Overview of ITU-T activities on combating counterfeiting, including approved ITU-T Recommendations and ongoing activities

João Alexandre Zanon
Vice-Chairman SG11 - Chairman WP4/11
Anatel - Brazil

February 2023

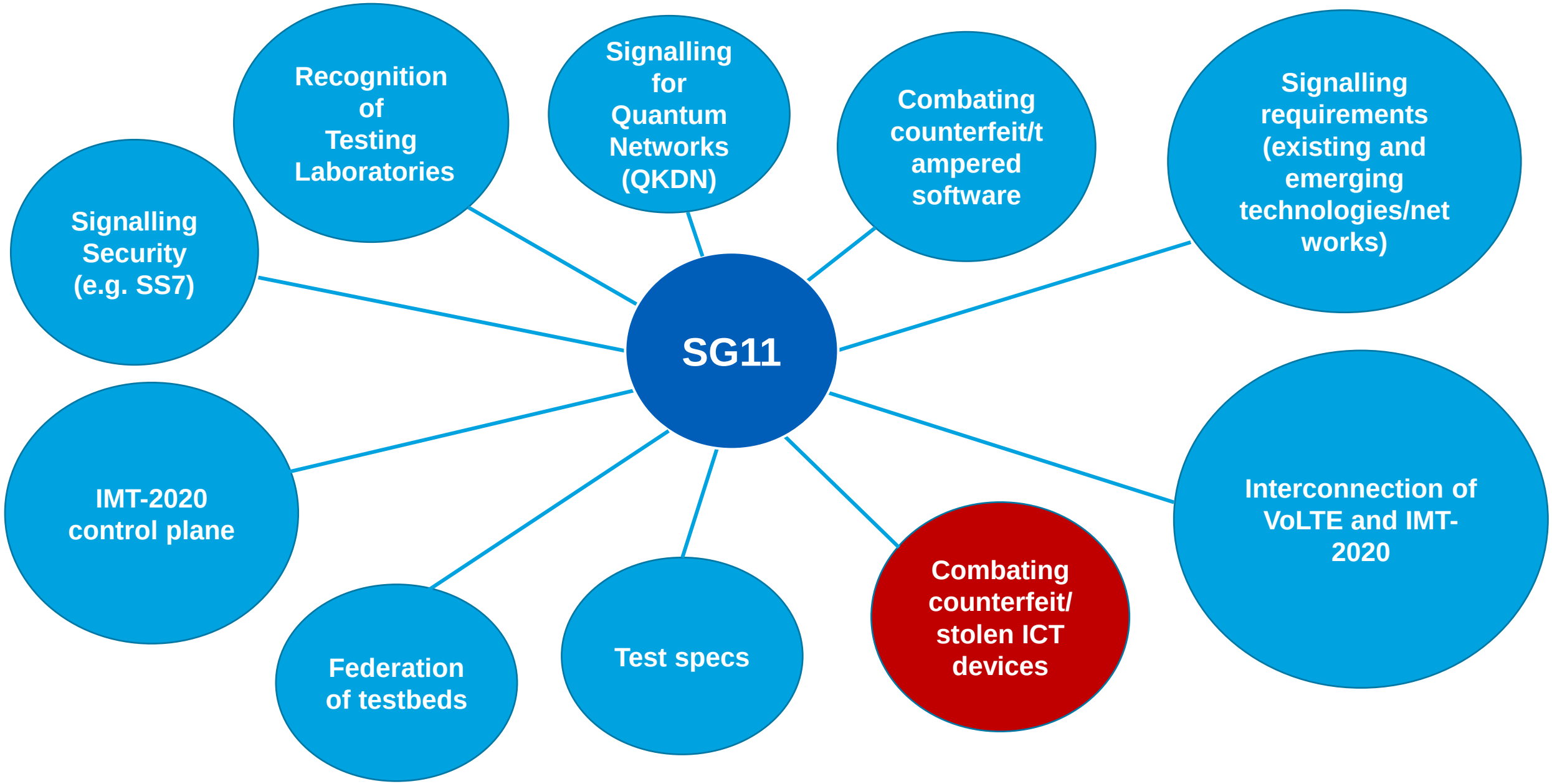
ITU-T SG11
Signalling requirements, protocols, test specifications and combating counterfeit telecommunication/ICT devices

Among other areas of responsibility, ITU-T SG11 is a lead group on combating counterfeiting of ICT devices as well as combating the use of stolen ICT devices.

