterfeit mobile phones has accumulated in recent years; hence, the current challenge is to identify if the implemented control measures are susceptible of being simplified.

6 Statistic on the effects of implementation of the use case

Table I.1 contains some of the effects of the implementation of the implemented use case, it is necessary to mention that as shown in Figure I.4, some typologies of IMEI blocking have been active for a longer period.

In addition, as shown in Figure I.7, there has been a reduction of the monthly average of reported devices with duplicated or invalid IMEI in recent years.

Table I.1 – Impact of the IMEI blocking typologies

Type of IMEI	Total IMEI impacted	Control measure taken
Incorrect format	2.3 k[11]	No access to the networks
Invalid	4 million	Permanently blocked
Non-homologated	4 million	Blocked, but can be reinstated once corrective actions are taken
Non-registered in positive database	9 million	Blocked, but can be reinstated once corrective actions are taken
Duplicated	1. 9 million	On-going blocking procedures are in effect

Source: CRC.

7 Roadmap of future planned evolution of the use case

According to the challenges presented in clause 5, the CRC is working towards the simplification of the implemented system, with this exercise it is intended to positively impact the efficiency in the operation costs of the adopted strategy.

The approximation of the analysis that the CRC is currently developing, includes the application of the regulatory impact analysis (RIA); hence, the possibility of not making any intervention and preserving the implemented mechanism will be equally reviewed.

8 Final remarks and conclusion

Since 2011, Colombia has been implementing a mechanism to combat counterfeit and stolen mobile devices, it is the result of the interaction and intervention between private agents (operators, the database administrators, manufacturers, sellers), public agents (MinTIC, CRC, police authorities) and the users; every one of them playing an active role in the reached results recently published; nevertheless, there are still some situations that are not entirely covered by the mentioned mechanism like the IMEI reprogramming and parts market, among others. It is expected that the information shared in this Supplement will be relevant to the ITU-T SG11 in order to propose preventive measures and possible solutions to deal with the above issues.

[11] Information of December 31, 2017.

I.III Asia

I.III.I Republic of India

National use case of India

As of 30th April 2018, there are 1 125 million wireless subscribers in India (*Ref. TRAI Press Release No. 68/2018, http://trai.gov.in/sites/default/files/PRNo68Eng26062018.pdf*). Existing issues include traceability of stolen phones, IMEI number duplication / cloned by way of re-programming, unauthorised IMEIs, etc. The availability of mobile handsets having duplicate/stolen/unauthorised IMEI in the Indian telecom network is not merely a law and order issue but it also has security implications in lawful interception and monitoring.

In the year 2008, it was observed that a large number of mobile handsets were either working without any IMEI / ESN or having all zeros. Such mobile handsets are a security risk as they cannot be traced by security agencies. Further, it was noticed that the networks of many service providers were not fully equipped with EIR for tracking the IMEI of the handset. Therefore, in the interest of national security, all access service providers were directed by the department of telecommunication (DoT) on 6th October 2008 to make provision for EIRs in their systems so that calls from mobile handsets without IMEI or that of IMEI with all zeros are rejected. Given the large number of innocent users of mobile handsets with fake IMEI, DoT permitted implanting of valid IMEIs as a one-time measure through the association of the telecom service providers.

Subsequent to this direction, all service providers have upgraded their network and presently have provisioned EIR in their network. The equipment identity register (EIR) is a database that contains a list of IMEIs of GSM based mobile handsets which are active in a mobile network. EIR maintains a white, grey and blacklist. The whitelist is composed of IMEIs of mobiles that are permitted for use. The grey list consists of devices that do not conform to the standards but could be permitted to connect under supervision or it triggers an alert. The blacklist contains IMEIs of devices that have been reported stolen or lost and are being denied access to the network. Accordingly, the TSPs can block the handset in its network.

Available legal provisions

a) Section 65 of the Information Technology Act, 2000 deals with the modification and altering of computer source code, which is a cognizable offence. The violation of section 65 attracts a penalty of imprisonment for a term of up to three years. The re-programming of IMEI in a mobile device is a kind of modification/altering of the source code of the mobile device. Thus, provisions of Section 65 of the Information Technology Act, 2000 can be invoked in case of re-programming of IMEI of a mobile phone device.

b) Section 25 of the Indian Telegraph Act 1885 talks about "*Intentionally damaging or tampering with telegraphs*". Since a mobile device is a part of the telegraph, provisions of section 25 of the Indian Telegraph Act, 1885 for the offence of duplicating/re-programming an IMEI.

c) On 28th August 2017, a new rule had been enforced by the Government of India to prevent tampering of a mobile device equipment identification number. As per this rule, IMEI number change is not permitted, it's defined as unlawful, except for mobile manufacturers.

As per existing policies, there is a provision to block the usage of black-listed mobile devices in the local network. India has 22 license service areas (LSA) – multiple telecom service providers (TSPs) are providing services in each LSAs. So, to block any mobile device in all of the networks, a central equipment identity register (CEIR) is planned.

CEIR will facilitate the following:

a) Curtail the fresh counterfeit mobile devices from entering the networks at the same time it will permit the use of such existing mobile phones.

b) Block stolen/lost mobile devices across all TSPs across the country.

c) Maintain device registry.

d) Enhanced mechanism to report lost/stolen mobile devices.

e) Enable IMEI based lawful interception.

f) Protecting the interests of the consumers by making them aware of the information related to fake and cloned mobile devices.

Department of telecommunication, Government of India has also initiated a dialogue with the Indian mobile manufacturers for making IMEI numbers non-modifiable. To resolve the issue of IMEI re-programming – it is to be implemented globally.

I.III.II Federal Democratic Republic of Nepal

Counterfeit devices are those devices that are misrepresented as to their origin or quality. Counterfeiting of devices can infringe the legitimate manufacturer's trademark right. Counterfeiters introduce counterfeit and substandard devices in the supply chain.

