International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5051

(03/2020)

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

Combating counterfeiting and stolen ICT devices

Framework for combating the use of stolen mobile devices

Recommendation ITU-T Q.5051

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
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	**Q.5050–Q.5069**

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

Recommendation ITU-T Q.5051

Framework for combating the use of stolen mobile devices

Summary

Recommendation ITU-T Q.5051 proposes a framework composed of requirements and a broad range of comprehensive and recommended measures that can be taken and applied to combat the theft and reuse of stolen mobile devices.

With the increased functions and capabilities available on mobile devices, the importance and usage of these devices in people's daily lives have been growing in recent years. As a side effect, there also has been observed a rise, in some countries, of actions aimed to steal these devices and generate profit, not only by selling the equipment itself but also by illegally using the information it contains.

As a response, initiatives are needed to deter the theft and reuse of stolen mobile devices and to protect the consumer data stored on these devices against illegal use. It is common for devices stolen in one country that may have deployed solutions to mitigate the use of stolen devices to then be sold into other countries or regions where similar mitigation measures have not been taken. Thus, it is critical to the success of such initiatives to have coordination and information sharing among governments and operators that aims to combat the theft and reuse of stolen mobile devices in a global environment. Otherwise, there is a risk of the illegal trade of stolen devices occurring across international borders.

Note that most solutions deployed today to deter the device theft and reuse problem rely on unique identifier lists. A common action taken by the traffickers then to bypass these actions is to tamper with the device to alter its unique identifier, sometimes choosing an identifier already in use by a legitimate device. This allows the equipment to return to the market and connect to mobile networks.

In response to this scenario, many countries are engaged not only in combating the use of stolen mobile devices, but also in preventing devices with unauthorized reprogrammed unique identifiers, commonly described as tampered identifiers, from returning to the network. Meanwhile, governments in other countries are challenged and unclear on the best strategies to adopt, mainly due to a lack of knowledge or expertise to understand the issue and the possible solutions, and to make informed choices to deploy solutions, tailored for their individual countries, that could be effective. In this sense, guidelines are necessary to address this challenge, as indicated on the WTSA Resolution 97 (Hammamet, 2016).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5051	2020-03-13	11	11.1002/1000/14140

Keywords

Combatting stolen mobile devices, conformance, framework, requirements, security.

---

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Q.5051

Framework for combating the use of stolen mobile devices

1 Scope

This Recommendation contains the reference framework and requirements that should be considered when deploying solutions to combat the use of stolen Mobile Devices.

2 References

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

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

[ITU-T X.1058] Recommendation ITU-T X.1058 (2017), *Information technology – Security techniques – Code of practice for personally identifiable information protection.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 kill switch [b-GSMA]: A "kill switch" is a way to disable crucial functions of a mobile device. It is essentially a function within the mobile equipment, so that if triggered, e.g., by a message of some format is sent to it, then the mobile will cease to operate as it is intended to, and can only be reactivated or reused if the device owner authorizes the reactivation of the device.

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

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

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 Recommendation

This Recommendation defines the following terms:

3.2.1 invalid identifier: Is a unique identifier that does not comply with the format defined in the technical standards or that is not included in the device identifier reference database distributed by responsible management entity.

3.2.2 cloned identifier: Is a valid device identifier properly assigned by the responsible management entity to one device but is being used by other different devices.

3.2.3 reliable unique identifiers: 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

EIR Equipment Identity Register

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

PII Personally Identifiable Information

RUI Reliable Unique Identifier

TAC Type Allocation Code

5 Conventions

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

a) the keyword "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed;

b) the keywords "should" and "is recommended" indicate requirements which are recommended but which are not absolutely required. Thus, this requirement need not be present to claim conformance;

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

6 General aspects

With the increased functionality and capabilities available on mobile devices, the importance and usage of these devices in people's daily lives have been growing in recent years. As a side effect, there also has been observed a rise, in some countries, of actions aimed to steal these devices and generate profit, not only by selling the equipment itself but also by illegally using the information it contains.

