

Recommendation

ITU-T Q.5054 (02/2025)

SERIES Q: Switching and signalling, and associated measurements and tests

Combating counterfeiting and stolen ICT devices

Consumer-centric framework for combating counterfeit and stolen information and communication technology mobile devices

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
PROTOCOLS AND SIGNALLING FOR COMPUTING POWER NETWORKS	Q.4140-Q.4159
PROTOCOLS AND SIGNALLING FOR QUANTUM KEY DISTRIBUTION NETWORKS	Q.4160-Q.4179
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.5054

Consumer-centric framework for combating counterfeit and stolen information and communication technology mobile devices

Summary

Recommendation ITU-T Q.5054 provides a consumer-centric framework through a unified platform considering possible scenarios and a multipronged approach for combating counterfeit and stolen mobile telecommunication/ICT devices.

This Recommendation builds upon Recommendation ITU-T Q.5050, which offers a reference framework with high-level challenges and requirements that should be considered when deploying solutions to combat the circulation and use of counterfeit information and communication technology (ICT) devices. Furthermore, Recommendation ITU-T Q.5051 presents a 'Framework for combating the use of stolen mobile devices'. It also defines possible communication channels and consumer interfaces with platform, indicative query and response formats including approaches for consumer education and awareness. The Recommendation also covers key features of the platform, key security considerations, implementation scenarios and possible technical challenges related inter alia to vendor agnostic interfaces, mobile equipment bulk verification, dealing with devices with replicated unique identifiers and the reporting and handling of stolen or lost mobile telecommunication/ICT devices and their restoration upon recovery.

With the rapid growth in the reach of the Internet and accelerated adoption and usage of ICT during the COVID-19 pandemic, the circulation and use of counterfeit ICT devices has increased considerably. According to an OECD report published in 2017, at that time already nearly one in five mobile phones shipped internationally was fake or counterfeit. The growing trade in counterfeit IT and communications hardware burdens on consumers, manufacturers and public finances.

A counterfeit ICT device is a product that explicitly infringes the trademarks, 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 policy requirements. Major mobile telecommunication/ICT devices include inter alia smartphones, tablets, IoT devices, wearables, modems, dongles and wireless local area network (WLAN) routers with cellular network connectivity. In addition to counterfeit mobile telecommunication/ICT devices, the use of stolen devices in mobile network also poses a serious security and law and order problem.

The unchecked proliferation of counterfeit and stolen mobile telecommunication/ICT devices in public land mobile networks (PLMNs) poses a serious challenge to regulators, law enforcement agencies (LEA) and end consumers and adversely affects the economy in general. The supply and demand economics of counterfeit and stolen devices complicate attempts to check the local as well as global market scenario for such devices.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.5054	2025-02-28	11	11.1002/1000/15946

Keywords

Combat counterfeit ICT and stolen devices, unified framework.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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/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 <https://www.itu.int/ITU-T/ipr/>.

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	General aspects	3
7	Reference unified platform framework (RUPF) requirements.....	4
	7.1 Type allocation code (TAC) database	4
	7.2 ICT device verification repository of brand owner or original equipment manufacturers	4
	7.3 National and international stolen device database.....	5
	7.4 National unified platform with central EIR.....	5
	7.5 Mobile network operator's equipment identity register.....	6
	7.6 Stakeholder interface(s) for mobile telecommunication/ICT device verification.....	6
8	Reference unified platform framework (RUPF).....	7
	8.1 Reference unified platform framework overview	8
	8.2 Key platform features	11
9	RUPF security and privacy considerations.....	12
Annex A	– Issues (aspects) and scenarios for the implementation of a reference unified platform framework.....	13
	A.1 Key considerations when implementing a reference unified platform framework.....	13
	A.2 Possible approaches for RUPF implementation	15
Appendix I	– Analysis of the mobile telecommunication/ICT device ecosystem and the main stakeholders involved in the use of counterfeit and tampered mobile telecommunication/ICT devices	18
	I.1 Mobile telecommunication/ICT device ecosystem and key stakeholders.....	18
	I.2 Impact of counterfeit and tampered devices on consumers.....	20
	I.3 Measures for mitigation of adverse impact on consumers	21
	Bibliography.....	23

Recommendation ITU-T Q.5054

Consumer-centric framework for combating counterfeit and stolen information and communication technology mobile devices

1 Scope

This Recommendation provides a framework to enable consumers to ubiquitously verify the authenticity of mobile telecommunication/ICT devices and provide a comprehensive overview to law enforcement agencies and regulators while enabling other stakeholders. The Recommendation will cover possible scenarios under which such mobile telecommunication/ICT devices may enter the mobile network ecosystem through any channel, emphasizing the need for a consumer centric approach to combat counterfeit, tampered and stolen mobile telecommunication/ICT devices including detection mechanisms for such devices with tampered/replicated unique identifiers.

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 solutions 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 Q.5052] Recommendation ITU-T Q.5052 (2020), *Addressing mobile devices with a duplicate unique identifier*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 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.

3.1.3 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 term:

3.2.1 replicated unique identifier: A valid device identifier properly assigned by the responsible management entity to one device, but which is being used by other devices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CEIR	Central Equipment Identity Register
CLI	Calling Line Identification
EIR	Equipment Identity Register
eUICC	embedded Universal Integrated Circuit Card
ICT	Information and Communications Technology
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of things
IT	Information Technology
LEA	Law Enforcement Agencies
M2M	Machine-to-Machine
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
OEM	Original Equipment Manufacturers
OTP	One-Time Password
PLMN	Public Land Mobile Network
QoE	Quality of Experience
RUPF	Reference Unified Platform Framework
SIM	Subscriber Identification Module
SMS	Short Message Service
TAC	Type Allocation Code
TBT	Technical Barrier to Trade
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Service Data
WLAN	Wireless Local Area Network

5 Conventions

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

- a) The keyword "is required to" indicates 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 keyword "should" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- c) The keyword "may" indicates an optional requirement 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 rapid growth in the reach of the Internet and accelerated adoption and usage of information and communication technology during the COVID-19 pandemic, the circulation and use of counterfeit and tampered mobile telecommunication/ICT devices has increased considerably. Mobile telecommunication/ICT devices include smartphones and other mobile devices such as tablets with a cellular network interface. In addition to mobile counterfeit ICT devices, the use of stolen devices in mobile networks also poses security and law-and-order problems.

