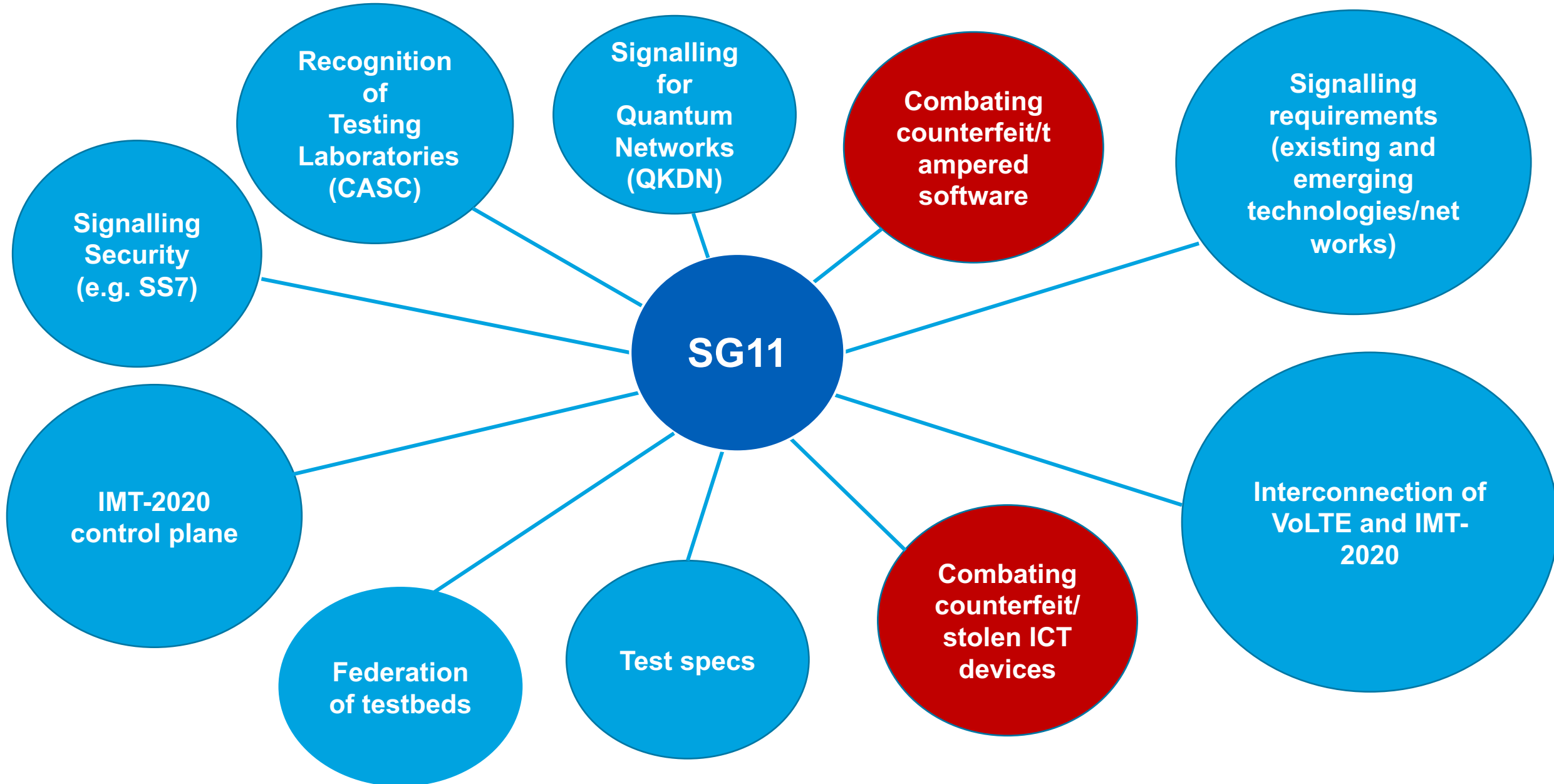# Overview of ITU-T SG11 activities on Combating counterfeiting and stolen ICT