As a response, initiatives are needed to deter the theft and reuse of stolen mobile devices and to protect the consumer data stored on these devices from being illegally used. It is common for devices stolen in one country that may have deployed solutions to mitigate the use of stolen devices, to then be sold into other countries or regions where similar mitigation measures have not been taken. Thus, it is critical to the success of such initiatives to have coordination and information sharing among governments and operators from different countries that aims to combat the theft and reuse of stolen

mobile devices in a global environment. Otherwise, there is a risk of the illegal trade of stolen devices occurring across borders being unintentionally facilitated.

In response to this scenario, many countries are engaged not only in combating the use of stolen mobile devices, but also in preventing the devices with unauthorized reprogrammed unique identifiers, commonly described as tampered identifiers, from returning to the mobile network. Meanwhile, governments in other countries are challenged and unclear on the best strategies to adopt, mainly due to a lack of knowledge or expertise to understand the issue and the possible solutions, and to make informed choices to deploy a solution, tailored for their individual countries, that could be effective. In this sense, recommendations are necessary to address this challenge, as indicated on the World Telecommunication Standardization Assembly (WTSA) Resolution 97 (Hammamet, 2016).

Therefore, this Recommendation describes a framework composed of requirements and a broad range of comprehensive and recommended measures that can be taken and applied to combat the theft and reuse of stolen mobile devices.

7 High level requirements

A number of challenges are faced by stakeholders when deploying solutions to address the use of stolen mobile devices. When deploying solutions to combat the use of stolen mobile devices, countries should consider the requirements in this clause.

7.1 Preventing stolen mobile devices from being used by unauthorized user

It is required to implement solutions that aim to deactivate devices, in case they are stolen or lost, rendering them inoperable to unauthorized users.

It is required that this process occurs automatically after an unauthorized user attempts to access the device some determined number of times (e.g., if the unauthorized user fails to enter the correct user password or personal identification number (PIN) after a certain number of attempts).

It is recommended that this process be capable of being activated remotely by the authorized device user when requested (e.g., by triggering a kill switch function on the lost/stolen device).

It is required to have the option to reverse the inoperability if the device is recovered by the authorized device user and to restore user data on the device to the fullest extent feasible.

[ITU-T X.1127] addresses the functional security requirements and architecture for mobile phones based anti-theft measures. That Recommendation describes the implementation of a kill switch tool for use in the event of a smartphone being lost or stolen. Such a tool should provide the capability to:

- remotely delete the authorized user's data that is stored on the smartphone;
- render the smartphone inoperable to an unauthorized user;
- prevent reactivation without the authorized user's permission to the extent technologically feasible;
- reverse the inoperability if the smartphone is recovered by the authorized user, and restore user data on the smartphone to the fullest extent feasible;
- provide location tracking of the lost or stolen mobile device.

It is recommended to educate mobile device users on how to configure and use this functionality and to report their lost/stolen mobile devices to their service providers or relevant police or judicial authorities in order to prevent the devices from accessing mobile networks and to enable law enforcement agencies to take appropriate actions.

7.2 Preventing stolen mobile devices from accessing the network

It is required to implement solutions to prevent stolen mobile devices from accessing the mobile networks, preferably through automated systems that are auditable.

It is required that only authorized persons, such as the legitimate owner of the device, be able to request the inclusion or removal of a stolen mobile device from all networks in the country.

It is recommended to develop a policy framework to prevent stolen devices from being used on the network.

It is important to note that devices blocked on mobile networks, using their unique identifiers, can still access networks that do not check mobile device unique identifiers, such as wireless fidelity (Wi-Fi) networks. Thus, it is important to complement this approach with others such as those described in clause 7.1.

7.3 Preventing the use of mobile devices with tampered and/or cloned unique identifiers

It is required to implement a solution to identify mobile devices with tampered and/or cloned unique identifiers and to differentiate them from genuine devices, with considerable accuracy, in order that disruptive actions can be taken, preferably through automated systems, with no impact on the genuine devices.

