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

ITU-T

International Telecommunication Union

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.5050

Framework for solutions to combat counterfeit ICT devices

Summary

There has been growing usage of information and communications technology (ICT) equipment in people's daily lives in recent years, but there have also been unwelcome side effects related to the increase in the sale, circulation and use of counterfeit ICT devices in the market.

A counterfeit ICT device is a product that explicitly infringes the trademark, copies hardware or software designs, or infringes brand or packaging rights of an original or authentic product and, in general, infringes applicable national and/or international technical standards, regulatory requirements or conformity processes, manufacturing licensing agreements, or other applicable legal requirements.

Among the various types of ICT devices used today, smartphones and other mobile devices have become pervasive and desirable items amongst the world population and, as a side effect, have also raised the attention of the global black/grey market.

This results in adverse consequences for stakeholders such as users, network operators, genuine device manufacturers, traders and governments, including decreased security protection and quality of service for users and revenue losses to a range of stakeholders.

Since the supply and demand economics for counterfeit ICT devices complicate attempts to tackle the global counterfeit market, no single solution can solve the problem alone, requiring that a broad range of measures to be taken in a holistic approach.

Recommendation ITU-T Q.5050 therefore aims to describe 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5050	2019-03-15	11	11.1002/1000/13702

Keywords

Combat counterfeit ICT devices, compliance, conformance, conformity assessment, framework, requirements, security, standard, unique identifiers.

---

* 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/.

Table of Contents

Recommendation ITU-T Q.5050

Framework for solutions to combat counterfeit ICT devices

1 Scope

This Recommendation contains the reference framework and requirements to be considered when deploying solutions to combat the circulation and use of counterfeit information and communications technology (ICT) 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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 conformity assessment [b-ISO/IEC 17000]: Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

3.1.2 conformity assessment scheme (or programme) [b-ISO/IEC 17000]: Conformity assessment system related to specified objects of conformity assessment, to which the same specified requirements, specific rules and procedures apply.

3.1.3 market surveillance [b-EC-Regulation]: Activities carried out and measures taken by public authorities to ensure that products comply with the requirements set out in the relevant legislation and do not endanger health, safety or any other aspect of public interest protection.

3.1.4 standard [b-WTO-TBT]: Document approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for products or related processes and production methods, with which compliance is not mandatory. It may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements as they apply to a product, process or production method.

3.1.5 surveillance [b-ISO/IEC 17000]: Systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.

3.1.6 technical barrier to trade (TBT) [b-WTO-TBT]: The Technical Barriers to Trade Agreement of the World Trade Organisation (WTO) aims to ensure that technical regulations, standards, and conformity assessment procedures are non-discriminatory and do not create unnecessary obstacles to trade.

3.1.7 technical regulation [b-WTO-TBT]: Document which lays down product characteristics or their related processes and production methods, including the applicable administrative provisions, with which compliance is mandatory. It may also include or deal exclusively with terminology,

symbols, packaging, marking or labelling requirements as they apply to a product, process or production method.

3.1.8 grey market [b-Gartner]: The import and sale of devices outside regular commercial channels as defined by the original manufacturer or the relevant government, creating a parallel market to authorized distribution channels.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 counterfeit ICT device: An information and communication technology (ICT) device that explicitly infringes the trademark, copies hardware or software designs, or infringes brand or packaging rights of an original or authentic product and, in general, infringes applicable national and/or international technical standards, regulatory requirements or conformity processes, manufacturing licensing agreements, or other applicable legal requirements.

3.2.2 tampered ICT device: 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.

3.2.3 unique identifier: An identifier associated with a single device that aims to uniquely identify it.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAS Conformity Assessment Scheme

DevID Device Identifier

DIRBS Device Identification, Registration, and Blocking System

EAP Extensible Authentication Protocol

EIR Equipment Identity Register

ICT Information and Communications Technology

IMEI International Mobile Equipment Identity

IoT Internet of Things

IPR Intellectual Property Rights

IVR Interactive Voice Response

PCB Printed Circuit Board

SIM Subscriber Identification Module

TAC Type Allocation Code

TBT Technical Barrier to Trade

TEE Trusted Execution Environment

TPM Trusted Platform Module

TRIPS Trade-Related Aspects of Intellectual Property Rights

5 Conventions

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

a) 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.

b) 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.

c) The keyword "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 General aspects

There has been growing positive usage of ICT devices in people's daily lives in recent years, but there have also been unwelcome side effects related to the increase in the sale, circulation and use of counterfeit ICT devices in the market. This has resulted in adverse consequences for multiple stakeholders such as users, network operators, genuine device manufacturers, traders and governments, including decreased security protection and quality of service for users and revenue losses to a range of stakeholders.

