



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5052

(09/2020)

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

Combating counterfeiting and stolen ICT devices

Addressing mobile devices with duplicate unique identifier

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/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.

Recommendation ITU-T Q.5052

Addressing mobile devices with duplicate unique identifier

Summary

The presence and detection of duplicate unique identifiers on mobile networks and identifying the authenticity of a device are two key problems that stakeholders are looking to find solutions for.

The detection mechanisms discussed in this documentation are based on post-processing mobile network data to identify devices for blocking purposes based on criteria defined by individual national regulatory bodies. Through incorporation of one or more of these mechanisms, systems can identify and address the problem that duplicate or cloned devices present to governments, operators, and consumers.

A combination of one or more methodologies described in this document can be employed at any given time. The decision regarding the methodology or methodologies to employ will determine the level of effectiveness of a country's detection mechanism.

Keywords

Duplicate device detection, genuine device detection, counterfeit mobile devices, eUICC authentication

Table of Contents

1.	Scope.....	3
2.	References.....	3
3.	Definitions	3
3.1.	Terms defined elsewhere	3
3.2.	Terms defined in this Recommendation	4
4.	Abbreviations and Acronyms	4
5.	Conventions	4
6.	General Aspects	5
7.	Detecting Duplicate IMEIs	5
8.	Determining Genuine Devices Among Duplicated IMEIs	11
9.	Detecting Fraudulent Use of IMEIs.....	12
10.	Preventing Duplication Using eUICC Authentication Mechanisms	12
	Bibliography.....	16

Recommendation ITU-T Q.5052

Addressing mobile devices with duplicate unique identifier

1. Scope

This Recommendation identifies challenges and proposes mechanisms to enable the detection of mobile devices with duplicate identifiers present on operator networks as well as recommending mechanisms for validating the legitimacy of such 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 Q.5051] Recommendation ITU-T Q.5051 (2020), *Framework for combating the use of stolen mobile devices*.

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 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.
- 3.1.3 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.
- 3.1.4 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.
- 3.1.5 unique identifier** [ITU-T Q.5050]: An identifier associated with a single device that aims to uniquely identify it.
- 3.1.6 invalid identifier** [ITU-T Q.5051]: Is a unique identifier that doesn't comply with the format defined in the technical standards or that is not included in the device identifier reference database distributed by the responsible management entity.
- 3.1.7 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.

3.1.8 reliable unique identifiers [ITU-T Q.5051]: 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.

3.1.9 equipment identity register (EIR) [b-3GPP TS 22.016]: Can be used to terminate access attempt or ongoing call when performing IMEI Check procedure depending on the status of the IMEI in one of its registers; blacklist, white list, or grey list.

3.1.10 charging data record (CDR) [b-3GPP TR 21.905]: A formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting.

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

3.1.12 non access stratum (NAS) [b-3GPP]: is a set of protocols in the Evolved Packet System. The NAS is used to convey non-radio signaling between the User Equipment (UE) and the Mobility Management Entity (MME) for an LTE/E-UTRAN access.

3.1.13 subscription manager data-preparation (SM-DP): Creates, encrypts, packages and installs operator profiles in the eUICC.

3.2. Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 mobile device identifier database (MDID): A database containing aggregated information about mobile devices unique identifiers.

4. Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

CDR	Charging Data Record
DDCDS	Device Duplication & Clone Detection System
eUICC	Embedded Universal Integrated Circuit Card
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MDID	Mobile Device Identifier Database
NAS	Non-Access Stratum
NID	National ID
UID	Unique ID
RAT	Radio Access Technology
SM-DP	Subscription Manager Data Preparation
TAC	Type Allocation Code

5. Conventions

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

- 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.
- 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.