Due to counterfeit and substandard mobile devices, the quality of service of the mobile network experienced and security of the devices may be compromised. These devices do not also meet the requirement e.g., operating frequency, power level, safety, health, etc. set by the government or regulator.

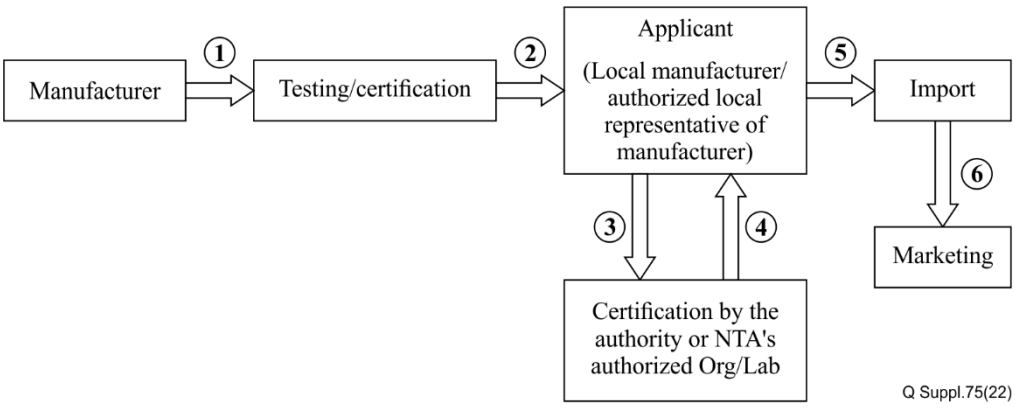
Type approval and the international mobile equipment identity (IMEI) registration mechanisms are the regulatory solutions to combat counterfeit and substandard mobile devices in the country. Nepal telecommunications authority (NTA) has been doing type approval of radio telecommunication customer premises equipment (CPEs) including mobile devices prior to importing and selling in Nepal since 2008. Registration of IMEI numbers of mobile devices prior to import and sale in Nepal was started since 2016 by NTA. NTA is going to establish the mobile device management system (MDMS) i.e., national equipment identity register (NEIR) system very soon.

GSMA's initiative to blacklist for stolen/lost mobile devices also supports making the devices useless. GSMA also requested the governments / regulators / operators to join the international effort and contribute to GSMA blacklist for stolen/lost mobile devices, on devices that cannot be used in the country.

Member States may also initiate coordination and collaboration for sharing a blacklist of IMEI numbers to make stolen/lost mobile devices inoperable within the Member States.

Type approval of mobile devices

As per the provision of Clause (f) of Section 13 and Section 14 of the Telecommunication Act, 1997 the NTA determines and/or approves the standard and quality standard of the plant and equipment relating to the telecommunications and the telecommunications service. Prior to the import and/or sale of any types of radio telecommunication CPEs in Nepal, the concerned manufacturers/authorized agents/representatives have to get a type approval certificate under the provision of type approval procedure defined by the NTA. The procedure for type approval is as depicted in Figure I.11.



NOTE – The numbers along with arrow shows the sequence of steps. Step 5 is possible only if the product(s) is certified to use in Nepal for specified use (i.e., Type approval certificate is granted to the applicant through step 4)

Figure I.11 – Type approval process

The detail regarding the type approval of mobile devices in the last three years is depicted in the Table I.2.

Table I.2 – Type approval in a three year period

Year	Provisional (for 6 months period)	Periodic permanent (for 5 years period)
2073 B. S.	719	193
2074 B. S.	522	316
2075 B. S	371	220

IMEI registration procedure

Importers shall register the IMEI numbers of mobile devices prior to import and sale in Nepal. NTA verifies the submitted IMEI numbers with the help of the GSMA IMEI database and issues the no objection letter to release the mobile devices from the concerned custom office if the submitted IMEI numbers are valid. The detail regarding the registration of IMEI numbers by importers in the last three (3) years is depicted in Table I.3.

Table I.3 – IMEI registration in the 3 years period

Year	Number of IMEIs registered by importers	Number of IMEIs registered by individuals
2073 B. S.	9 994 764	4 062
2074 B. S.	9 574 588	1 240
2075 B. S	8 911 487	2 570

In case of stolen/lost mobile devices, after receiving the application to trace IMEI of those devices, NTA sends them to the mobile operator to trace and to latch the new mobile number. After receiving information of the traced mobile devices from the mobile operator, NTA sends it to Nepal police for further investigation to get the stolen/lost mobile devices.

There is a module called "Know your mobile device" which provides the information on whether the mobile device is type approved or not and its IMEI is registered or not. This way people are facilitated to get a standardized mobile device with the help of an IMEI of that device.

Mobile device management system

Mobile device management system (MDMS) will have the database of IMEI number of mobile devices registered inside the country. Following are the reasons for the implementation of MDMS.

- To increase the tax revenue from the import of mobile handsets by discouraging the illegal import of mobile handsets.
- Ensure consumer security and national security.
- Trace or block the lost or stolen handset.
- To secure the market for genuine mobile handsets.

In an effort to address the challenges associated with the proliferation of illegal mobile devices connected to the public telecommunications networks, the system will facilitate registration, identification and verification of the use of mobile devices. The generic flowchart of the MDMS towards the management of mobile devices is as shown in Figure I.12.