Also, ITU-T SG11 studies issues related to combating counterfeit or tampered telecommunication/ICT software

http://itu.int/go/tsg11

Key directions of study of ITU-T SG11



Key events on counterfeit issues

Joint ITU/MWF Webinar "Combating Counterfeit and Irregular Mobile Devices: How to address the Problem"
Virtual, 31 May 2021

WSIS Forum 2021 – Session 406: Combating counterfeit telecommunication/ICT devices and software Virtual, 7 May 2021

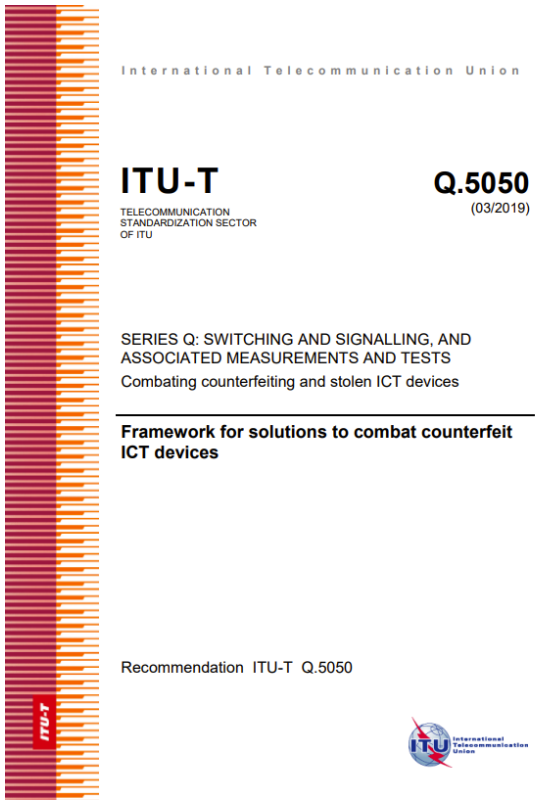
Third ITU-T Study Group 11 Regional Workshop for Africa on “Counterfeit ICT Devices, Conformance and Interoperability Testing Challenges in Africa” Tunis, Tunisia, 30 September 2019

ITU Workshop on Global approaches on combating counterfeiting and stolen ICT devices
Geneva, Switzerland, 23 July 2018

Second ITU-T Study Group 11 Regional Workshop for Africa on “Counterfeit ICT Devices, Conformance and Interoperability Testing Challenges in Africa” Tunis, Tunisia, 23 April 2018

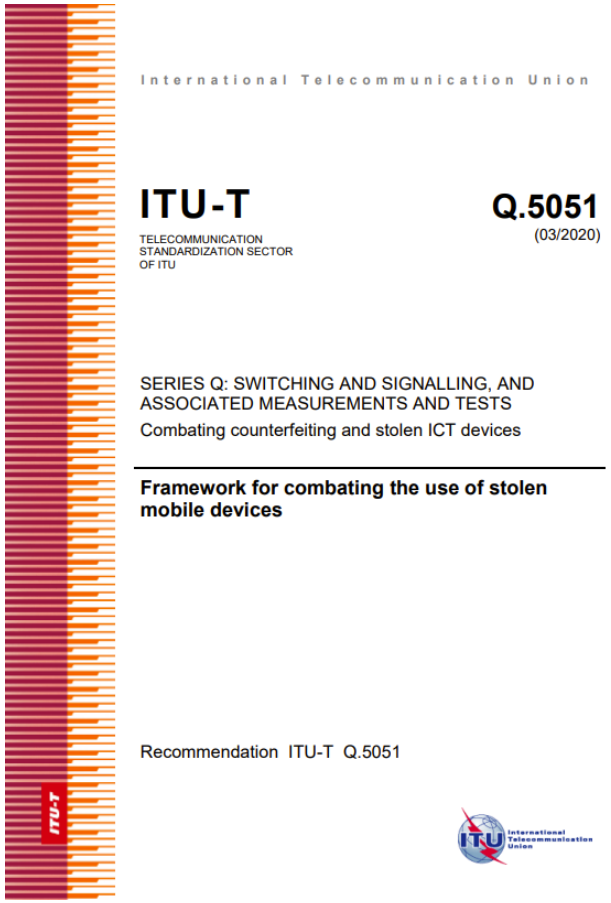
Counterfeit ICT Devices, Conformance and Interoperability Testing Challenges in Africa Cairo, Egypt, 5 April 2017

ITU-T Q.5050 “Framework for solutions to combat counterfeit ICT devices” (2019)