The unchecked proliferation of counterfeit and tampered mobile telecommunication/ICT devices in the public land mobile network (PLMN) is a serious challenge to regulators, law enforcement agencies (LEA) and end consumers that also adversely affects revenue collection and therefore the economy in general. The supply and demand economics of counterfeit and tampered mobile telecommunication/ICT devices complicate the efforts to check the local as well as global market scenario for such devices.

[ITU-T Q.5050] has already considered possible approaches to solving the problem of counterfeit ICT products. In order to have a general understanding of possible directions for creating solutions to combat counterfeit, tampered and stolen telecommunication/ICT devices, Appendix I (clause I.1) provides a general analysis of the mobile telecommunication/ICT device ecosystem and the main stakeholders involved. Knowledge of the stakeholders and their roles in the ecosystem will allow us to define the general contours of the reference unified platform framework (RUPF).

This Recommendation aims to provide a comprehensive approach for combating counterfeit, tampered and stolen mobile telecommunication/ICT devices with a consumer-centric unified platform framework. By this proposed approach, the source of counterfeit and tampered mobile telecommunication products can also be assisted in tackling such issues, to the extent possible, in the markets where they are manufactured and from which they are exported and in the countries in which they are sold.

It is very difficult for anyone to differentiate between authentic and counterfeit or tampered mobile telecommunication/ICT devices by inspecting or testing them because counterfeiters attempt to create products very similar to the genuine device and even provide similar documentation and packaging. It is crucial that these factors are considered when deploying technology solutions to avoid creating more problems for users and genuine manufacturers than those the solutions aim to address.

However, in order to effectively check the proliferation and to combat the induction of counterfeit and tampered ICT including stolen devices in the mobile network, the information technology (IT) solution framework should enable consumers to verify the authenticity of any mobile telecommunication/ICT device ubiquitously while making purchasing decisions.

Consumers are the most affected and vulnerable stakeholder in the telecommunication/ICT mobile device ecosystem and a consumer-centric approach can play an important role in combating the proliferation of counterfeit and tampered mobile telecommunication/ICT devices. This is because

they often pay similar prices for the counterfeit devices while suffering consequences including compromised performance, security and privacy. Thus, the success of any solution to combat counterfeit or tampered mobile telecommunication/ICT and stolen devices lies in the empowerment of the end consumer through tools and awareness so that they can take informed decision while buying mobile telecommunication/ICT devices. Such a solution should cover all possible local and global scenarios through which counterfeit mobile telecommunication/ICT devices may enter the mobile network ecosystem through unauthorized channels. Further, the rejection of such devices by consumers, based on their awareness and empowerment with enabling tools, will also create a huge disincentive to the unauthorized manufacturing and trade of counterfeit and tampered telecommunication/ICT devices.

The ecosystem of counterfeit and tampered mobile telecommunication/ICT devices is focused on exploiting susceptible consumers. Due to a lack of consumer awareness and ignorance combined with the cheaper cost of counterfeit and tampered devices, consumers are enticed to buy them. Thus, consumers may suffer possible negative impacts when using counterfeit and tampered device. (Appendix I (clause I.2)).

Therefore, the Member States either planning or implementing countermeasures for restricting the usage and proliferation of counterfeit and tampered telecommunication/ICT device should consider a holistic multipronged, consumer-centric approach while implementing a relevant IT solution framework.

7 Reference unified platform framework (RUPF) requirements

Considering the above stakeholder analysis of the counterfeit and tampered telecommunication/ICT device ecosystem and possible roles of that can be played by the different stakeholders in combating this menace, the requirement for RUPF and different reference data sources are discussed below.

7.1 Type allocation code (TAC) database

The type allocation code (TAC)¹ is the first 8 digits of the international mobile equipment identity (IMEI) (which is 14 digits plus 1 check digit in length) which identifies the device model, brand owner and original equipment manufacturers (OEM). A TAC is allocated for a specific device model and brand owner. The TAC database and IMEI are important for the functioning of mobile devices and the mobile ecosystem. Device brand owners have to apply for TAC even for outsourced manufacturing. Therefore, access to the consolidated global TAC database provides the basic reference data for TAC codes against which the validity of any TAC code, used in any mobile telecommunication/ICT device, can be verified. A TAC database can provide important information about a device including its manufacturer, model name, TAC allocation date, OEM, subscriber identification module (SIM) slots, type of universal integrated circuit card (UICC) or embedded universal integrated circuit card (eUICC) operating system, frequency bands and radio interfaces. These details may be used effectively by RUPF and thereby help customs, LEAs and other stakeholders to differentiate counterfeit devices from genuine ones.

7.2 ICT device verification repository of brand owner or original equipment manufacturers

The TAC database is made up of the first 8 digits of the IMEI based on the details of ICT devices provided by the device brand owners or manufacturers concerned. The remaining six digits and one check digit of IMEI are assigned by the brand owners or manufacturers themselves according to the actual utilization or production of the respective model of that device. Therefore, it is possible that

¹ Global System for Mobile Communications Association (GSMA) is responsible for allocating type approval codes (TAC) to mobile device manufacturers.