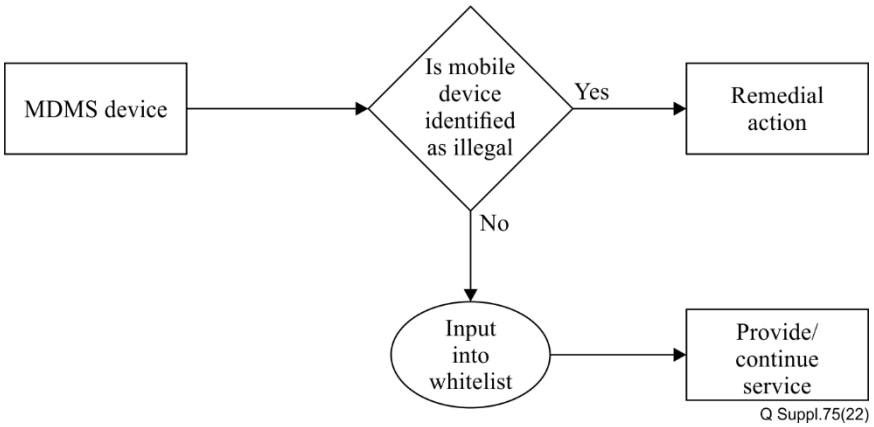


Figure I.12 – Flowchart of the action of the proposed MDMS

The MDMS will minimize the illegally imported (including counterfeit) mobile devices and deter the theft of mobile phones to achieve the specified objectives. The system would consist of whitelist, greylist and blacklist of IMEI codes and provide interfaces to importers, customs and law enforcement agencies, mobile operators, the general public and the NTA.

The MDMS will have the following facilities:

- Detection SIM box
- Detection of counterfeit / substandard mobile devices
- Detection of mobile devices reported as stolen/lost
- Provision of whitelisting of IMEI numbers of mobile devices.

Coordination between Member States

Member States may share the blacklist IMEI to minimize the illegally imported (including counterfeit) mobile devices and to deter the theft of mobile phones. By joining the international effort and contribution to GSMA's initiative for blacklisting of IMEI numbers of stolen/lost mobile devices, coordination between the Member States may be established to combat the illegally imported (including counterfeit) mobile devices and to deter the theft of mobile phones.

Conclusion

The type approval, IMEI registration, the international effort and contribution to GSMA's initiative for blacklisting of IMEI numbers of stolen/lost mobile devices and establishment of mobile device management system are the best solutions to combat the counterfeit and substandard mobile devices including stolen/lost mobile devices.

I.III.III Sultanate of Oman

Of the mobile devices registered on the national network of Oman, almost two million have invalid IMEI codes. Some IMEI numbers have been repeated almost 10 times because more than 10 devices carry the same IMEI.[12] This creates a technical problem in terms of registering these devices on local networks and increases the financial burden on consumers in general, by undermining confidence in these products.

Regulators are keen to ensure that all off-the-shelf ICT devices from dealers and importers fully comply with relevant orders and decisions issued by the regulatory authority. To this end, the telecommunications regulatory authority (TRA) inspection body is responsible for ensuring compatibility and compliance with applicable standards and technical specifications for ICT equipment sold on the national market.

The TRA has set up a helpline together with local operators to enable customers to verify IMEI codes. Despite this, the organization still faces difficulties, including the lack of access to an international database of IMEI codes, because full access to the GSMA database is not granted to regulators, but only manufacturers and operators in a given country.

I.III.IV Islamic Republic of Pakistan

The Pakistan telecommunication authority has launched, in collaboration with Qualcomm, an open-source technology platform called the device identification, registration and blocking system (DIRBS) (see Figure I.13) to ensure that only approved, legal devices can operate on mobile networks in the country.[13] DIRBS allows the identification of all devices; captures an installed base of devices; monitors all new device activations; addresses illegal and counterfeit devices, including mobile thefts; and allows for exceptions/amnesties.

[12] ITU-D SG2 Document 2/326 from Oman

[13] More information is available on the PTA website: http://www.dirbs.pta.gov.pk/