It is recognized that supply and demand economics for counterfeit ICT devices complicate attempts to tackle the global black/grey market and that no single solution to combat counterfeit can be a panacea. The present Recommendation proposes a framework composed by a broad range of measures that can be taken and applied in a holistic approach to tackle this problem. The source of counterfeit products should also be tackled as much as possible in the markets where they are manufactured and exported from with the assistance of the countries in which they are sold.

Differentiation between authentic and counterfeit ICT devices can be particularly difficult for anyone inspecting or testing a product since a counterfeiter's aims are to create products very similar to the genuine device by providing false or stolen genuine documentation, sometimes including hardware taken from the genuine product or its accessories and even copying the legitimate software or unique identifiers, all to hamper identification for all stakeholders. It is crucial that these factors and others are considered when deploying solutions, to avoid creating more problems for users and genuine manufacturers than the ones the solutions set out to solve.

Among the various types of ICT devices used today, smartphones and other mobile devices have become pervasive and desirable items amongst the world population, and as a side effect, have also raised the attention of the global black/grey market. In response to the problem of counterfeit ICT devices, some countries have adopted measures and deployed successful solutions to deter the circulation and use of counterfeit ICT devices while governments in other countries are challenged and unclear on the best strategies to adopt.

In an attempt to address the use of counterfeit ICT devices, many of the solutions adopted share some similarities, such as relying on unique device identifiers, assistance of a conformance assessment regime and means to block the access of these fraudulent devices to the network (as proposed for mobile devices in Annex A).

However, various governments around the world are still challenged in combating counterfeit ICT devices for different reasons including technical aspects, the efforts of counterfeiters to elude and evade detection and the sheer desirability of the products which mean that consumers actively make a decision to purchase counterfeit products.

Therefore, countries who choose to combat counterfeit ICT should consider holistic multi-agency/stakeholder approaches and technology solutions deployed in other countries that are already engaged on the issue for guidance and examples of best practice.

7 Fundamentals of an orderly telecom equipment marketplace

There are many factors that underlie creation of an orderly marketplace in telecommunication products and services. A primary requirement is the establishment of robust technical requirements for products entering the marketplace. Such requirements, among others, address safety of personnel, both the user community and the network service provider personnel, and the establishment of an interference free environment for telecommunication services.

Interference free services – wireless and wireline – are implicated in the economic development of a society as participation in the global digital economy demands robust, secure and dependable telecommunication platforms over which the economic activity takes place. Furthermore, a market access regime that is well defined, well managed, non-discriminatory and transparent inspires trust and confidence in equipment suppliers, service providers and people in general. Such a regime backed up by an appropriate legislative and regulatory framework is a fundamental building block to deliver the requisite quality of national and international connectivity crucial to participation in the global digital economy. In fact, in a very real way it reflects the priorities and values of a society [b-ITU-D-CI-Guidelines].

8 Considerations when deploying solutions for combating counterfeit ICT devices:

There are several challenges to be faced by stakeholders when deploying solutions to address counterfeit ICT devices:

8.1 Detection and identification of counterfeit ICT devices

One of the aims of a counterfeiter is to enable their product to be sold in markets around the world. From the look and feel, copy of unique identifiers, software and even the internal components of ICT devices, counterfeiters will do their utmost to make a product as close to the genuine original as possible.

This presents some challenges. For example, all identifiers that are created by authentic manufacturers of goods can and are abused by counterfeiters to achieve their aims of duping consumers and the authorities that their product is genuine. Any identification mechanism and the security around it may become a target for counterfeiters and criminals. Type approval logos and icons as well as electronic identifiers are often deliberately subverted, or even set in blank to be self-programmed in local markets, to evade customs and law enforcement checks at borders. [b-ITU-T TR-Counterfeit]

All identifiers that are created by authentic manufacturers of goods can be tampered by counterfeiters in order to achieve their aims of duping consumers and the authorities that their product is genuine. This is a problem in many industries, not just ICT. The reader should bear in mind that any identification mechanism and the security around it will become a target for counterfeiters and criminals. [b-ITU-T TR-Counterfeit]

For instance, a common practice of counterfeiters is to tamper with unique identifiers that some devices use to authenticate on the network in a way that the counterfeit ICT devices are recognized by the network as genuine equipment. Another practice is to intercept genuine devices and tamper with their software so it appears to be an upgraded (and more expensive) version or even change internal genuine parts, such as batteries, with counterfeit versions in order to sell the genuine parts on the market.