João Alexandre Zanon

Vice-Chairman SG11 - Chairman WP4/11

Anatel - Brazil

October 2023

Key directions of study of ITU-T SG11

Combating counterfeiting and stolen ICT

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

WP4/11	Combating counterfeit telecommunication/ICT devices/software and mobile device theft
Q15/11	Combating counterfeit and stolen telecommunication/ICT devices
Q17/11	Combating counterfeit or tampered telecommunication/ICT software

http://itu.int/go/tsg11

SG11 Workshop series on combating counterfeiting and stolen ICT
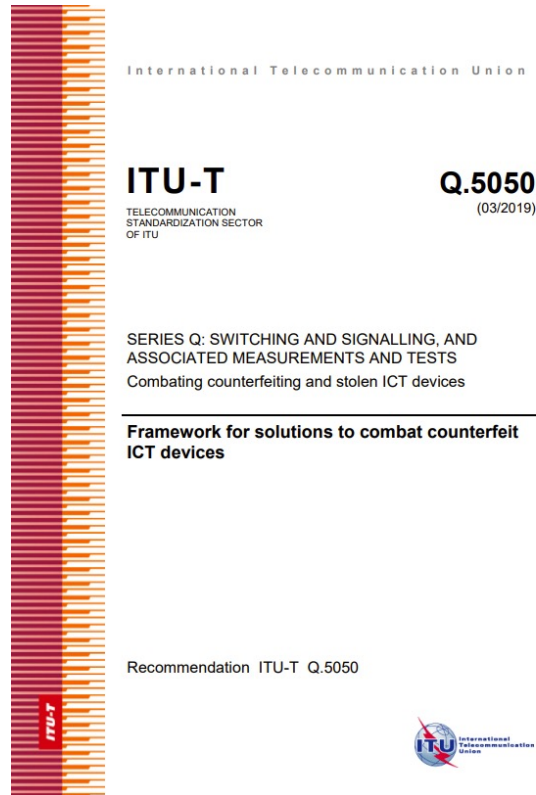
[SG11 workshops (2022-2023)](#)

SG11 past events on combating counterfeiting and stolen ICT

[SG11 workshops (2017-2021)](#)

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

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

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)
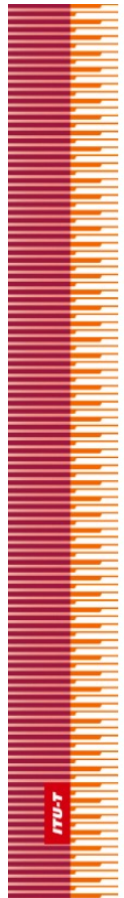
International Telecommunication Union

ITU-T   **Q.5051**
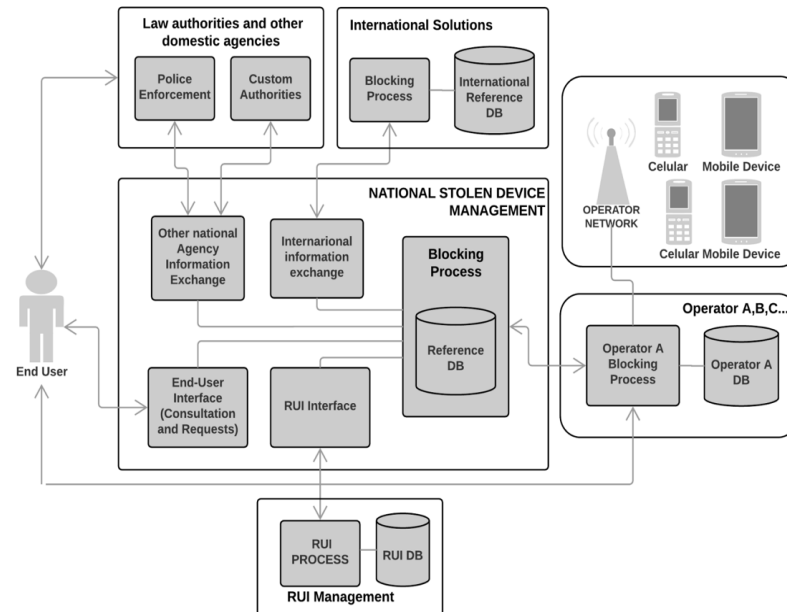(03/2020)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