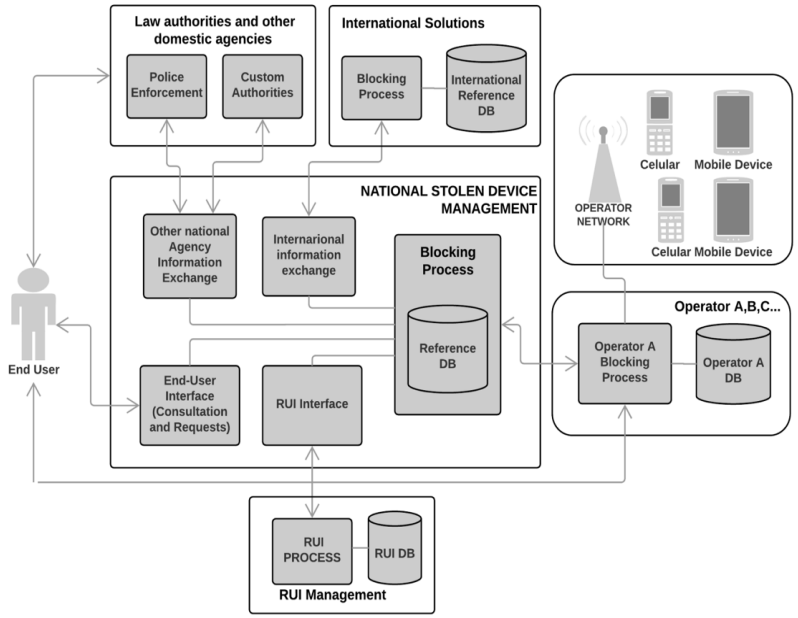


It describes a reference framework, with high-level challenges and requirements that should be considered when deploying solutions to combat the circulation and use of counterfeit ICT devices

ITU-T Q.5051 “Framework for combating the use of stolen mobile devices” (2020)



It is important not only to combat the use of Stolen Mobile Devices, but also to prevent the devices with unauthorized reprogrammed unique identifiers from returning to the network.

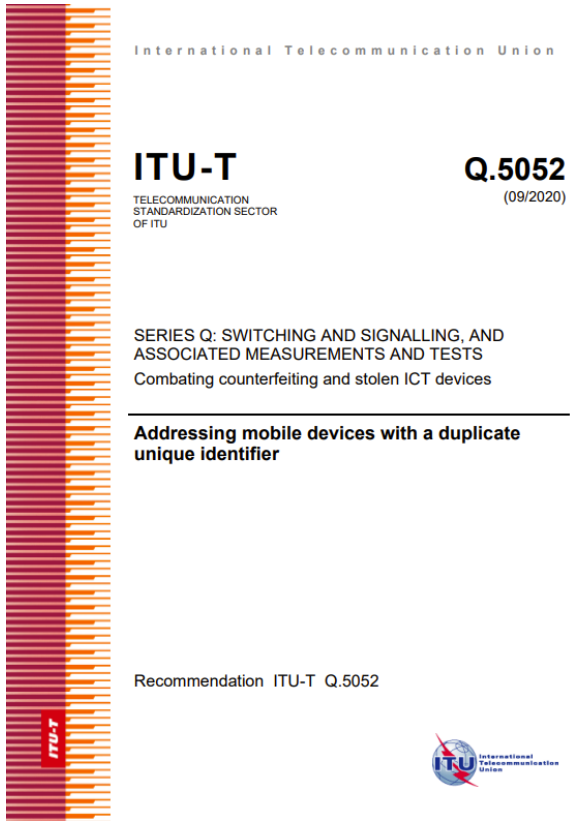


The global database should provide appropriate information if available (e.g. device characteristics, country where the device was stolen, date of event, etc.).

If the stolen device identifiers were found in multiple countries, the global database should provide that information in its results.

This global database should be available to all stakeholders from anywhere in the world to verify whether a device has been reported stolen.

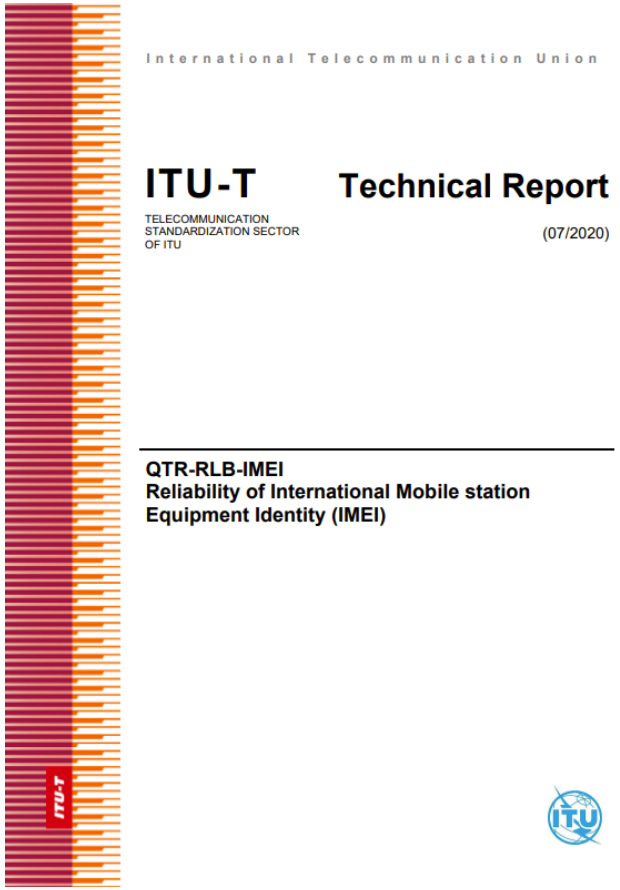
ITU-T Q.5052 “Addressing mobile devices with a duplicate unique identifier” (2020)



It 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

The detection mechanisms for duplicate unique identifiers (UIDs) defined in this standard are based on post-processing mobile network data to identify devices for blocking purposes based on criteria defined by individual national regulatory bodies.