It is recommended that reference databases are part of this solution in order to identify information pertaining to genuine devices and the legal origin of these genuine devices. National registration databases that identify legally imported and acquired devices, and databases of unique identifiers allocated to manufacturers and other characteristics of these devices should be used as the source of information for reference databases to facilitate the differentiation of genuine devices from the tampered ones.

It is required to consider in this solution that a tampered unique identifier could require different typologies to be addressed in the detection and control process, such as: invalid identifiers, cloned and, when applicable, non-type approved or not registered in national reference databases.

7.4 Preventing stolen mobile devices from other countries to access the network

It is recommended that local laws and regulations facilitate the coordination and information sharing between the governments and operators from different countries to prevent the use of stolen devices, regardless of where they were stolen.

Failure to encourage and facilitate international data sharing allows the illegal international trade of stolen devices to continue unchecked, resulting in devices stolen in one country being exported to and sold in other countries or regions.

It is recommended that a global database of stolen devices be accessible to all constituents from anywhere in the world for reporting a stolen device and checking the status of a device in order to address and solve this issue.

Local national device blacklists should be exchanged and made available to the global community by requiring the connection and exchange of local stolen device data with the global database of stolen devices.

7.5 Reduce consumer impact

Consumer impact should be considered when adopting any solution against the use of stolen mobile devices. When multiple approaches are available to consumers to achieve the same objective, adopt the one that reduces the overall impact on legitimate consumers.

It is recommended that devices with invalid identifiers newly active in the network are controlled and provide prior notification to users, giving sufficient and proper time to present proof of legal acquisition, and to reduce or avoid the impact of these devices from suddenly being denied service.

It is recommended to avoid blocking the user service subscription when measures are taken to control devices with tampered and/or cloned identifiers.

It is recommended that educational and awareness campaigns be publicly disseminated by all means about the measures to be taken, their aims, their benefits and the options and actions that users can take if their handsets are lost or stolen, or if they acquire devices with tampered or cloned identifiers.

It is recommended that when adopting measures against devices with tampered and/or cloned identifiers, that amnesty or transition periods be considered. Devices that are already in use could have been acquired in good faith and their users be unaware of the risks. If it is decided to not block legacy devices, additional measures should be taken to avoid these devices from being activated by new users.

It is recommended to establish efficient ways to take reports and information from users and to take actions to proceed with the suspension of services and the blocking of device identifiers.

It is recommended to facilitate the establishment of the identifier of the device to be blocked without requesting the user to remember or look for it, for example, by seeking the call record activity of the device in the operator's network to determine the lost/stolen identifier.

It is recommended to suspend the services and to block the identifiers of the lost/stolen devices as soon as possible. For example, block the device as soon as the request is validated by the stakeholders responsible for blocking the device.

It is required to provide tools for the all stakeholders to check and verify if a device has been blocked.

It is recommended that the stakeholder responsible for blocking a device respond to the user when the device is blocked or with reasons why the reported device may not be blocked if the request is refused.

7.6 Protect consumer private data

Consumer private data should be protected in the event that a device is lost or stolen. As a primary action, it is recommended to implement mechanisms to disallow the operation of the device including access to the private data held on it by an unauthorized user.

It is recommended to educate consumers on the importance of protecting and backing up their personal data, and on how to use the functionalities that allow them to remotely wipe personally identifiable information (PII) on the stolen device.

It is recommended that [ITU-T X.1127] features be included by manufactures on all new devices by default.

It is recommended that stakeholders educate consumers on how to configure and use this functionality.

7.7 Preventing stolen mobile devices from accessing the markets

It is recommended that telecommunications national regulatory agencies collaborate with other relevant national agencies (e.g., customs) to improve controls for devices reported as lost or stolen nationally and in other countries.