Type approval logos and icons as well as electronic identifiers are often deliberately subverted in order to evade customs and law enforcement checks at borders. This creates practical issues for manufacturers, consumers, customs and law enforcement officials who then have trouble distinguishing the fake identifying marks of counterfeit equipment from genuine ones, even before considering the product itself.

8.2 Tracking of counterfeit ICT device producers and traffickers

When an irregular device is identified, the involved agents should trace back the economies of origin, producers and traffickers of the illegal devices and remove the producers and traffickers from the market [b-OECD].

Without effective identification and enforcement actions against producers and traffickers in the provenance economies, actions in the destination economies may not be effective.

8.3 Removal of counterfeit ICT devices already in use in the market

Post market control of counterfeit ICT devices is dependent on opportunities to act upon them. Potential actions could be (i) the detection and verification, physically or remotely, against the characteristics of the original product, (ii) ceasing their usage and/or (iii) seizing the item.

These opportunities and actions present several challenges:

– To physically verify an item, a few opportunities arise: during a servicing event, a market surveillance event, or in some situation where a legal authority is entitled to check the device. The challenge here is to create the required knowledge base and interest in the agencies to perform such tasks.

– Verification could be done logically or remotely, for example, by cross checking unique identifiers and product fingerprints during some sort of on-line system registration, however this generally requires a connection to the Internet and this may be challenging in remote or rural environments, particularly in developing countries of the world. Even though electronic processes should take part, it is necessary to be able to contrast physical characteristics with information in the databases of the product.

– If the device uses a unique identifier to register on the network, such registration can be denied for counterfeit ICT devices by using a database with the authorized devices to operate on a specific market. The challenge is to build and maintain the registration system and a database especially if a considerable number of devices have already been deployed without this kind of control.

– Care should be taken to avoid the abuse of identifier and registration systems, to respect consumer rights and to not negatively impact users of ICT devices. Consumers should also be protected from arbitrary disconnection from networks.

– The seizure of counterfeit ICT devices depends on a physical verification and, in most cases, will involve or require the work of law enforcement agencies that relies in a legal framework that supports judicial actions that could arise. Challenges reside on establishing cooperation between different agencies, on defining a legal framework and on determining responsibility for counterfeit ICT devices.

– The impact on the user should not be underestimated. It should be considered that disconnecting any device may not be permitted in some countries and that the user's life may be put at risk.

8.4 Limit the import, circulation and sale of new counterfeit ICT devices on the market

Measures that limit the import, smuggling, circulation and sale of new counterfeit ICT devices on the market should be implemented in addition to actions aimed to remove those in inventories or already in use.

This approach can assist to reduce the overall presence of counterfeit ICT devices on the market within the financial and time constrains of the administration that choose to take these actions and reduce the end user impact when compared to actions that aim to disconnect counterfeit ICT.

As quoted in clause 8.2, these measures should also focus on the sources of the counterfeit ICT device.

8.5 Differentiation between genuine and counterfeit ICT devices

To guarantee the effectiveness of actions to remove counterfeit ICT devices deployed on the market and to deter entrance of new ones, it is necessary to implement solutions and criteria able to differentiate between genuine and counterfeit devices. This needs to be performed with considerable accuracy even when considering cloned unique identifiers, so that disruptive actions can be taken preferably through automated systems or manually for limited numbers of ICT devices.

The following aspects should be considered when differentiating between genuine and counterfeit ICT devices:

– The counterfeiter's objective is to create a product which is very close to the genuine original product.

– The counterfeiter may actively attempt to confuse inspection by providing false or purloined genuine documentation, hardware and software as part of their counterfeit.

– Some elements of a counterfeit product can come from a genuine product and its accessories, including but not limited to: software, unique identifiers, casing hardware, printed circuit board (PCB) layout and chipsets.

– Genuine products are subject to regular firmware software updates, primarily for security reasons. This also applies to applications and for some accessories. As such, a defined device "fingerprint" of a genuine product can be challenging.