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

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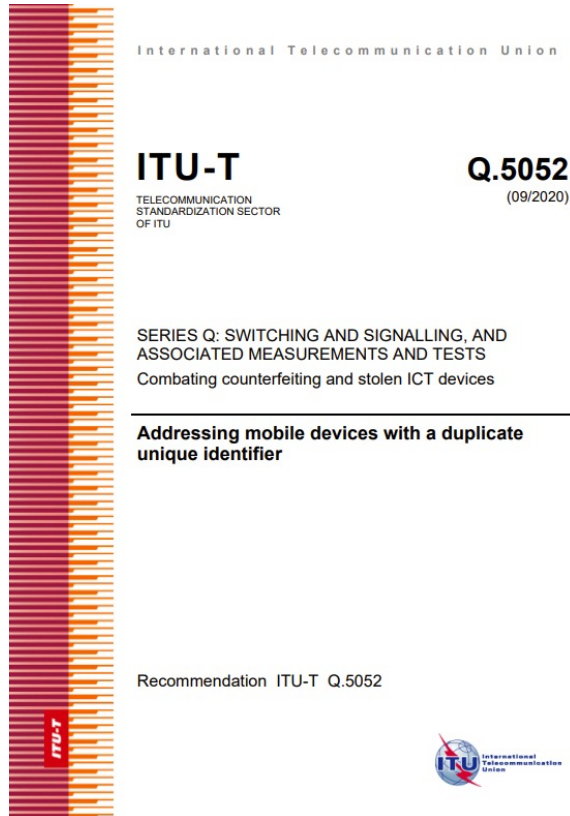
The global database should provide appropriate information if available (e.g. device characteristics, country where the device was stolen, date of event, etc.).

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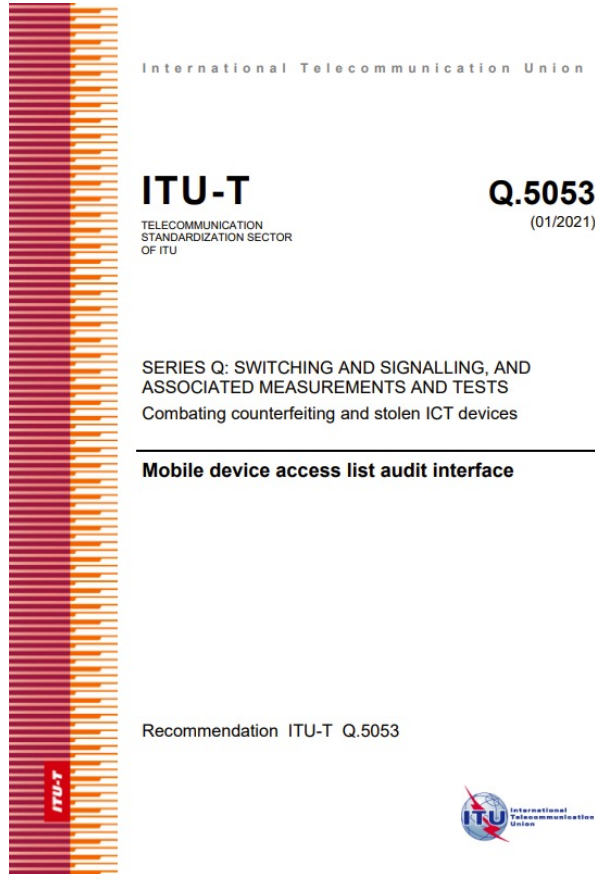
ITU-T Q.5052 "Addressing mobile devices with a duplicate unique identifier" (2020)

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 a duplicate
unique identifier**

Recommendation ITU-T Q.5052

International Telecommunication Union

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 Q.5053 "Mobile device access list audit interface" (2021)

International Telecommunication Union

ITU-T

Q.5053

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01/2021)

SERIES Q: SWITCHING AND SIGNALLING, AND
ASSOCIATED MEASUREMENTS AND TESTS
Combating counterfeiting and stolen ICT devices

