

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

Combating 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/>.

© ITU 2020

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	2
7 High level requirements.....	3
7.1 Preventing stolen mobile devices from being used by unauthorized user.....	3
7.2 Preventing stolen mobile devices from accessing the network	3
7.3 Preventing the use of mobile devices with tampered and/or cloned unique identifiers.....	4
7.4 Preventing stolen mobile devices from other countries to access the network.....	4
7.5 Reduce consumer impact.....	4
7.6 Protect consumer private data	5
7.7 Preventing stolen mobile devices from accessing the markets	5
7.8 Other considerations to address the tampering of stolen mobile devices unique identifiers	6
8 Framework requirements	6
8.1 Centralized reference database	6
8.2 Network support for blocking the devices.....	7
8.3 Reliable unique identifiers.....	7
8.4 Close collaboration with law enforcement agencies and other domestic agencies	7
8.5 Tools to check the status of mobile devices	8
8.6 Support of applicable national legal and regulatory frameworks.....	8
9 Reference framework.....	9
10 Desirable features	10
10.1 Lost and stolen devices global reference database	10
10.2 Actions regarding establishments that sell lost, stolen or tampered devices..	11
Appendix I – GSMA approach to combating mobile device theft	12
Bibliography.....	14

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.