– Many times, visual inspection will not be enough to differentiate a genuine device and further technical expertise, support or laboratory tests could be required.

8.6 Limit impact on authentic ICT device manufacturer

Solutions utilized to combat counterfeit ICT devices should limit as much as possible the impact on authentic ICT device manufacturers and focus on the counterfeit ICT devices, the producers and traffickers of such products.

Therefore, schemes which add additional cost to the manufacture and disposal of a legitimate device by an authentic manufacturer should be avoided because they also inadvertently benefit the counterfeiter, that usually relies on cheaper prices to get the consumers to actively choose the counterfeit ICT device.

8.7 Reduction of end-user impact when considering removing counterfeit ICT devices

Any solution adopted to remove or disconnect counterfeit ICT devices should carefully consider the impact over end-users and, when multiple paths are available to achieve the same objective, adopt the one that reduces the overall impact on the consumer.

Therefore, the following challenges should be considered:

– Disconnecting ICT devices may not be permitted in some countries.

– Contacting users is not always possible through the device before it is disconnected (e.g., data or SMS only devices, call forwarding, interactive voice response (IVR) systems, among others, not having user contact).

– Blocking could be critical on counterfeit ICT devices that support critical business (e.g., medical applications a financial services among others.).
– Ensuring that users' rights are not violated and that such action is taken in accordance with national legislation.

8.8 Consumer education

Consumers should be educated on the issues associated with the purchase and continued use of counterfeit ICT devices, including but not limited to potential health risks and/or poor quality of service.

Consideration must be given to the fact that consumers often make an active decision to purchase counterfeit goods based on price, in spite of the potential consequences, therefore raising consumer awareness on the negative impact of the use of counterfeit ICT and benefits of genuine devices is essential.

8.9 Avoiding technical barriers to trade (TBTs)

Care should be taken not to prevent the valid importation and use of genuine ICT device, which would constitute a technical barrier to trade (TBT) as defined by the World Trade Organization (WTO) trade-related aspects of intellectual property rights (TRIPS) [b-TRIPS Agreement].

This may include the use of "white lists" which, through a mistake or a bad design decision, could prevent legitimate users, including travellers and tourists from using an ICT device. Such requirements to register devices could inadvertently create a TBT.

9 Framework requirements

When deploying a solution to address counterfeit ICT devices, countries should consider the following requirements:

9.1 Identification and enforcement actions against producers and traffickers of counterfeit devices

It is required to establish a process, while combating the use of counterfeit ICT devices deployed on the market or entering the country, to trace back the source and remove from market the producers and traffickers that deployed these products.

Since counterfeit ICT devices often cross different countries before being sold, it is required to establish a strong collaboration between the stakeholders involved on this process between the equivalent parties in the other involved countries to fulfill this requirement.

It is required to have identification and enforcement actions against producers and traffickers in economies of origin, as noted in clause 8.2.

9.2 Consultation with industry and consumer groups

It is required to establish communication with all stakeholders involved, such as network operators and industry and consumer groups, prior to any remedial action being taken, so that industry initiatives can be consulted and agreements reached on appropriate and reasonable courses of action that will create minimal disruption to the end users.

Additionally, the consumers can be aware of their obligations and rights regarding the use and acquisition of ICT devices and the combat of counterfeit ICT devices can have a reduced negative impact on all stakeholders. Every effort should be made to minimize and avoid any disruption and misunderstandings. All information provided should be clear and easy to understand by end users.

It is also required to implement actions focusing on promoting availability and accessibility of devices and consumer education showing the benefits of using legal devices and the negative implications associated with the use of counterfeit products.

9.3 Reliable unique identifier

Genuine ICT devices are required to have unique and persistent identifiers that are secure, in the sense that they cannot be changed by unauthorized entities, are unique to each equipment and have been assigned by the authorized assigner.

Manufacturers are recommended to store this unique identifier on a secure element on the equipment and implement security measures, to the extent technologically feasible, to detect the tampering of the unique identifier and as a result render the device inoperable until the original identifier is restored.

The identifier issuer entity is recommended to implement a process that ensures the correct and secure use of these unique identifiers.

9.4 Centralized reference database

It is recommended to deploy a centralized reference database of authorized equipment in a specific market, based on unique identifiers, to effectively differentiate between genuine and counterfeit ICT devices.