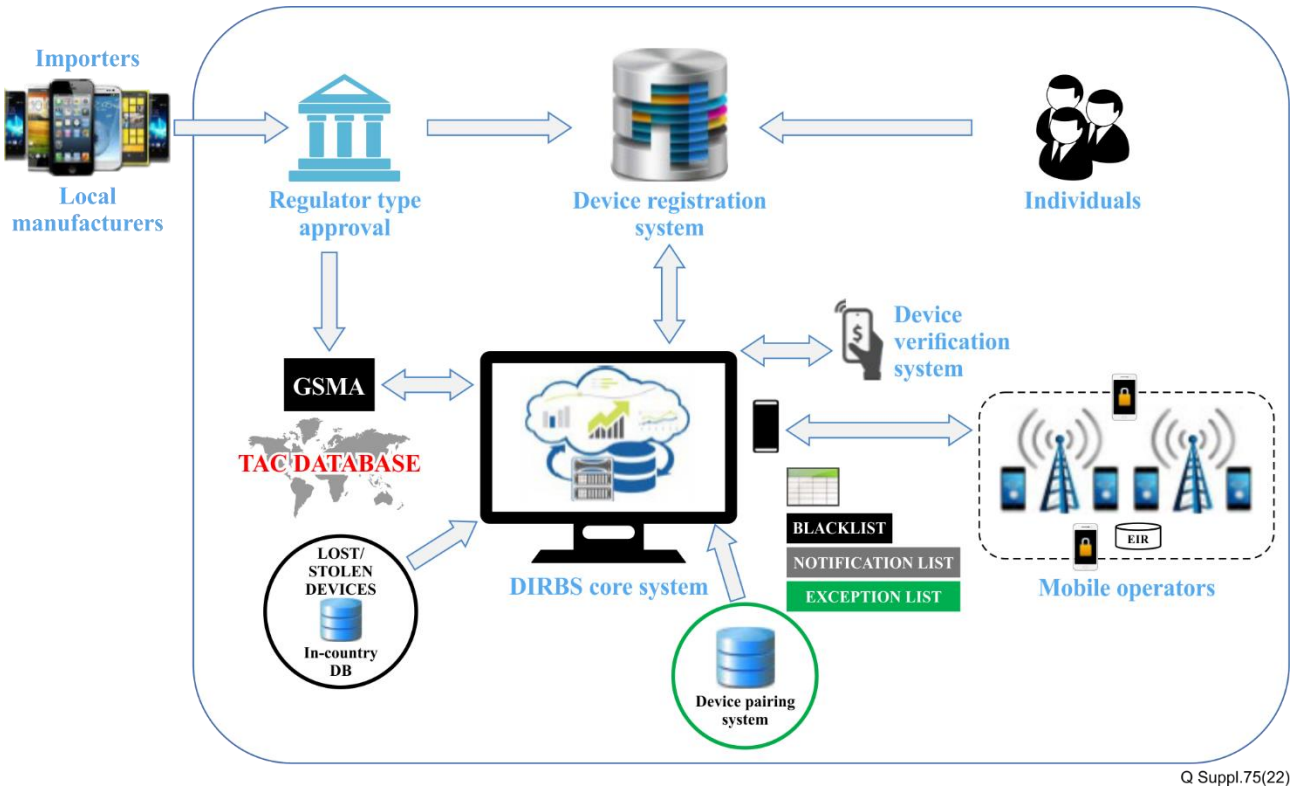


Figure I.13 – Device identification, registration and blocking system (DIRBS)

I.III.V Republic of Uzbekistan

- **Common information about use case**

1) Title of the use case

The UZIMEI – System of mobile devices IMEI codes registration in the Republic of Uzbekistan.

2) Location where the use case is implemented (country and/or private use case)

The Republic of Uzbekistan.

3) Dates of implementation of the use case (month/year)

1) Decree of the cabinet of ministers on 22 October 2018, № PKM-847 "On measures to organize the accounting system of mobile devices in the Republic of Uzbekistan".
2) March-April 2019: EIRs deployment (4 MNOs), www.uzimei.uz portal deployment.
3) 1 April 2019: start of auto-registration.
4) August 2019: finalizing UZIMEI requirements.
5) Decree of the cabinet of ministers on 17 September 2019, PKM-778 "On approval of the Regulation on the procedure for registration of mobile devices used, imported and produced for sale or personal use on the territory of the Republic of Uzbekistan".
6) 1 November 2019: start of mandatory free registration.
7) 1 December 2019: start of mandatory paid registration (payments are available through 2 payment systems and any bank).
8) February 2020: connecting one more payment system with CEIR.
9) April 2020: integration with interactive public services portal (my.gov.uz) – new online service for IMEI registration.
10) September 2020: additional verification of applicants, start of blocking stolen devices.

11) December 2020: connecting one more MNO with CEIR.

12) March 2021: allow individuals to register IMEIs at MNO offices.

4) Source (ITU associated): LLC Svyazcom.

- **Common statistics for country's use case**

1) Telecommunication statistic (e.g., number of users of mobile devices, operators, etc.)

The number of subscribers amounted to 23 million. In the year of project implementation there were four (4) mobile network operators.

2) Statistic of the problem (e.g., number of counterfeit devices, stolen devices, etc.).

The imports of mobile devices (handsets, smartphones, and tablets) are estimated at 3-5 million units. However, official customs clearance was carried out for a very small portion – less than 60 000 units.[14] Firstly, it led to a loss of customs and other payments. Secondly, it allowed imported devices to be sold at a lower price and therefore made the competition more difficult for a local mobile device manufacturer.

The share of devices with an incorrect IMEI was about 1 %.

The number of IMEIs suspected of being duplicated was more than 60 000 (spread over 3 million devices).

3) General statistics with regard to use case (e.g., size of the economy, population, etc.).

The population of Uzbekistan amounted to 33 million.

GDP of Uzbekistan: $6 999 (2019 est.).

- **Scope of the use case**

The following had been done to implement the project:

1) Adoption of the legislative framework of the project.

2) Conducting explanatory work among the population and market participants (operators, importers, manufacturers, retailers).

3) Selected a supplier who can supply all technical parts of the project: CEIR, several EIRs, public web portal for IMEI checking and registration.

4) Installed and activated EIR systems in each GSM network of Uzbekistan (four pieces). It was decided not to involve the two small CDMA networks in the project.

5) Deployed a public portal. At first it only provided an IMEI checking service, and then a registration function was added.

6) Developed and launched a CEIR implementing business processes in accordance with legal requirements.

7) Performed the integration of CEIR with customs and border services.

8) Performed the UZIMEI operator's staff training (system administration, analysis of business processes, reception of applications for IMEI registration from legal entities and individuals.

9) Performed the postal service employees' training (reception of applications for IMEI registration from individuals).

10) Performed the integration of CEIR with an interactive public services portal – a new online service was added for IMEI registration.

11) Creating of UZIMEI call centre.

12) A state acceptance of the system had been passed.

[14] https://mitc.uz/ru/news/1691

Since some of the importers have tried to circumvent mandatory IMEI registration, the UZIMEI system had to refine business processes for 1.5 years. Processes also had to be changed because of the pandemic COVID-19 (lockdown) and due to regulatory changes. Since all the parts of the UZIMEI system were from one supplier, it was possible to do it quickly.

- **Description of use case's solution**

To solve the main problems, it was decided to prohibit the use of the IMEIs in the cellular networks of Uzbekistan those that have not passed customs clearance. To implement this, an IMEI whitelist is created. In the networks of Uzbekistan MNOs, only those IMEIs, which are in the whitelist are allowed to be registered. IMEI can be included in this whitelist in the following ways:

1) All IMEIs that were found in the country's mobile networks before the system was launched were added to the amnesty list – this is part of the whitelist. For this purpose, EIRs were launched before mandatory registration. From 1 April, 2019 to 1 November, 2019, auto-registration was performed – EIRs allowed IMEIs into the network and sent them to CEIR, where they were placed on the amnesty list.
2) Only correct IMEIs were placed in the amnesty list (verification by the TAC list allocated by GSMA). Registrations of incorrect IMEIs were allowed until 1 November, 2019 and IMEI-IMSI bundles were created for these IMEIs – a bundle whitelist. For IMEI from these bundles, registration in the operator's network is allowed only if they are used with the same SIM cards (IMSI). After 1 November, 2019 registration and creation of new bundles for incorrect IMEIs is prohibited. This is how the distribution of counterfeit mobile devices was prevented.
3) The analysis of registration events from 1 April 2019, to 1 November, 2019 revealed duplicate IMEIs. For these IMEI, the IMEI-IMSI bundles were created – a bundled whitelist. For IMEI from these bundles, registration in the operator's network is allowed only if they are used with the same SIM cards (IMSI). In this way, the distribution of devices with duplicate IMEIs was prevented.
4) To add the IMEI of their devices on the whitelist importers must submit a customs declaration and pay the UZIMEI operator a fee for each IMEI. There can be no more devices in one application than in the declaration. One declaration can be used part-by-part – in more than one application for registration. CEIR is integrated with the database of the state customs committee to check declarations.
5) Local manufacturers have to pay UZIMEI operators a fee for each IMEI to whitelist their devices. They are allowed to submit IMEIs only with certain TACs.
6) Individuals must pay the UZIMEI operator a fee for each IMEI to put the IMEI of their devices on the whitelist. At the same time, compliance with the customs legislation is checked. The conditions are quite complicated, as it stipulates the cases when a person can import a mobile device for free. In other cases, the person must go through customs procedures and present a customs declaration or a customs receipt order. All these conditions are checked and controlled at the CEIR. For this purpose, the CEIR is integrated with the database of the state customs committee (checking the customs declarations and customs receipt orders) and the database of the state personalization centre (checking the method and date of entry of an individual into the country).
7) Foreigners can also apply for adding IMEI to the CEIR whitelist. Foreigners, like Uzbekistan citizens, have to pay the UZIMEI operator a fee for each IMEI. There are no customs clearance checks for foreigners, but there is a limit to the number of devices that can be registered to one foreign passport in a certain period.

IMEI that first occurs in the cellular networks of the country is automatically placed in the greylist. Starting from this moment, the time for IMEI registration (inclusion into the whitelist) starts at – 30 days. There is no restriction on access to the network in the greylist. Anyone can register IMEI – not

only those who used it first. Every new subscriber who uses an IMEI from the greylist will get a notification that it has to be registered, with a deadline. If no one registers an IMEI within 30 days, it is automatically moved to the blacklist.

Blacklisted IMEI is not allowed to register on the network. An IMEI is blacklisted in the following ways:

1) blocked at the request of law enforcement authority.

2) IMEI from the greylist, which were not registered within a certain period.

The following procedure is provided for blocking at the request of law enforcement:

1) The law enforcement officer writes an official letter to the UZIMEI operator, specifying the IMEI and a few parameters (to block or only to monitor, who uses the IMEI, from what date to block, whether to send a notification to the phone when it is registered).

2) UZIMEI employee creates an application in a special workplace of the interface, where all this information is entered. After that IMEI is placed in the blacklist from the specified date, or in the tracking list.

To exclude an IMEI from the blacklist, previously entered by the law enforcement authority, a similar procedure is used.

If an IMEI is blacklisted from the greylist, it can still go through the registration procedure: apply and pay for it. After that the IMEI number is removed from the blacklist and placed on the whitelist.

The rules for registration of mobile devices are described in the Decree of the Cabinet of Ministers No. 778 of 17 September, 2019. This Decree approves the regulation on the registration procedure for mobile devices used, imported and produced for sale or personal use in the territory of the Republic of Uzbekistan. The UZIMEI system, consisting of the CEIR system, several EIRs and the portal www.uzimei.uz now updated to https://new.uzimei.uz/ implements business processes in full compliance with this regulation. Basic information of the provision:

- Specifies for which devices it is not allowed to use in Uzbekistan networks (devices with incorrect IMEI and if IMEI is in the blacklist).
- Specifies for which devices the registration procedure is required (devices whose type according to the TAC GSMA database is defined as HANDHELD, MOBILE PHONE/FEATURE PHONE, SMARTPHONE, PORTABLE (INCLUDED PDA), TABLET).
- Specifies which devices do not require registration (all except those mentioned in the previous paragraph and when using a foreign SIM card).
- Specifies the ways to apply for IMEI registration:
    - For organizations (importers and manufacturers) – both via a personal visit to the office of the UZIMEI system operator and via the single portal of interactive public services.
    - For individuals – via a personal visit to the UZIMEI system operator's office, personal visit to the registrar's office (post offices), via SMS requests, via USSD requests, via the site www.uzimei.uz and via the interactive public services portal. However, for citizens of other states, the application can only be submitted through a personal visit to the office.
    - The maximum terms for processing of the application are specified.
    - Specifies at what moments the subscriber or applicant must be notified.
    - Provides application forms / questionnaires that must be completed when submitting an application when visiting the registrar's office.
    - The fees for whitelisting IMEI for different conditions are specified:
        – For importers

- For local manufacturers
- For foreigners
- For Uzbekistan citizens
- For Uzbekistan citizens (registration is overdue and IMEI is already on the blacklist)

Although the law specifies the maximum term for processing the application (the bill must be issued within one working hour), all checks are performed automatically, and the result is known to the applicant almost immediately. After the payment is received through the payment systems, the IMEI is immediately added to the whitelist, and the applicant is notified about it. Processing of payments made through the bank is automated only partially, so there is some delay for these cases.

MNO's EIRs are integrated with their SMSCs. Due to this UZIMEI can automatically notify subscribers in bulk, for example, in case of changes in the conditions of the service.