As part of this collaboration, providing the following should be considered, where applicable:

1) access to stolen devices databases but also, since it is possible to alter the unique identifier to bypass the national and international stolen databases, additional information such as invalid, non-type approved devices;
2) access to a global database of identifiers that have been allocated to legitimate manufacturers, in order to validate if the structure of the identifiers belonging to devices to be imported;
3) access to the list of type approved device brands and models to allow the importation only of type approved device models, according to relevant national regulations;

4) access to the national reference databases with a record of the legally imported and acquired device identifiers, as applicable;

5) access to a global database of stolen devices along with access to a database that provides device specific information to be able to confirm the authenticity of devices. The latter would be beneficial in scenarios where a stolen device's unique identifier may have been altered and reprogrammed with an identifier that represents a different device.

It is recommended to scrutinize the complete identifier against the national device database to avoid the entry of a device with an identifier that belongs to another device that has already entered the country.

It is recommended to take legal actions against point of sales that offer for sale stolen devices.

7.8 Other considerations to address the tampering of stolen mobile devices unique identifiers

Other considerations to address tampering of stolen mobile devices may include:

- consider developing policy frameworks to prevent tampered stolen mobile devices from being used or sold in the market;
- provide education and training on the technical aspects related to the theft and tampering of unique identifiers of mobile devices;
- consider controls on the use of hardware and/or software used to tamper the mobile devices identifiers.

It is recommended to have legal grounds and support to allow law enforcement authorities to penalize those who change, modify, alter, erase or tamper with the identifiers of mobile devices with the objective to circumvent the actions to prevent stolen devices to be used in the market.

It is recommended that such a legal framework also covers actions that can be taken against those who offer, possess, import or sell hardware and/or software used to tamper with the mobile device identifiers.

It is recommended that law enforcement authorities are educated and trained on the technical aspects related to the theft and tampering of unique identifiers of mobile devices, and the legal framework to allow for the prosecution of offenses.

It is recommended for manufacturers of mobile devices to include mechanisms to ensure the reliability and integrity of mobile device unique identifiers.

8 Framework requirements

When deploying solutions to address stolen mobile devices, the following requirements should be considered.

8.1 Centralized reference database

It is recommended to use a centralized reference database to store the information of lost and stolen devices. Therefore, all carriers should make use of this database to prevent stolen devices from accessing any mobile network. This database should contain, at least, the unique identifier of the stolen device, the date of the event and the entity that included the information on the database.

It is recommended that such a database also includes other types of identifiers and information to assist identifying and address stolen devices with tampered identifiers.

It is recommended to include information related to legally imported and/or acquired devices in this reference database.

It is recommended that authorized entities have access to all relevant databases.

It is recommended to implement mandatory device registration. When implementing mandatory device registration, care should be taken when linking the device with PII and the side effects on the trade of legal mobile devices and mobile market competition.

It is recommended to implement audit procedures to verify if reported stolen devices have been blocked and if the correct procedures have been adopted by all the stakeholders.

8.2 Network support for blocking the devices

It is required that mobile networks should contain elements capable of preventing access by stolen devices whose valid identifiers were included on the blacklist and also for those devices that transmit identifiers with a format that do not comply with the standards for unique identifiers[1].

It is recommended that blocking solutions used in mobile networks should support features to avoid the use of devices with cloned unique identifiers and therefore differentiate genuine devices from cloned ones[2].

8.3 Reliable unique identifiers

It is recommended that the reference databases used to prevent stolen mobile devices from accessing mobile networks be based on reliable unique identifiers (RUIs), since tampering with the device unique identifiers can negatively impact the efficiency of solutions that aim to remove the stolen devices from the market.

It is recommended that mobile devices store[3] their unique identifier in a secure element within the equipment and that the device implements security measures, to the extent technologically feasible, to detect the tampering of the secure element or the information stored in it, and as a result, render the device inoperable until and unless the original data are restored.

It is recommended that the management entity responsible for the unique identifiers implement a process that incentivizes the correct and secure use of unique identifiers by legitimate device manufacturers to which identifiers have been allocated.