The following items should be considered when building this database:

– This centralized database should be shared with relevant stakeholders of the country, such as customs authorities, police enforcement and regulators, so that institutions can be aware of the transit of merchandise and, if is the case, stop the importation, circulation and sale of incoming counterfeit ICT devices on the market and aid tracking counterfeit producers and traffickers.

– This centralized database should be the cornerstone of the solution that aims to remove counterfeit ICT devices already in use in the market.

– Specific market databases exist which can provide information for products within that country, some of which are natural subsets or even linked in some way to a global database.

9.5 Deployment of a conformity assessment regime

The use of (or the establishment of) an existing robust conformity assessment scheme (CAS) is required to efficiently deploy a centralized national reference database of authorized equipment, based on type approval logos, icons or other unique identifiers created by authentic manufacturers of goods, so that all stakeholders (such as customs authorities, customers and industry) can differentiation between genuine and counterfeit ICT devices.

– Several national administrations, regional and international organizations, private companies and many ICT players have placed efficient CAS on the ground. In general practice, when related to the use of ICT at a global scale, devices necessary follow a set of internationally accepted standards and pass through conformity assessment procedures. (e.g., ITU lab recognition – CASC, ISO/CASCO, IECEE CB, GSMA, FCC, Innovation, Science and Economic Development Canada, ANATEL, GCF, PTCRB, ARIB, etc.).

– These organizations hold a large amount of data related to product control, for instance: entities responsible for the manufacture and selling of such products; sets of standards and national regulations (e.g., spectrum allocation) and the origin of the products.

– There are several ways to move forward with the establishment of an orderly ICT market. One example is: Under Pillar 4 of the ITU C&I Programme, different guidelines have been

produced. The C&I programme portal can be found at: http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

9.6 Close collaboration with customs authorities and appropriate domestic agencies

To effectively limit the circulation, import and sale of new counterfeit ICT devices on the market it is required to establish a close collaboration between the authorities responsible for the centralized national reference database, the customs authorities and between customs of distinct countries.

– As customs authorities and other relevant national authorized domestic consumer authorities play a critical role in the interception of counterfeit products it is important to give them the tools to identify counterfeit ICT devices, such as the Centralized National Reference Database.

– The illegal trade in ICT devices, including the counterfeit, contraband and stolen devices, can be combated by employing mechanisms to authenticate the identity of an individual device to check that it is the genuine article if permitted by the laws and regulations of that country.

– Enforcement procedures and communication between different organizations must be established and fully operational. This could include the exchange of relevant information, such as the national database of ICT devices in conformance with the national, regional or international standards.

– It is recommended that customs adopt an online inter-governmental platform that shares products information and alerts that assist in identifying counterfeit equipment, such as the World Customs Organization IPM [b-WCO-IPM].

9.7 Share information with end-user before any remedial action

It is required to inform consumers of the dangers of purchasing counterfeit ICT devices and that counterfeits may not be safe to use and may not perform as well as the genuine articles.

Furthermore, the motives for not allowing counterfeit ICT devices such as safety risks, lower quality of service and consequently increases in complaints, interference hazards, and intellectual property rights (IPR) infringement, etc. must be clearly explained to consumers and any eventual misinformation about the reasons behind procedures that may cause effects on the market should be clarified.

In case of developing the technological solutions to identify counterfeit ICT devices, it is recommended to provide a tool for the general public to check the authenticity of a product.

9.8 Support of applicable national legal and regulatory frameworks

Before implementing any restrictive actions against counterfeit ICT devices, it is required to have the support of an applicable national legal and regulatory framework, covering:

– The restriction of activation of counterfeit ICT devices on telecommunications networks;

– The restriction of the importation, circulation and sale of counterfeit ICT devices and accessories on the market which are not compliant with a country's legislative and regulatory framework;

– Establishment of the necessary solutions for the differentiation between authentic and counterfeit products by authorities, consumers and the sales channel;

– Enhancement of the security measures that deter the manufacture of counterfeit and other illegal products;

– Establishment of legal framework against the tampering of unique identifiers.

When considering this requirement due reference should be given to existing national legislation and regulatory frameworks that may already address aspects covered.

9.9 Consideration for products already in use in the market

Before any disruptive action of counterfeit ICT devices in the market, it is recommended to consider the need to protect the user of these products. This would mitigate negative impact to users of these devices who are not aware of national legal or regulatory provisions or requirements related to the purchase and use of these counterfeit ICT devices.

