

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Q

Supplement 73

(03/2021)

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

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

ITU-T Q-series Recommendations – Supplement 73

ITU-T

ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

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

Supplement 73 to ITU-T Q-series Recommendations

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

Summary

There are two alternative types of mechanisms and technology platforms available to address the issues related to counterfeit, illegal and stolen mobile devices in a country. There are inherent pros and cons to each approach. Supplement 73 to ITU-T Q-series Recommendations provides a detailed and comprehensive understanding of the underlying matters that should be clearly recognized, understood and addressed in order to have a successful system implementation.

Over the last few years many governments and countries have realized the importance and necessity of implementing technical solutions to combat the issues associated with the influx of counterfeit mobile devices, the illegal importation of mobile phones and mobile theft.

Given the complexities and the impact associated with the system implementation due to the requirements to handle these enormous issues, it is no wonder that governments are inundated with many difficult questions that are challenging to answer. Governments are generally not equipped with the technical expertise, especially in countries where the above-mentioned problems are most prevalent.

For the governments with the prime responsibility of developing the regulatory framework required for ensuring a smooth system deployment without causing any inconveniences to consumers, operators or importers, this creates a dependency on vendors and solution providers who offer technical solutions to address the above-mentioned issues.

There are two types of mechanisms that are available and can be deployed, permissive mechanisms and restrictive mechanisms. However, it is rather difficult for governments to find accurate and balanced information that covers all aspects for a complex deployment as well as the impact on various elements including the government, device manufacturers, local assembly, operators, importers, and most importantly the consumers.

This has resulted in a need to provide comprehensive information to governments so that they fully understand all relevant aspects and issues of system implementation and its impact on all stakeholders in the country. Equipped only with this knowledge, governments could determine and decide the best course of action and the right technical solution that suits their countries' needs and caters to local dynamics of the society.

This Supplement provides detailed information on the two mechanisms and highlights the strengths and weaknesses of each approach. Additionally, it provides guidelines to ensure a successful system implementation with a broad range of comprehensive measures to be adopted to combat the said issues.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q Suppl. 73	2021-03-26	11	11.1002/1000/14608

Keywords

Blocked-list, CEIR, counterfeit, EIR, illegal, IMEI, mobile devices, permissive systems, permissive, permitted-list, restrictive systems, restrictive, stolen, system implementation.

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

FOREWORD

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

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

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

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

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2021

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 Supplement	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	System implementation modes	2
	6.1 Permissive versus restrictive modes	3
7	Considerations for system deployment.....	8
	7.1 Customer considerations	8
	7.2 Technical considerations	10
	7.3 Regulatory considerations	10
8	Conclusion	11
	Appendix I.....	12
	Bibliography.....	13

Supplement 73 to ITU-T Q-series Recommendations

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

1 Scope

This Supplement provides guidelines for permissive versus restrictive system deployments that should be considered when deciding what approach to employ in order to address the issues of counterfeit, illegal and stolen mobile devices.

2 References

- [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*.
- [ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *ITU-T X.1120-X.1139 series, Supplement on security aspects of smartphones*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloned identifier [ITU-T Q.5051]: Is a valid device identifier properly assigned by the responsible management entity to one device but is being used by other different devices.

3.1.2 equipment identity register (EIR) [b-3GPP TS 22.016]: An EIR is a network element in the core of mobile networks that is used to terminate an access attempt or ongoing call when performing IMEI Check procedure depending on the status of the IMEI in one of its registers; blocked-list, permitted-list, or tracked-list.

3.1.3 invalid identifier [ITU-T Q.5051]: Is a unique identifier that does not comply with the format defined in the technical standards or that is not included in the device identifier reference database distributed by responsible management entity.

3.1.4 mobile device [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, or a smartphone.

3.1.5 radio access technology (RAT type) [b-3GPP TS 29.060]: 3GPP RAT type indicates which radio Access Technology is currently serving the User Equipment.

3.1.6 smartphone [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.

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