It is recommended that unique identifiers comply with integrity principles (any and all manufacturers must have allocated identifier ranges from the designated entity) and industry defined security principles (all set measures or a combination of them to implement the identifiers in such a way that tampering with them is not possible)[4].

It is recommended that the processes that industry have in place to enforce these principles are supported by governments or national regulatory frameworks.

It is required that unique identifiers are not reprogrammable, even during maintenance service. Allowing identifiers to be changed after the manufacture process may reduce the security of the unique identifier, allowing it to be tampered by unauthorized third parties.

8.4 Close collaboration with law enforcement agencies and other domestic agencies

To effectively limit the circulation of stolen devices on the market, it is required to establish a close collaboration between the entities responsible for maintaining and providing reference databases, the national customs agencies and between these entities from distinct countries and relevant stakeholders. Consider the following:

---

1 See [b-3GPP TS 122.016] and [b-3GPP TS 123.003] for 3GPP/3GPP2 compliant devices.

2 For 3GPP/3GPP2 compliant devices, when using IMEI as the unique identifiers, the support of IMEI-IMSI check from the radio access network to the core network can assist on this requirement.

3 For example, [b-3GPP TS 122.016] defines that the IMEI shall not be changed.

4 For example, see [b-IMEI-SEC] for 3GPP compatible mobile device.

- since, customs agencies and other relevant national authorized agencies play a critical role in the surveillance and interception of stolen, lost or tampered products, it is important to give them the tools to identify stolen, lost, tampered and even legal devices, such as via a centralized reference database;
- enforcement procedures and communication between different organizations must be established and fully operational. This could include the exchange of relevant information, such as the databases of mobile devices in conformance with the national, regional or international standards;
- the illegal trade of stolen mobile devices can be combated by employing mechanisms to authenticate the identity of an individual device to check that it is the genuine article and if it is permitted for use by the laws and regulations of that country;
- law enforcement agencies, based on national legal frameworks, may choose to not immediately block devices for investigation purposes in order to identify the origin of the stolen devices being sold on the market although preference should be given to blocking all devices as quickly as possible unless there are valid and exceptional grounds not to do so in individual cases.

It is recommended that high level lead-strategy comes from the top of the government to drive the alliances and comprehensive set of measures in order to facilitate the commitments and execution of activities from different sectors and authorities separate from industry (e.g., law enforcement, customs, commerce, etc.).

8.5 Tools to check the status of mobile devices

It is required to make available a public tool for consumers and other stakeholders to check the status of mobile devices. Consumers and other stakeholders should be able to check, preferably using the Internet, if certain devices are flagged as stolen or lost.

It is recommended that the entity responsible for blocking a device be listed in the response to a device check (including the country in which the blocking was applied) to make it possible for the consumer to avoid purchasing or acquiring stolen devices and also to address complaints in case an incorrect block or a third-party block caused by a cloned device with the same identifier. Also, this is an important tool for the consumer for pre-purchase checking.

It is recommended that retailers and entitles involved in handling devices carry out checks on devices they acquire to ensure those devices have not been reported lost, stolen or with a duplicated unique identifier. Records should be maintained to prove due diligence was observed to mitigate the possibility of trading devices that have been reported lost, stolen or with a duplicated unique identifier.

8.6 Support of applicable national legal and regulatory frameworks

It is recommended to develop mechanisms to identify and block lost and stolen devices and also devices with tampered unique identifiers in the mobile network, where the technical capability exists to do so. This should be checked with the local mobile network operators.

It is recommended to have the support of applicable national legal and regulatory framework before implementing any restrictive actions against stolen devices with tampered and duplicated unique identifiers, covering:

- the restriction of network access to stolen devices on telecommunications networks, either reported nationally or in other country;
- the restriction of network access to devices with tampered identifiers on telecommunications networks;

– the restriction of tampering with mobile devices unique identifiers, and the consequences to do it;
– the establishment of the necessary solutions for the differentiation between authentic and stolen tampered devices by authorities, consumers, and the sales channel;
– having an authority responsible for the enforcement of the above points.