Blocking operational ICT devices may cause heavy and unexpected impacts to different types of networks, end users and infrastructure. In this case, one option is to adopt applicable transitional mechanisms, such as starting by blocking only new terminals and allowing devices that are already on the network to continue to operate but, ultimately, users will have to move to genuine terminals.

10 Possible counterfeit ICT solution approaches

Considering the requirements quoted above and based on information provided in the case studies contained in [b-ITU-T TR-Counterfeit] and gleaned from elsewhere, the following represent some possible approaches to combatting counterfeit ICT devices and some considerations that should be accounted when deploying some of these solutions.

10.1 Prohibit the use of invalid and non-genuine device identifiers

If the device uses a unique identifier to register on the network, such registration can be denied for counterfeit ICT devices by using databases with the authorized devices to operate on a specific markets.

In these cases, if the ICT device in fact possesses a reliable unique identifier, one could deploy solutions that would:

– block the equipment with invalid unique identifiers on their networks;

– block the use of equipment that is not type approved by the regulator;

– block the illegal import and sale of these devices.

If this path of actions is chosen, it is also recommended to raise the consumer awareness of these requirements. Besides, it may be required to adopt appropriate legislation changes at the national level as pointed out in clause 9.8.

When adopting a solution to combat counterfeit ICT devices by determination and blocking of devices with invalid unique identifier codes, this solution may also assist to:

– ensure that only legal devices are imported or sold thus having an effect on increases of the payments of customs duties and value-added tax;

– combat device theft by registering the unique identifier codes of stolen equipment in a "black list" upon lawful request;

– ensure the consumer protection against use of low-quality equipment, which could be unauthorized or dangerous for human health or which do not ensure adequate quality of services (protection is ensured by implementing the tool for easy verification of the legality of the equipment prior to its purchase).

Care should be taken in the standards process to respect the protection of personal information and not negatively impact the users of ICT devices via identifier registration mechanisms. Consumers should also be protected from arbitrary disconnection from networks.

More information on a possible implementation for a solution aimed for mobile devices can be found on Annex A.

10.2 Certification of the ICT device and market surveillance

As pointed out in clause 9.5, the deployment of a conformity assessment scheme (CAS) can assist on the construction of a national reference database of authorized equipment that contains the list of unique identifiers and additional information for the devices (such as approval marks, technical specifications and physical characteristics), so that all stakeholders (such as customs authorities, customers and industry) can identify approved devices.

Also, with this information customs officials would to be able to identify counterfeit products by imposing market surveillance and other enforcement measures which may be needed. In addition, importers with a track record of ignoring import controls can be identified and put on a special list. When shipments of ICT devices are being imported by smugglers, regulatory authorities can be notified so that a decision can be made to carry out inspections and enforcement should then be warranted.

As an integral part of the CAS policy, the market surveillance of deployed telecommunication equipment has the objective to ensure that products placed on the market do not cause electromagnetic interference, harm the public telecommunications network and endanger health, safety or any other aspect to protect the public.

In practice, market surveillance includes any necessary action (e.g., prohibitions, withdrawals, recalls) to stop the circulation of products that do not comply with all the requirements set out in the relevant legislation and regulations, to bring the products into compliance and to apply sanctions.

Market surveillance is vital to the smooth functioning of the telecommunications marketplace. It is essential in protecting consumers and workers against risks presented by non-compliant products. In addition, market surveillance helps to protect responsible businesses from unfair competition by unscrupulous economic operators who ignore the rules or cut corners.

Many regulatory bodies worldwide have specific legal requirements for the organization of market surveillance. Regulations characteristically set out clear obligations for market surveillance authorities, stipulating that they must have the necessary powers, resources and knowledge to properly perform their functions [b-ITU-T-CI-Portal]. The regulation requires procedures to be put in place for following up complaints, monitoring accidents, verifying that corrective action has been taken and gathering scientific and technical knowledge concerning safety issues. In addition, ITU Member States establish, implement and periodically update national market surveillance programs and review and assess the functioning of their surveillance activities periodically e.g., every few years. [b-ITU-D-CI-Guidelines]

EC Regulation No. 765/2008 defines market surveillance as: activities carried out and measures taken by designated authorities to ensure that products comply with the requirements set out in the relevant legislation and do not endanger health, safety or any other aspect of public interest protection. [b-EC-Regulation]

Therefore, to complement the actions being taken at the moment the product arrives at the country's borders, it is recommended to have additional post-market surveillance to assist in identifying counterfeit goods and therefore guarantee the product being sold to the end-user in fact corresponds to the one that was submitted to the certification process. [b-ITU-D-Rep]

The United Nations Economic Commission for Europe (UNECE) recommends that national market surveillance and customs activities be coordinated and that rights holders be given the possibility of informing market surveillance authorities about counterfeits [b-UNECE].