The www.uzimei.uz portal provides:

1) Information about the UZIMEI system
2) IMEI checking
3) Instructions on other ways to check the IMEI
4) Registration of one or more IMEIs of one device
5) Instructions on all the ways to apply for IMEI registration
6) Instructions on all the methods of payment of the application
7) Addresses of all customs offices where you can pass customs clearance
8) Addresses of all registration offices where you can apply
9) FAQs
10) Videos about UZIMEI

- **Statistic on the effects of the implementation of the use case**
  - The number of official importers increased by 2.7 times.
  - Revenues from imports of mobile devices increased by more than eight times.
  - The share of local producer devices in the market increased from 1.2 % to 1.7 %.
  - The number of counterfeit devices among phones, smartphones and tablets decreased by 98.5 % (CEIR statistics). No new counterfeit devices appear. The remaining 1.5 % are allowed because they were used before the launch of CEIR.
  - Whitelist:
    - Before November 1, 2019, more than 42.6 million IMEIs were automatically registered.[15]
    - During November 2019, 1.47 million IMEIs were registered for free.[16]
    - Assumptions about the volume of devices imported were correct: 3-5 million devices, each with an average of 1.5 IMEI.
  - The usual statistics for the month:
    - Registrations divided by type of applicant:
      - Importers – 52 %
      - Uzbekistan citizens – 42 %

[15] https://mitc.uz/ru/news/1690

[16] Ibid.

- Local manufacturers – 3 %
- Foreigners – 3 %

o Registrations divided by the manner in which the application was submitted:

- Personally at the UZIMEI office – 56 % (such a large portion because the importers use this method)
- At the uzimei.uz portal – 28 %
- Personally at the post office – 8 %
- SMS – 7 %
- USSD – less than 1 %
- Via interactive public services portal – close to 0 %

– IMEI of stolen devices are blacklisted at the request of the law enforcement agency, but the impact of this innovation on the number of stolen phones has not yet been studied.

• **Difficulties after starting registrations**

A large number of problems were created by the fact that most devices now have more than one SIM slot. This has created two types of problems:

1) There are phones that were in the country before November 1, 2019, but they have only one IMEI on the amnesty list. Although the population was constantly informed that it was necessary to insert SIM-cards in all SIM-slots of the device for their automatic registration, not all did so.

2) Customs clearance is performed on the device, but in the UZIMEI system separate IMEIs are registered. Therefore, if only one IMEI is registered in the application, then when a person wants to register the second slot, it will show up as, this customs document has already been used.

For both of these cases, it was decided to put such IMEIs on the whitelist for free. For cases of second SIM slot amnesty, an automatic solution was developed – so that a person does not have to come to the office for proceedings. Thus, additional automatic amnesties were conducted after November 1, 2019, and about seven (7) million additional IMEIs were added to the amnesty list. For the second slots of devices brought in after November 1, 2019, whitelisting was done manually, but later it was decided to implement this feature in the interface, so that it could be done by registrars, for regular applications.

The requirements for the system did not take into account the need for automatic verification of international mail and courier shipments. For devices that are now imported from abroad by mail, UZIMEI employees manually check the registration of the corresponding parcel on the mail portal.

Since the fees for Uzbekistan citizens and foreigners are different, EIR systems are integrated with the operators' billing systems, through which the owner of the subscriber number indicated in the application – resident or non-resident of Uzbekistan – is checked. However, due to fraud, it was necessary to add the sending of a one-time password to the number, so that applicants would not indicate other subscribers' numbers in the application.

When entering the country by air, one mobile device is allowed to be registered without customs clearance. This has led to the illegal use of other people's passport data. Someone who knows the passport data of someone who has entered the country uses it in his application. Because of this, the person who arrived could not later register their device without customs clearance. To solve the problem, they began to check the correspondence between the indicated subscriber number and passport data through the operators' billing systems.

- **Roadmap of future planned evolution of the use case**

The following enhancement of the UZIMEI system functionality is planned:

- Automatic check of international mail shipments
- Combating duplicate IMEI (currently in test mode only)

Connection of additional payment systems

I.IV Europe

I.IV.I Republic of Turkey

1 Common information about use case

1.1 Title of the use case

Mobile equipment registration system (Mobil Cihaz Kayıt Sistemi in Turkish – MCKS).

1.2 Location where the use case is implemented (country and/or private use case)

MCKS is located in the premises of the information and communication technologies authority (ICTA), the NRA of Turkey in Ankara. All devices having IMEI numbers, either imported, manufactured in Turkey, or brought from abroad by passengers, must be registered to MCKS in order to receive electronic communication services in Turkey.

1.3 Dates of implementation of the use case month/year)

MCKS was set up in 2006 according to repealed Law No. 5392. Currently, the system is operated by ICTA according to the Electronic Communication's Law No. 5809 and secondary legislation under ICTA's responsibility.

1.4 Source (ITU Member): ICTA – Turkey

2 Scope of the use case (including problems to be tracked such as counterfeit, stolen, tampered and/or cloned devices)

MCKS is composed of IMEIs of legally registered, unregistered, cloned, stolen, lost devices.

3 Common statistic for country's use case

3.1 Telecommunication statistic (e.g., number of users of mobile devices, operators, etc.)

Number of mobile operators: 3

Number of mobile service users: 74.206.085

Number of total mobile subscriptions: 80.790.877

3.2 Statistic of the problem (e.g., number of counterfeit devices, stolen devices, etc.)

For the stolen and lost devices and for the devices that have been taken without the consent of the user; the legal user can notify ICTA via e-government portal or by calling the short number of ICTA's consumer communication centre in order to prevent the device to receive services from the electronic communication network. Applications can be made to the judicial authorities, as well.

The number of applications (2018): 52.689

The number of applications (2019): 44.785

3.3 General statistics with regard to use case (e.g., size of economy, population, etc.)

GDP of Turkey (May 2020): 1.071.098.000.000 TL/ 176.146.000.000 USD

Total population of Turkey (83.154.997)

(Source: Turkish Statistical Institute)

4 Description of use case's solution

4.1 Overview of the solution

MCKS system is composed of three lists; the whitelist is composed of legally registered devices, blacklist is composed of stolen or cloned devices, and the paired whitelist is composed of IMEIs with special conditions.

4.2 Framework of the solution including diagrams and detailed description

MCKS is a multi-interface system in which close online/offline interactions with various ministries/public authorities take place. These parties include but are not limited to the Ministry of Trade, Ministry of Justice, Ministry of Interior, Ministry of Treasury and Finance (Revenue administration) and mobile operators in Turkey.