ITU-T Technical Report QTR-RLB-IMEI “Reliability of International Mobile station Equipment Identity (IMEI)” (2020)

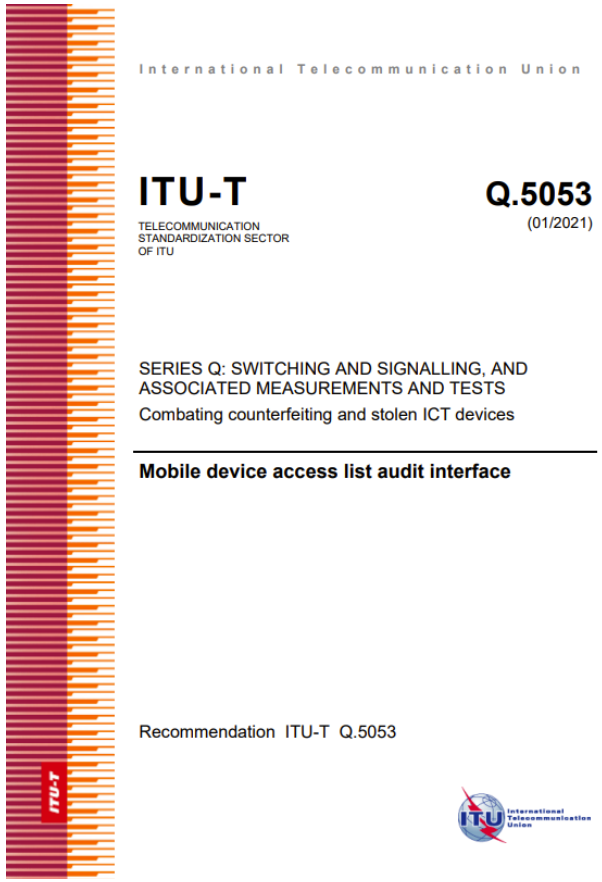


This Technical Report contains a study on the reliability of IMEI, including information about key vulnerabilities to IMEI reprogramming on mobile devices, challenges to make the IMEI non-reprogrammable, effects of IMEI tampering on mobile users, brand owners, manufacturers, service providers, regulators, governments, law enforcement agencies and on national security.

It addresses key challenges faced by a range of stakeholders that arise from cloned/tampered IMEIs, including concerns about the misuse of IMEI numbers raised by Member States at ITU Council-17 and ITU Council-18.

It also proposes ways to improve IMEI reliability and preventive steps for solving the issues on a national and international level.

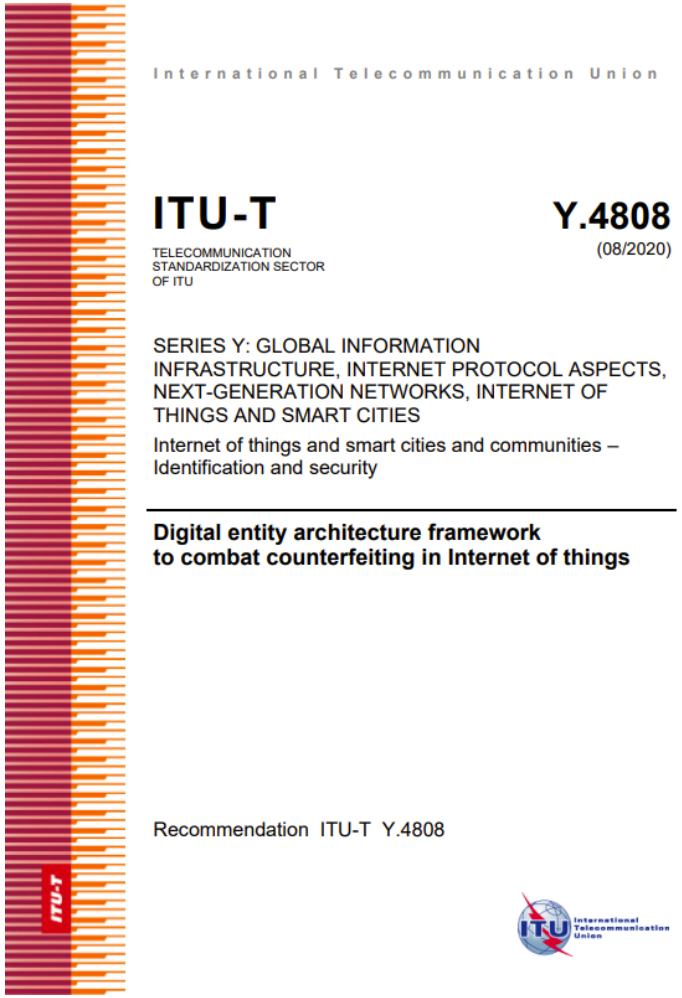
ITU-T Q.5053 “Mobile device access list audit interface” (2021)