10.3 Device lifecycle management

The ability to discern between an original ICT device and a clone, without compromising the rights of a user, is desirable. These clones normally abuse the identifiers or other uniquely identifying elements to purport to be the original device.

To assist these stakeholders and guarantee the authenticity of the products, one possible solution should be to deploy a device lifecycle management system, based on these unique identifiers, that are able to track the ICT devices from the beginning of the manufacture process (including component origin, transportation and retail store where it will be sold) until it is delivered to the end-user.

This information should be available to all stakeholders and, even though the counterfeit could clone the unique identifiers, the authorities and even the end-user would be able to verify the authenticity of this information. For instance, if a user is in a store in one country and by checking the unique identifier, the tool would show that the product is supposed to be sold at another retailer or even another country. This should be strong evidence that, even with a unique identifier that is valid, the product is a counterfeit.

Care should be taken when using this kind of solution while addressing the resale of used products by end-users, since the national legislation should consider the impact on protection of personal information to have the link between the user and the device being managed.

It should be considered that the product identified by this kind of approach may not be a counterfeit but instead a genuine product sold on a grey market and additional actions to identify the counterfeit product would be needed.

11 Reference framework

Based on the common points of the different possible approaches presented in clause 10, a proposed framework to address the production, circulation and use of counterfeit ICT devices is depicted in Figure 1.

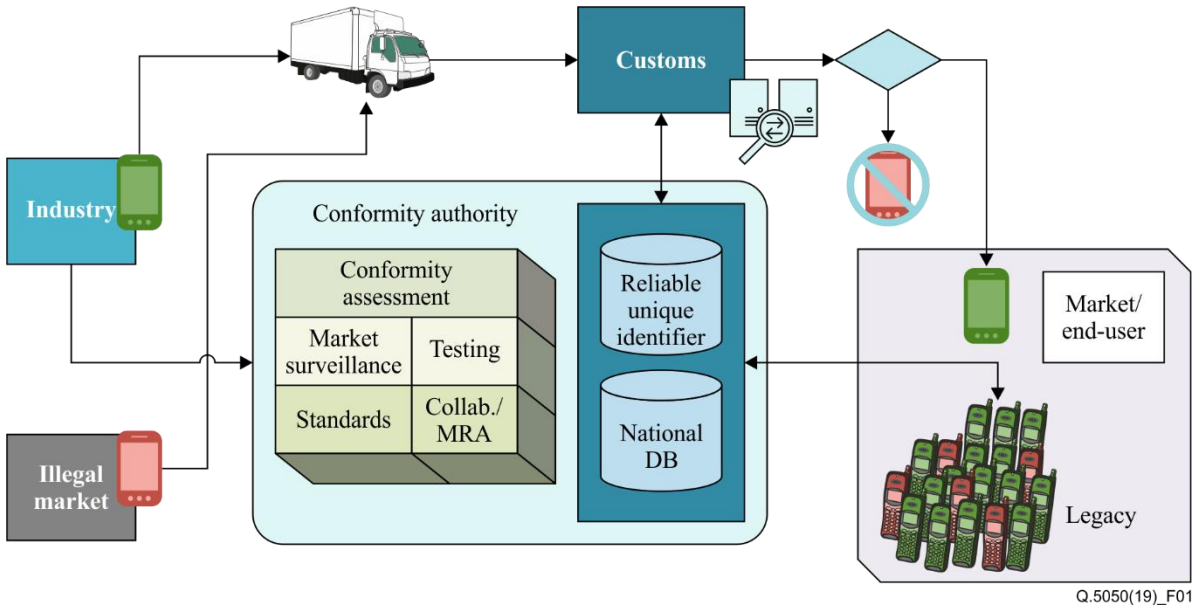

Figure 1 – Proposed general framework

A diverse range of activities and information systems, operated by different organizations, should work together to control and produce critical information to identify and combat the use of counterfeit and tampered devices.