When considering this requirement, due reference should be given to existing national legislation and regulatory frameworks that may already address aspects covered.

9 Reference framework

Based on the framework requirements outlined in clause 8, a proposed reference framework to combat the theft and use of mobile stolen devices is depicted in Figure 1. It is important to note that not all functional elements described in Figure 1 are required and each country could implement elements according to their needs.

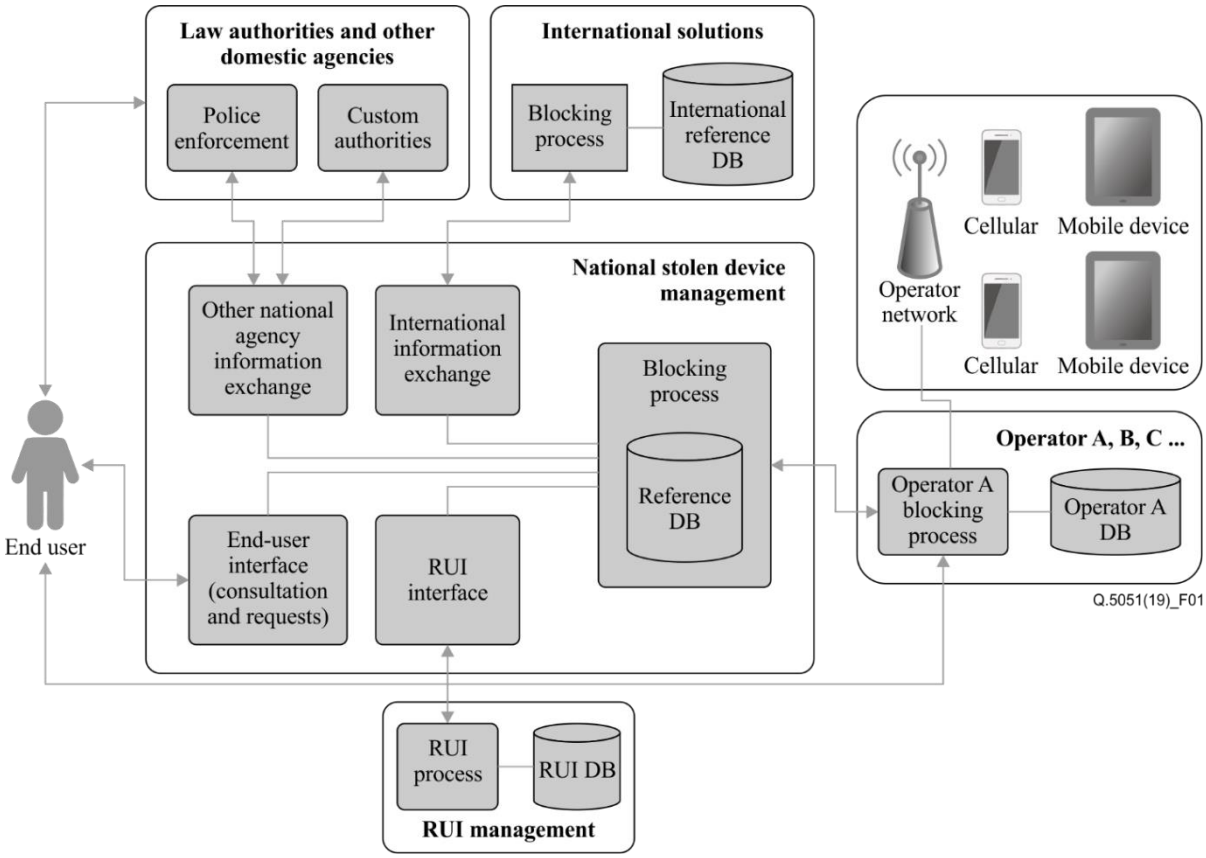

Figure 1 – Proposed general framework

A diverse range of activities and information systems, operated by different organizations, should work together to control and produce critical information to identify and combat the use of lost and stolen mobile devices and with those with invalid identifiers.