In some countries, international mobile equipment identities (IMEIs) to be restricted (blocked list), thus blocking access to the mobile network, or to be allowed (permitted list) by the mobile network operators (MNOs), may be provided by a telecom authority or law enforcement agency (LEA) via mobile device identifier database (MDID).

This standard describes different types of methodologies and interfaces to check and reconcile the mobile device access list used by the MNOs to comply with the regulations for the mobile device access list audit system (MDALAS).

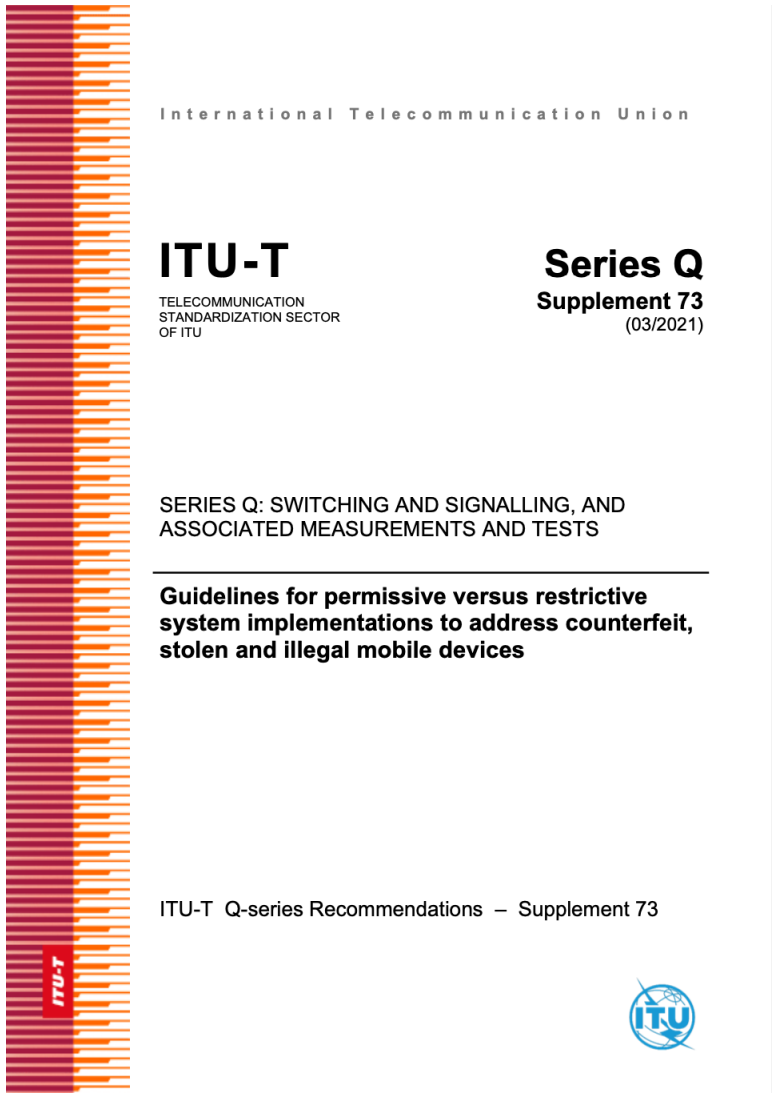
ITU-T Y.4808 “Digital entity architecture framework to combat counterfeiting in Internet of things” (2020)



Systems based on digital entity architecture may be considered as one category of candidate tools which allow vendors/industries (not only ICT industry) to store their products' profile in digital form.

Therefore, Recommendation ITU-T Y.4808 can be used in different industries such as the information communication technology (ICT), pharmaceutical, automotive and aviation industries.

ITU-T Q Suppl.73 “Guidelines for Permissive versus Restrictive System Implementations to address counterfeit, stolen and illegal mobile devices” (2021)



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.

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.