Operators feed the system with up-to-date usage information of the devices from their own network separately and these separate pieces of information flows to MCKS. This information is used for detecting clone devices as well as unregistered devices.

For devices brought from abroad, a cross-check is fulfilled by the Ministry of Interior's law enforcement agency units if the passport meets the criteria, and by the revenue administration, if the fee is paid.

For the imported devices, the process starts in the Ministry of Trade's single window system in which the IMEIs provided by importers are checked by MCKS via web services about their states in the database. If the provided IMEIs are listed in the blacklist, the importing procedure is not allowed. The same procedure is applied in the export procedure if the declared IMEIs are listed in the blacklist, the exportation is not allowed.

Ministry of Justice can inform the system via web service so that the related devices state can be updated according to trial decisions.

4.3 Description of additional measures taken to engage the problem MCKS is continuously being developed according to newly emerging regulatory needs. This makes the system even more complicated day by day

A regulation requiring the use of single window system of the Ministry of Trade during import and export caused some extra workload on the system as ICTA is given the responsibility to check the IMEI numbers according to their state of being lost, stolen or smuggled or being counterfeit via MCKS during import and export.

Another regulation, Law No. 7186 entered into force in July 2019, which regulates to blacklist devices, which are detected as unused for seven (7) consecutive years. The law is executed by MCKS and it targets the unused devices which are potential sources for cloning. However, some traders applied to the ICTA with the complaint that they suffer from the law since they have been holding devices that are not in use for over 7 years for various reasons.

4.4 References to open web resource for more details (optional)

https://mcks.gov.tr/en (English) https://mcks.gov.tr/ (Turkish).

4.5 Other relevant remarks (optional)

5 Overview of challenges and countermeasures with regard to implementation of use case

In the beginning, all devices within the borders of Turkey were asked to be registered by their owners with a fee via sending messages to their mobile operators. Citizens who were already using their devices did not welcome this. Over 15 million devices were registered during this period.

Until the system reached a certain level of maturity keeping importers in line with the new regulatory changes and authenticating them physically was bothersome. Currently, importers are using their electronic signatures for authentication after completing the importing procedure via the single window system of the Ministry of Trade.

6 Statistics on the effects of the implementation of the use case

Mobile device theft was decreased by 90 % in the first three years of implementation. Nearly 35 million mobile devices were sold illegally between 1996 and 2005, which represented a three billion tax loss that was prevented by MCKS after 2006. In addition, consumer awareness has increased, and illegal devices became non preferred by consumers.

7 Roadmap of future planned evolution of the use case

Even though most of the services of MCKS are provided to the citizens via the e-Government portal; the ultimate aim is to be able to provide all the services online via e-Government and to end the submission of physical supporting documents. Due to the necessities of the new regulations, sometimes it takes time for some relevant authorities to keep pace with MCKS and to provide all the services online to the citizens.

8 Final remarks and conclusion

Battling with theft and smuggling of mobile devices is a big challenge for public authorities around the world. In the case of theft, device owners are not only losing their valuable property, but are also placing themselves in danger of physical harm. If the stolen devices are disabled quickly, device theft becomes much less attractive for thieves and fewer people come under the risk of being harmed because of their mobile devices. In Turkey, MCKS had a very positive impact in the battle against device theft. In addition, smuggling of mobile devices which causes a great deal of tax loss has decreased in Turkey. Other special conditions aiming to hinder tax loss and directing consumers to the internal market are considered to be met thanks to MCKS.

I.IV.II Ukraine

1 Common information about use case

1.1 Title of the use case

There are no official names for scenarios on the combat of counterfeit ICT and stolen mobile devices.

1.2 Location where the use case is implemented (country and/or private use case)

The implementation of national scenarios usually takes place in Ukraine centrally and covers the entire country.

1.3 Dates of implementation of the use case: since 2009

1.4 Source (ITU Member): Administration of Ukraine

2 Scope of the use case (including problems to be tracked such as counterfeit, stolen, tampered and/or cloned devices)

In 2009, a generalized database of international identifiers of terminal equipment imported from abroad was introduced based on the UCRF, which also provided for the use of separate modules to combat counterfeit and stolen mobile devices. Due to the abolition of licenses for the import of electronic devices at the legislative level in 2014, the obligation to enter the IMEI codes of imported terminals was abolished, which led to the actual cessation of the provision of data by importers to this database. The current procedure for importing from abroad and the sale of electronic means and radiating devices in Ukraine stipulates that importers including citizens, have the right to apply to the UCRF with a corresponding application (notification) for registration of international terminals of IMEI after completion of customs procedures, which are imported into Ukraine as per the requirements of the customs code. Currently, data entry is carried out on a voluntary (optional) basis, which leads to a lack of relevant and complete information in the database. The existing system needs to be replaced or significantly modernized due to changes in the legal, technological, and technical requirements.

3 Common statistics for country's use case

3.1 Telecommunication statistic (e.g., number of users of mobile devices, operators, etc.): The number of active identification telecommunication cards in the mobile networks as of 31 December 2019, amounted to 54 843 thousand units.

3.2 Statistic of the problem (e.g., number of counterfeit devices, stolen devices, etc.): There are no statistics on the number of counterfeit devices used in mobile networks. The average annual number of stolen mobile devices is about 100 thousand units. (according to open sources of information).

3.3 General statistic with regard to use case (e.g., size of the economy, population, etc.): The number of the available population of Ukraine on 01.03.2020 is 41 858 119; Gross domestic product for 2019 amounted to UAH 3 974 564 million, of which in the section "Information and Telecommunications" – UAH 179 246 million; Gross national income amounted to UAH 4 097 674 million.