Consumer and other stakeholders should be able to check if a certain device is flagged with any restriction (stolen, lost or with an invalid identifier).

A request for blocking a stolen device could be submitted through different stakeholders (consumer, law enforcement agencies, mobile operator or direct to the central system). Regardless of where the request to block the devices in use is submitted, actions should be made to validate the user identity and also device ownership. For those devices that have not been sold to the consumer, e.g., those

stolen in transit, from retail outlets, etc., a legal denounce should accompany the request to block the device.

To limit the circulation of stolen devices in the market, other relevant national agencies (e.g., law enforcement and customs agencies) should have the ability to check device status using all available references databases and sources.

Exchange with international entities is also critical and can be done on a bilateral basis or with a global reference database.

To guarantee the effective blocking of stolen devices on the country mobile networks, all operators should be synchronized with a national and global reference database.

It is required to have a RUI management integrated with the stolen mobile blocking process because it is possible to tamper with the unique identifiers of some devices to bypass the blocking process.

It is required to implement a process to identify and control mobiles devices with invalid identifiers on the networks that could be the result of tampering of a stolen device after it is blocked.

10 Desirable features

When deploying a solution to combat the use of stolen mobile devices, countries should considerer the desirable features in the following clauses.

10.1 Lost and stolen devices global reference database

Because blocked devices can be transported or even sold to consumers in different countries, it is recommended to use a global reference database to conduct the sharing and blocking of lost and stolen devices identifiers in order to blacklist the stolen devices in a single point of information that facilitates sharing and reduce the times for blocking.

It is recommended that, regardless of the operator size, all devices with identifiers in this global reference database should be prevented from connecting to the local network. However, alternative approaches could be considered depending on the specific environment of each implementation (e.g., batch processing of active unique identifiers against the global reference database).

It is required that the global reference database to be available for law enforcement authorities and other government agencies for report and query groups of identifiers in order to facilitate their legal actions in the combat of theft of mobile devices.

It is recommended that the information to be reported to the global database be verified for the accuracy of the devices being reported stolen. Only after such verification, the stolen device lists compiled by the parties mentioned above should be provided for inclusion into this global stolen device database.

This global database should be available to all stakeholders from anywhere in the world to verify whether a device has been reported stolen. The access to the database should be available both at the system level, to parties that can block stolen devices, and at the consumer level, where consumers from any country should be able to check whether the device has been reported stolen.

The global database should provide appropriate information if available (e.g., device characteristics, country where the device was stolen, date of event, etc.). If the stolen device identifiers were found in multiple countries, the global database should provide that information in its results.

Procedures should be implemented so that the participants of the global database can address unintended blocking (e.g., erroneous blocking, blocking related to duplicated and cloned devices identifiers).

10.2 Actions regarding establishments that sell lost, stolen or tampered devices

It is recommended that countries consider a framework that establishes the responsibilities of points of sale to only offer type approved devices for sale and the consequences of offering stolen devices or devices with tampered identifiers. This will empower law enforcement agencies with the legal support to combat the sale of and demand for those devices.

It is possible to include on the national reference database the identifiers of legally imported and sold devices. This database could assist a variety of national enforcement actions and activities such as importation, sales, use in networks and law enforcement authority's actions, etc.

Therefore, this could assist law enforcement agencies with access to this database of authorized devices to take actions against establishments offering stolen, tampered or cloned devices to the public, or even to identify and intercept products being illegally imported.

Appendix I

GSMA approach to combating mobile device theft

(This appendix does not form an integral part of this Recommendation.)

As in a growing number of countries, operators allow consumers to report a mobile device as lost or stolen. The operator can then establish the device's unique identifier, i.e., the international mobile equipment identity (IMEI), and the mobile network operator can then block the phone from accessing their mobile network. This is called IMEI blacklisting[5].

As an example of the use of a global database, in the mobile operator community the blacklisted IMEIs are provided to the GSM Association's (GSMA's) global IMEI database allowing operators to exchange data and to block devices on multiple networks nationally and internationally.