ITU-T Q Suppl.74 “Roadmap for the Q.5050-series - Combat of Counterfeit ICT and Stolen Mobile Devices” (2021)

International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

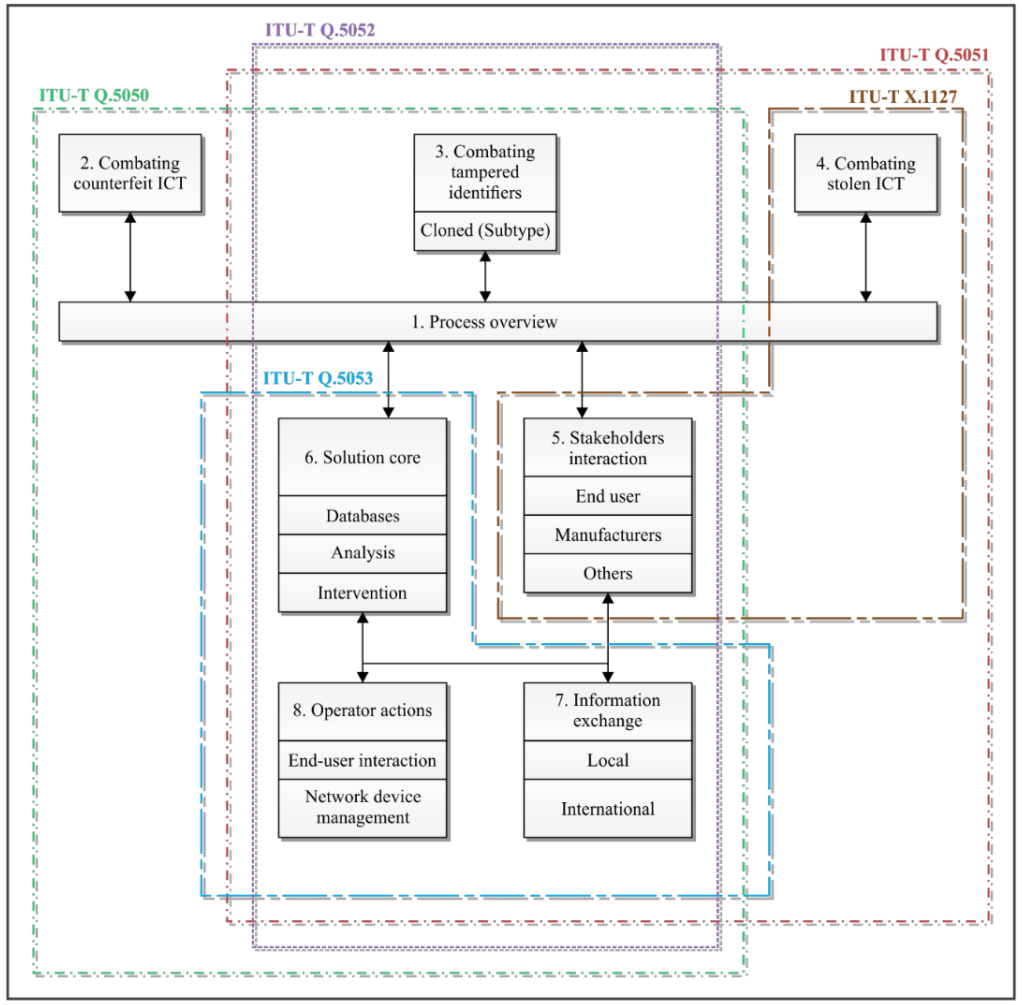
Series Q
Supplement 74
(03/2021)

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

Roadmap for the ITU-T Q.5050-series – Combat of counterfeit ICT and stolen mobile devices

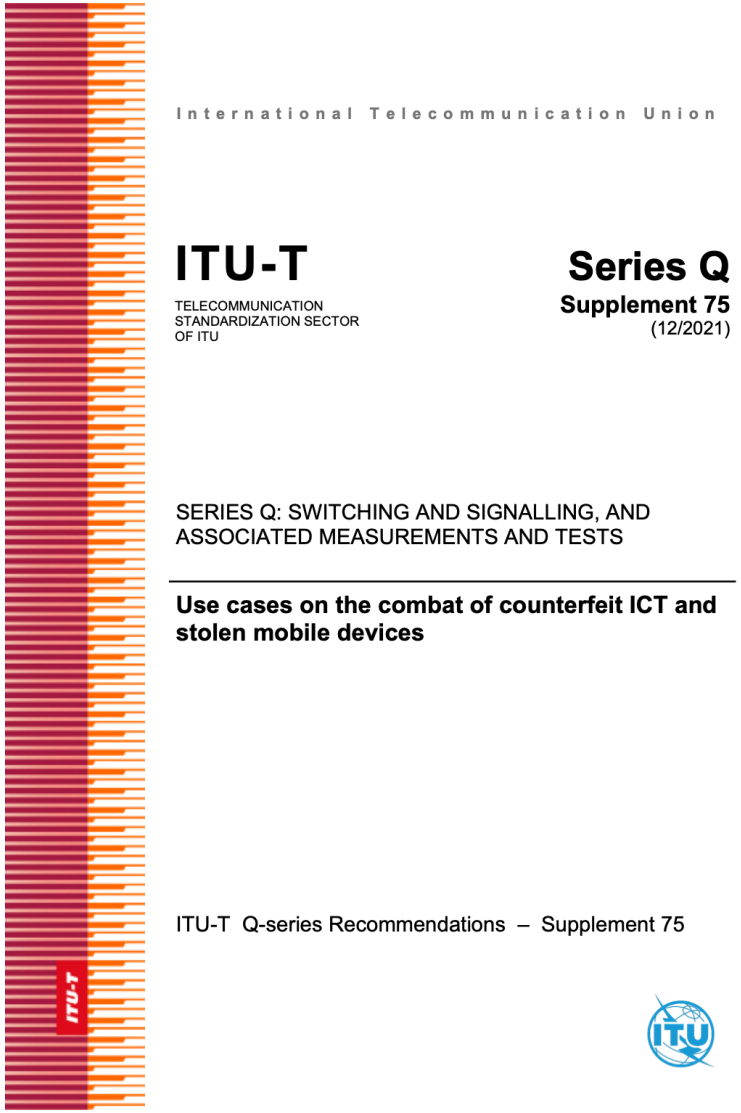
ITU-T Q-series Recommendations – Supplement 74

