

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5050

(03/2019)

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

Combating counterfeiting and stolen ICT devices

Framework for solutions to combat counterfeit ICT devices

Recommendation ITU-T Q.5050



International
Telecommunication
Union

Documents
Document Sharing Hub

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.5050

Framework for solutions to combat counterfeit ICT devices

Summary

There has been growing usage of information and communications technology (ICT) equipment in people's daily lives in recent years, but there have also been unwelcome side effects related to the increase in the sale, circulation and use of counterfeit ICT devices in the market.

A counterfeit ICT device is a product 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.

Among the various types of ICT devices used today, smartphones and other mobile devices have become pervasive and desirable items amongst the world population and, as a side effect, have also raised the attention of the global black/grey market.

This results in adverse consequences for stakeholders such as users, network operators, genuine device manufacturers, traders and governments, including decreased security protection and quality of service for users and revenue losses to a range of stakeholders.

Since the supply and demand economics for counterfeit ICT devices complicate attempts to tackle the global counterfeit market, no single solution can solve the problem alone, requiring that a broad range of measures to be taken in a holistic approach.

Recommendation ITU-T Q.5050 therefore aims to describe a reference framework, with high-level challenges and requirements that should be considered when deploying solutions to combat the circulation and use of counterfeit ICT devices.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5050	2019-03-15	11	11.1002/1000/13702

Keywords

Combat counterfeit ICT devices, compliance, conformance, conformity assessment, framework, requirements, security, standard, unique identifiers.

* 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/>.

© ITU 2019

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	3
6	General aspects	3
7	Fundamentals of an orderly telecom equipment marketplace	4
8	Considerations when deploying solutions for combating counterfeit ICT devices:.....	4
	8.1 Detection and identification of counterfeit ICT devices	4
	8.2 Tracking of counterfeit ICT device producers and traffickers	5
	8.3 Removal of counterfeit ICT devices already in use in the market	5
	8.4 Limit the import, circulation and sale of new counterfeit ICT devices on the market	5
	8.5 Differentiation between genuine and counterfeit ICT devices.....	6
	8.6 Limit impact on authentic ICT device manufacturer	6
	8.7 Reduction of end-user impact when considering removing counterfeit ICT devices.....	6
	8.8 Consumer education	7
	8.9 Avoiding technical barriers to trade (TBTs)	7
9	Framework requirements	7
	9.1 Identification and enforcement actions against producers and traffickers of counterfeit devices	7
	9.2 Consultation with industry and consumer groups	7
	9.3 Reliable unique identifier	8
	9.4 Centralized reference database	8
	9.5 Deployment of a conformity assessment regime.....	8
	9.6 Close collaboration with customs authorities and appropriate domestic agencies	9
	9.7 Share information with end-user before any remedial action	9
	9.8 Support of applicable national legal and regulatory frameworks.....	9
	9.9 Consideration for products already in use in the market	10
10	Possible counterfeit ICT solution approaches	10
	10.1 Prohibit the use of invalid and non-genuine device identifiers	10
	10.2 Certification of the ICT device and market surveillance.....	11
	10.3 Device lifecycle management.....	11
11	Reference framework.....	12

	Page
Annex A – Mobile devices solutions	14
Appendix I – Other industry solutions	17
Bibliography.....	20

Recommendation ITU-T Q.5050

Framework for solutions to combat counterfeit ICT devices

1 Scope

This Recommendation contains the reference framework and requirements to be considered when deploying solutions to combat the circulation and use of counterfeit information and communications technology (ICT) devices.

2 References

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

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 conformity assessment [b-ISO/IEC 17000]: Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

3.1.2 conformity assessment scheme (or programme) [b-ISO/IEC 17000]: Conformity assessment system related to specified objects of conformity assessment, to which the same specified requirements, specific rules and procedures apply.

3.1.3 market surveillance [b-EC-Regulation]: Activities carried out and measures taken by public authorities to ensure that products comply with the requirements set out in the relevant legislation and do not endanger health, safety or any other aspect of public interest protection.