Mobile device access list audit interface

Recommendation ITU-T Q.5053

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

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

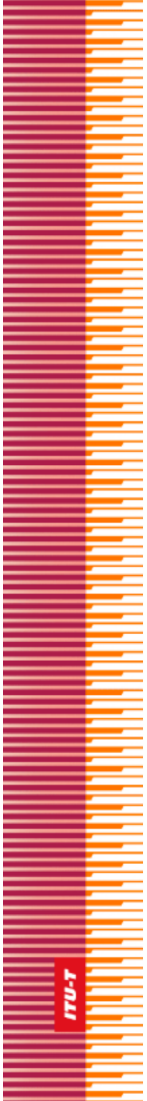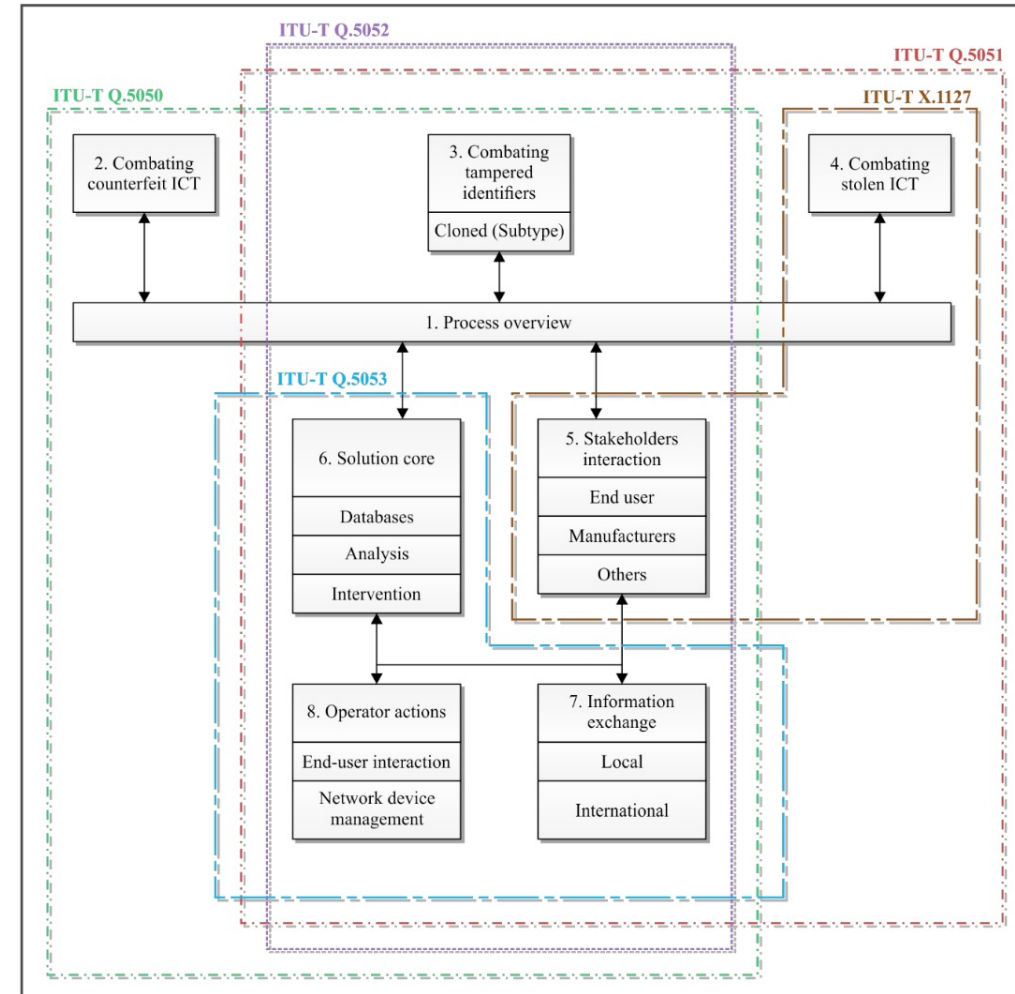# ITU-T Q.Suppl.75 "Use cases on the combat of counterfeit ICT and stolen mobile devices" (2021)