Provide an overall index and relation of the ITU-T Q.5050-series of Recommendations.



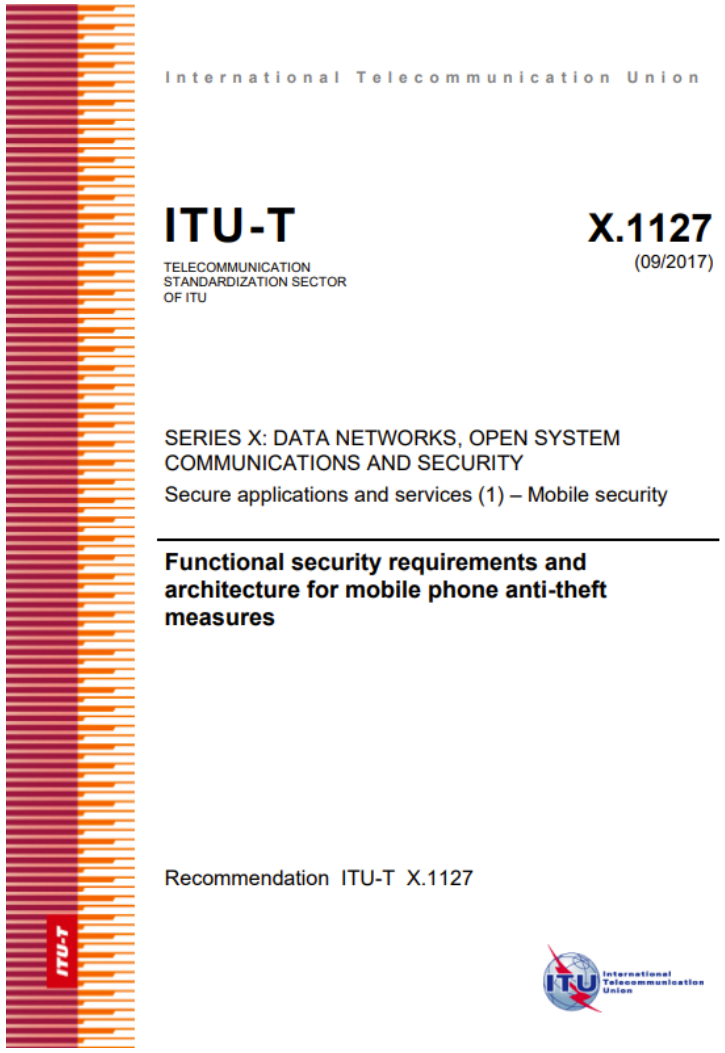
Q Suppl.74(21)_F01

ITU-T Q.Suppl.75 “Use cases on the combat of counterfeit ICT and stolen mobile devices” (2021)



Collects use cases provided by ITU Members that reflects challenges, opportunities and results on the combat of counterfeit ICT and stolen mobile devices.

ITU-T X.1127 “Functional security requirements and architecture for mobile phone anti-theft measures” (2017)