3.1.4 standard [b-WTO-TBT]: Document approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for products or related processes and production methods, with which compliance is not mandatory. It may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements as they apply to a product, process or production method.

3.1.5 surveillance [b-ISO/IEC 17000]: Systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.

3.1.6 technical barrier to trade (TBT) [b-WTO-TBT]: The Technical Barriers to Trade Agreement of the World Trade Organisation (WTO) aims to ensure that technical regulations, standards, and conformity assessment procedures are non-discriminatory and do not create unnecessary obstacles to trade.

3.1.7 technical regulation [b-WTO-TBT]: Document which lays down product characteristics or their related processes and production methods, including the applicable administrative provisions, with which compliance is mandatory. It may also include or deal exclusively with terminology,

symbols, packaging, marking or labelling requirements as they apply to a product, process or production method.

3.1.8 grey market [b-Gartner]: The import and sale of devices outside regular commercial channels as defined by the original manufacturer or the relevant government, creating a parallel market to authorized distribution channels.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 counterfeit ICT device: 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.

3.2.2 tampered ICT device: 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.

3.2.3 unique identifier: An identifier associated with a single device that aims to uniquely identify it.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAS	Conformity Assessment Scheme
DevID	Device Identifier
DIRBS	Device Identification, Registration, and Blocking System
EAP	Extensible Authentication Protocol
EIR	Equipment Identity Register
ICT	Information and Communications Technology
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IPR	Intellectual Property Rights
IVR	Interactive Voice Response
PCB	Printed Circuit Board
SIM	Subscriber Identification Module
TAC	Type Allocation Code
TBT	Technical Barrier to Trade
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TRIPS	Trade-Related Aspects of Intellectual Property Rights

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 keyword "should" indicate 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" 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

There has been growing positive usage of ICT devices in people's daily lives in recent years, but there have also been unwelcome side effects related to the increase in the sale, circulation and use of counterfeit ICT devices in the market. This has resulted in adverse consequences for multiple stakeholders such as users, network operators, genuine device manufacturers, traders and governments, including decreased security protection and quality of service for users and revenue losses to a range of stakeholders.

It is recognized that supply and demand economics for counterfeit ICT devices complicate attempts to tackle the global black/grey market and that no single solution to combat counterfeit can be a panacea. The present Recommendation proposes a framework composed by a broad range of measures that can be taken and applied in a holistic approach to tackle this problem. The source of counterfeit products should also be tackled as much as possible in the markets where they are manufactured and exported from with the assistance of the countries in which they are sold.

Differentiation between authentic and counterfeit ICT devices can be particularly difficult for anyone inspecting or testing a product since a counterfeiter's aims are to create products very similar to the genuine device by providing false or stolen genuine documentation, sometimes including hardware taken from the genuine product or its accessories and even copying the legitimate software or unique identifiers, all to hamper identification for all stakeholders. It is crucial that these factors and others are considered when deploying solutions, to avoid creating more problems for users and genuine manufacturers than the ones the solutions set out to solve.

Among the various types of ICT devices used today, smartphones and other mobile devices have become pervasive and desirable items amongst the world population, and as a side effect, have also raised the attention of the global black/grey market. In response to the problem of counterfeit ICT devices, some countries have adopted measures and deployed successful solutions to deter the circulation and use of counterfeit ICT devices while governments in other countries are challenged and unclear on the best strategies to adopt.

In an attempt to address the use of counterfeit ICT devices, many of the solutions adopted share some similarities, such as relying on unique device identifiers, assistance of a conformance assessment regime and means to block the access of these fraudulent devices to the network (as proposed for mobile devices in Annex A).

However, various governments around the world are still challenged in combating counterfeit ICT devices for different reasons including technical aspects, the efforts of counterfeiters to elude and evade detection and the sheer desirability of the products which mean that consumers actively make a decision to purchase counterfeit products.