The GSMA IMEI database maintains a global blacklist collated from the data provided by the contributing operators. GSMA provides the blacklist information on a 24/7 basis to the operators that have established connections to the IMEI database for them to download and use within their own networks for device blocking purposes. Participating operators select an operator list from which they take blacklist data from and this is what dictates the degree to which data sharing coverage is achieved.

It is often unclear to the subscriber reporting a device as missing to its service provider if the device has been lost or stolen therefore no distinction is generally made between these states. If the owner finds the device and reports it to its service provider, the device can be unblocked and the IMEI removed from the IMEI Database. GSMA then sends an unblacklist instruction to the connected operators that downloaded the original blacklist record.

Due to the nature of this global database, and the commitment of the different stakeholders in the market to prevent device theft, GSMA developed a facility to allow the status of IMEIs to be checked. This is known as device check and it enables the sharing of data and device status information with approved partners, including retailers, insurers, recyclers and law enforcement agencies.

With this system, interested stakeholders can find out whether a device has been reported lost or stolen, providing years of a device's history as well as the device model information and capabilities. A number of benefits are derived from this kind of checking capability: a) helps resellers identify and eliminate stolen devices before they can enter supply chains, b) confirms the true device model for authenticity and to help calculate device value, c) discourages device theft by reducing the value of a stolen device and d) confirms the network operator that reported the device stolen or lost, which helps with repatriation to the rightful owner.

In addition to network operators, many other organizations in the mobile device ecosystem can use the device check service, including: a) device recyclers, retailers and dealers that use the data to reduce the likelihood of devices reported as stolen or lost from entering their recycling or resale stream, b) insurance companies that rely on the database to reduce false or overstated insurance claims for lost/stolen devices, and c) law enforcement agencies that use it to identify and assist in the investigation and/or repatriation of stolen or lost goods[6].

Access to consult a single identifier in the global IMEI database can be provided to a range of additional stakeholders including consumers, through service offerings from entitles such as national authorities that provide local language and hosted portals that allow IMEI lookups to be performed. Access to submit entries to the blacklist and/or to unblacklist identifiers is currently only granted to network operators that can unequivocally identify and attest IMEI data for their customers thereby

5 See [b-GSMA-IMEI-Blklst].

6 See [b-GSMA-IMEI-DevChk].

preserving the integrity of the blacklist. Consideration is being given to extend write access to the blacklist to other parties, such as device manufacturers, retailers, etc. that can attest and vouch for the IMEIs to be blocked.

The above related systems (GSMA IMEI database and IMEI device check) bring to stakeholders a range of advantages in comparison to national databases that result in fragmentation but could be built as a result of bilateral or multilateral efforts to exchange and block identifiers reported as lost or stolen. These advantages could represent: a) less time for implementation and fine tuning, b) less capital expenditures (CAPEX) and operational expenditures (OPEX) costs, c) less complexity and more effectiveness (one common point of exchange, instead of several origins and destinations), and d) less information replication. These items are based on the following characteristics of the referred systems: a) modularity, b) no connection fees for operators/governments, and c) the IMEI database is a mature and stable technology platform that has existed since 1996.

Bibliography

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

[b-IMEI-SEC] GSMA (2016), *IMEI Security Design Principles. Enabling stolen mobile device blocking. V4.0.* <https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 version 3.1.0 Release 1999).*

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10).*

[b-GSMA] GSM Association, Official Document SG.24 (2016), *Anti-Theft Device Feature Requirements v3.0*.

[b-GSMA-IMEI-Blklst] GSMA Services, *IMEI Blacklisting*. <https://www.gsma.com/services/gsma-imei/imei-blacklisting/> (last accessed 13 April 2020)

[b-GSMA-IMEI-DevChk] GSMA Services, *Device Check*. <https://www.gsma.com/services/gsma-imei/about-device-check/> (last accessed 13 April 2020)

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2020