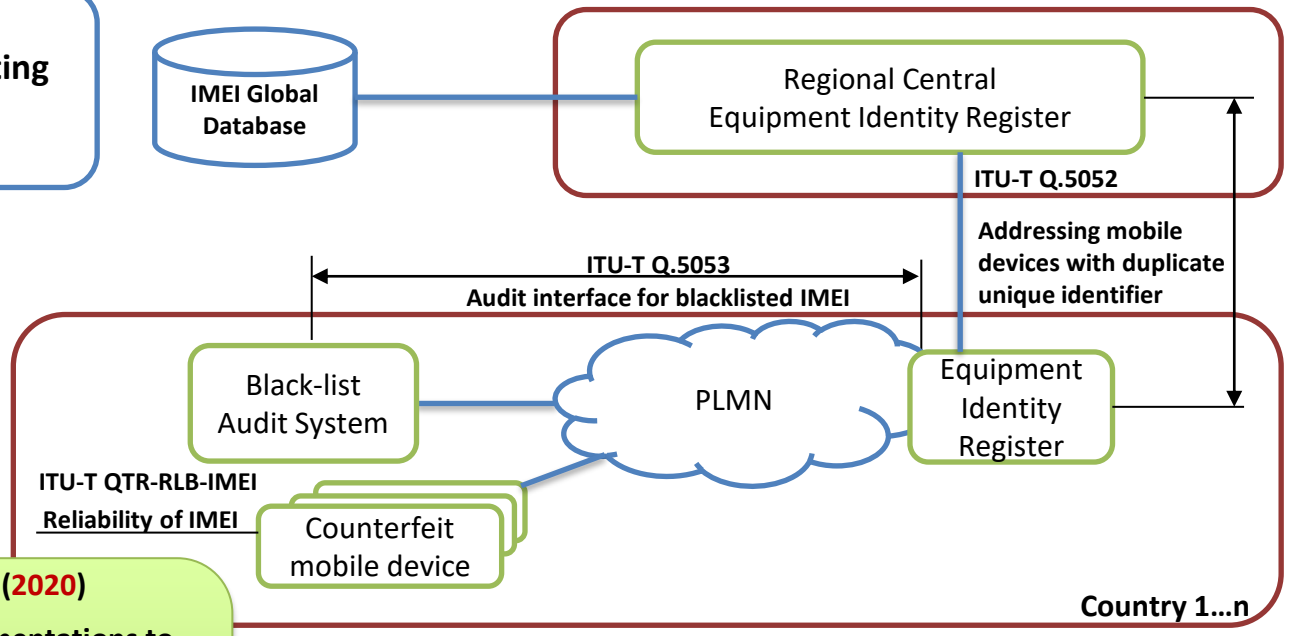
This Recommendation addresses the functional security requirements and architecture for the smartphone anti-theft measure (i.e., a kill switch), which allows users to remotely delete their personal data or disable stolen or lost smartphone devices.

Key achievements: Counterfeit & ICT theft (2017-2022)

Combating counterfeiting of ICT devices

Resolution 96 of WTSA-16
ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices

- Technical Report on Counterfeit ICT Equipment (2015)
- QTR-CICT - Survey report on counterfeit ICT devices in Africa region (2017)
- ITU-T Q.5050 "Framework for solutions to combat counterfeit ICT devices" (2019)
- Questionnaire on Reliability of International Mobile Equipment Identity (IMEI) – (2019)



- ITU-T Q.5052 "Addressing mobile devices with a duplicate unique identifier" (2020)
- ITU-T Q Suppl.73 "Guidelines for Permissive versus Restrictive System Implementations to address counterfeit, stolen and illegal mobile devices" (2021)
- ITU-T Q Suppl.74 "Roadmap for the Q.5050-series - Combat of Counterfeit ICT and Stolen Mobile Devices" (2021)
- ITU-T Q.Suppl.75 "Use cases on the combat of counterfeit ICT and stolen mobile devices" (2021)

Combating the use of stolen ICT devices

Resolution 97 of WTSA-20
Combating mobile telecommunication device theft

- ITU-T Q.5051 "Framework for combating the use of stolen mobile devices" (2020)

Ongoing activities

- Draft Recommendation Q.CEIR “Technical requirement, interfaces and generic functions of CEIR”. *It provides detailed technical description of the CEIR system, its requirements, interfaces and basic functions that should be provided by the system and also some optional features.*

- Draft Recommendation Q.CCF-CCSD “Consumer centric framework for combating counterfeit and stolen ICT mobile devices”. *It will provide a consumer centric framework through unified platform combining all scenarios for combating counterfeit and stolen devices as covered in ITU-T Q.5050 Recommendation Series.*

- Draft Supplement Q.Sup.CEIR-EIR-int "Common approaches and interfaces for data exchange between CEIR and EIR“
  It aims to identify current industry approach on the data exchange between CEIR and EIR and propose common approaches and interfaces on this topic.

- Draft Technical Report TR-CF-QoS "Impact of Counterfeit Mobile devices on Quality of Service”
  It aims to study the negative effects and impact of counterfeit mobile devices on network’s quality of service along with the negative effects and service degradation experienced by the mobile subscribers

- Draft Supplement Q.Sup.CFS-AFR (ex.TR-FCM) "Guidelines on combating counterfeit and stolen mobile devices in African region“
  It proposes a guideline to combat the circulation and use of counterfeit and stolen mobile devices in the African region, based on the Q.5050 series and also the African region members’ experiences.

ITU-T web portal

http://itu.int/go/CS-ICT

Contacts

- zanon@anatel.gov.br
- tsbsg11@itu.int
- http://itu.int/go/tsg11