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

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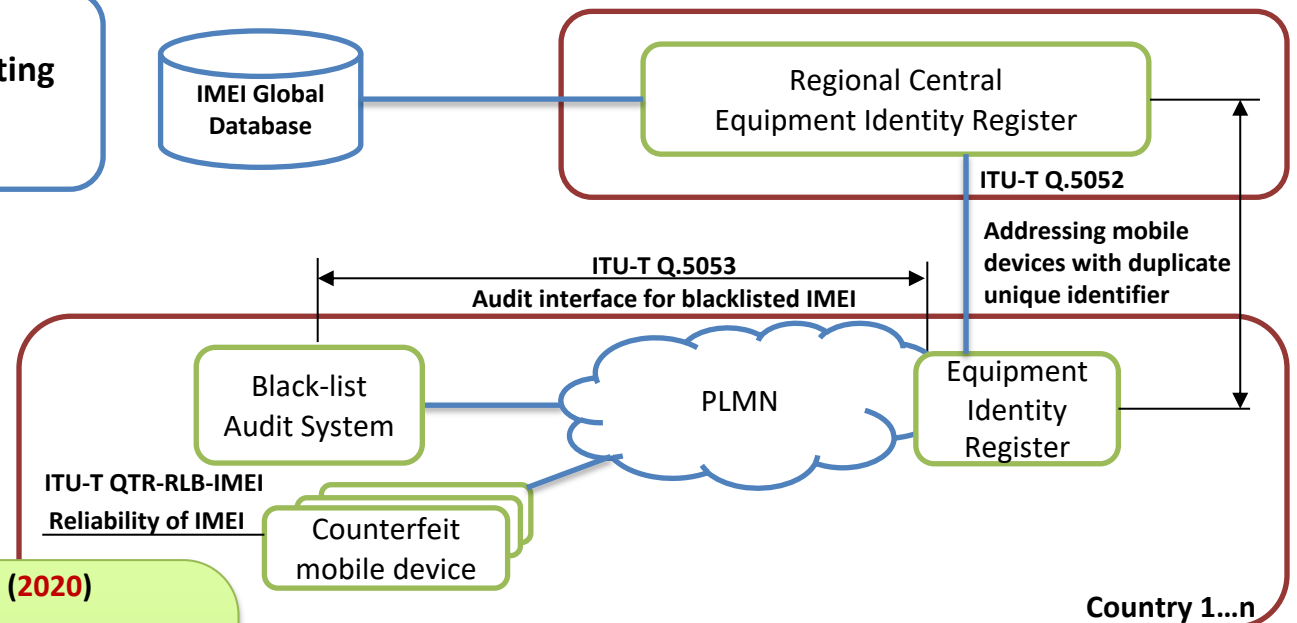
ITU-T Q Suppl.73 "Guidelines for Permissive versus Restrictive System Implementations to address counterfeit, stolen and illegal mobile devices" (2021)

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)

Resolution 97 of WTSA-20
Combating mobile telecommunication device theft

IMEI Global Database

Regional Central Equipment Identity Register

ITU-T Q.5052

Addressing mobile devices with duplicate unique identifier

ITU-T Q.5053
Audit interface for blacklisted IMEI

Black-list Audit System

PLMN

Equipment Identity Register

ITU-T QTR-RLB-IMEI
Reliability of IMEI

Counterfeit mobile device

Country 1...n

Combating the use of stolen ICT devices

- **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.

- Draft Recommendation *Draft recommendation Q.FC-MCM: "Framework for combating Multimedia Content Misappropriation". Contains a reference framework with requirements and actions that should be considered when deploying solutions to combat multimedia content misappropriation.*

- *Draft Technical Report TR-MCM-Use-Cases: Use Cases on the combat of Multimedia Content Misappropriation: aims to collect use cases from ITU Members that reflects challenges, opportunities and results on the combat of multimedia content misappropriation and, with this information compendium, assist ITU members in engaging this problem.*

ITU-T web portal

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

Contacts

Joao Zanon

zanon@anatel.gov.br

TSB secretariat
tsbsg11@itu.int
http://itu.int/go/tsg11