4 Description of use case's solution

4.1 Overview of the solution: The main attention in the implementation of the system in 2009 was paid to combat the smuggling of equipment. IMEI codes were used to create a database of devices that were illegally imported into Ukraine. The following lists were maintained: a "white" list of devices that were legally imported, a "gray" list of devices of unconfirmed status, and a "black" list of devices that were not to be serviced. Access to this database was provided to regulatory and customs authorities, network operators, and the general public with access rights of the appropriate level.

4.2 Framework of the solution including diagrams and detailed description: The introduction of the system in Ukraine ensured the legalization of the terminal market and led to a sharp reduction in the "gray" (illegal) import of mobile devices to Ukraine.

4.3 Description of additional measures taken to engage the problem:

4.3.1 Consumer protection. Each buyer had the opportunity to check the legality of the mobile terminal before purchasing it. This could be done by using the official website of the UCRF or by sending an SMS with the IMEI code of the checked terminal to the number "307", common to all mobile operators. A few seconds later, the response provided the status of the requested IMEI code in the shared IMEI database. This

provided protection of the Ukrainian market from terminals that do not meet the requirements for their use in Ukraine. The current Ukrainian legislation at that time prohibited the sale of mobile terminals with IMEI codes that were not registered in the general IMEI database.

4.3.2 Combat terminal theft. The IMEI codes of stolen terminals were blacklisted at the request of law enforcement, which made the theft of terminals useless. The same procedure was used to block terminals at the request of owners of lost phones.

4.3.3 Cessation of illegal imports. At the first connection to the network of any operator, any terminal was immediately registered in the corresponding network. The IMEI codes of the terminals served by the operator's network (except for those that were on international roaming) were automatically sent on time (at night) by mobile operators to the general IMEI database. The system detected IMEI codes that were not in the "white" list of the generalized IMEI database and such IMEI codes were registered in the "gray" list. All owners of the respective terminals received via SMS a warning about possible blocking of the terminals within 90 days. At the end of the 90 days, the IMEI code was transferred from the "gray" list to the "black" list. Terminals from the "black" list were not to be serviced by operators (a refusal to register in the network, except for urgent calls to the number "112"). Connection to the network of any other operator did not change the status of the "gray" or "black" terminal. After receiving an SMS warning about inclusion in the "gray" list and a limited 90-day service period, the owner had the opportunity to contact the UCRF to confirm the legal import of this terminal. UCRF staff reviews the owner's application and, in case of confirmation of the legal nature of the import, transferred the IMEI code from "gray" to "white" list. After this procedure, mobile operators would start servicing the terminal without any time limits.

4.4 References to open web resource for more details (optional):

Report on the work of the NCCIR for 2019:

https://nkrzi.gov.ua/images/upload/142/9088/Zvit_2020_NKRZI.pdf

Accounting and maintenance of international identifiers of terminal equipment:

https://www.ucrf.gov.ua/ua/services/vvezennya-v-ukrayinu-radioelektronnih-zasobiv-ta-viprominyuvalnih-pristroyiv

State statistics service of Ukraine:

http://www.ukrstat.gov.ua/

The automated information system of accounting of mobile terminals in the territory of Ukraine.

https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-CCICT-2015-PDF-E.pdf.

4.5 Other relevant remarks (optional): The system brought significant positive results, but since the terminals included in the "black" list were not disconnected from the networks, it later lost its effectiveness and at the legislative level, the introduction of IMEI codes in 2014 became voluntary.

5 Overview of challenges and countermeasures with regard to implementation of use case

Given that the system was built in 2009, nowadays it needs to be upgraded and/or replaced to make it technically possible to fully implement the ITU-T Q.5050 series of Recommendations. These measures may be taken only after appropriate amendments have been made to existing national legislation.

6 Statistic on the effects of implementation of the use case

Results of the system implementation in Ukraine in 2009-2014: "Gray" (illegal) imports of mobile terminals to Ukraine decreased sharply. The share of legally imported mobile terminals increased in 2010 to 93-95 % (compared to 7.5 % in 2008). From 2010 to 2012, the state budget of Ukraine received revenues for more than $ 500 million in the form of customs import duties on mobile terminals compared to $ 30 million for the previous three years. The Ukrainian market of mobile terminals consisted mainly of mobile terminals that met the technical requirements for use in Ukraine. As of 30 April 2013, 140 865 260 IMEI codes of mobile terminals were registered in the general IMEI database. The system became profitable in just seven months due to the funds received by the UCRF from the payments of importers.

7 Roadmap of future planned evolution of the use case

Currently, in Ukraine, certain bills provide for the elimination of some problematic issues that have arisen in recent years in the field of telecommunications. The introduction of a new system that will effectively combat counterfeit ICT devices and the use of stolen mobile devices in accordance with ITU-T Q.5050 series Recommendations or the modernization of the existing one will be possible after the relevant amendments to the legislation.

8 Final remarks and conclusion

In the implementation of such a scenario, it is important at the legislative, technical, and technological levels to ensure unconditional long-term implementation of all stages envisaged in the system design process. Otherwise, the scenario will not work effectively to combat counterfeit ICT devices and the use of stolen mobile devices.

Appendix II

Private sector and NGO initiatives

II.I The GSM association

The GSM association (GSMA) manages the international mobile equipment identity database, a global central database containing basic information on the serial number (IMEI) ranges of millions of mobile devices.[17]

GSMA provides a "device check" service to device traders, recyclers and insurers, and to law enforcement agencies (in some markets, consumers can also access the service directly). It allows users to find out instantly whether a device has been reported lost or stolen through the device status registry, as reported to the GSMA by its mobile network operator members worldwide.

GSMA seeks to connect as many mobile network operators as possible to the IMEI database.

In September 2016, the GSM association partnered with the World Customs Organization to combat counterfeiting and fraudulent mobile commerce. The integration of the IMEI database will facilitate cross-checking and filtering of counterfeit devices identified by their IMEI at the point of import.

[17] ITU-D SG2 Document SG2RGQ/80 from the GSM Association (GSMA)

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, 2022