The legal commerce allows checking that a product entering a country is compliant and has a representative/responsible for the equipment.

When the products arrive at a control point, an entity (e.g., customs) verifies all legal aspects of such devices, including compliance of the devices with any applicable regulatory and certification

requirements such as radio frequency allocation, safety and interoperability, etc. Checks can also be conducted against device white list[1] to verify that the identifiers of the devices being imported have been legitimately allocated and that the make and model of device being examined matches the details recorded when the identifiers were issued.

At this time, non-authorized products, such as counterfeit products, are prevented from entering the market. Entity personnel are supported by a conformity assessment regime that may be in place and a database with stored information on what should be in the containers being imported.

Such inventory databases can also support enforcement activities once equipment (legal or not) is placed in the market.

[1] e.g., GSMA Global TAC database may be used to assist building a White List for 3GPP compliance devices.

Annex A

Mobile devices solutions

(This annex forms an integral part of this Recommendation.)

When dealing with 3GPP compliant mobile devices, some solutions to identify genuine and legally imported mobile terminals are based on the use of the international mobile equipment identity (IMEI) registration system. The solutions relying on IMEI to deter the spread of counterfeit mobile devices are based on:

– blocking the mobile devices with invalid IMEI (e.g., no IMEI, all-zero IMEI, non-standard format strings, duplicate IMEIs, IMEIs allocated by unauthorized organizations and valid IMEI still not allocated by the designated organization) numbers on their networks,[2]

– performing other actions on consumer awareness, enforcement measures and appropriate legislation changes on the national level.

To block the use of counterfeit mobile devices the system may be deployed based on a register of every valid IMEI code (identifier according with standards, formally allocated by a designated organization, legally imported and type approved or homologated) of mobile devices that shows activity in national networks. The registration of mobile device IMEIs ensures that the mobile devices are in compliance with national regulations and, in some countries, that they have been legally imported.

- **Reference databases**

The IMEI codes are used to create a database with "white list", "grey list" and "black list" of devices. A "white list" is the register of the devices authorized to be used in the country (such as those that have been legally imported or manufactured in this country), a "grey list" is the register of devices of unconfirmed status (not entered into the "white list" or "black list") and a "black list" is the register of devices for which services must be denied in the telecommunication network.

Prior analysis should be conducted on what impacts on networks and users could have a "white list" "grey list" and "black list" deployment, since it could limit the movement of devices between countries and impact on foreign visitors and network operators.

The "grey list" and "black list" are generated automatically by processing the data from "white list" and data from operators, importers and the customs authority.

- **Integration with the operator network**

To ensure active interaction with the registration system the telecommunication operators have to maintain their equipment identity registers (EIRs) and ensure the regular synchronization and automatic data exchange between the EIRs and the database of IMEI codes (e.g., on daily basis).

With the first connection and registration of a mobile phone with an operator network, the IMEI code of the terminal is forwarded by the mobile operator to the database. The system reveals the IMEI codes which are not available in the "white list", identifies the counterfeit mobile devices and registers the corresponding IMEI codes in the "grey list". An owner of the respective terminal receives a SMS notice and has to confirm the terminal's legal origin within specified period after the date of entering the "grey list".

The reliability and security of the registration system and associated processes should be ensured. An access to the database is generally provided to the regulatory and customs authorities, network

[2] The GSMA Global TAC database may be used for validating misappropriated or cloned IMEIs for 3GPP compliant devices.

operators and the general public with appropriate levels of access privileges. Users should have access to this database to check whether a mobile device is allowed to operate in the country (usually, by sending an SMS or using a webpage).

It is important to note that SMS should be considered an insecure medium by which to communicate with a customer and it could be exploited by fraudsters, so additional measures may be needed.

- **Detecting cloned IMEI**

As it is possible to tamper with the unique identifiers of some devices and it is probable that traffickers start cloning IMEIs of regular devices to avoid this system, additional measures should be implemented to identify and act against irregular devices with cloned legitimate IMEIs.

One possible path is the adoption of a database with additional information on the product that could be used to verify if the product using the identifiers is in conformity with the other attributes. These tools could be implement with the assistance of a support conformity assessment regime that would collect this information during the certification process of the device and store it on a database accessible to all the stakeholders.

- **Additional consideration**

Besides, a solution to combat counterfeit mobile devices by determination and blocking of the mobile devices with invalid or tampered IMEI codes, this solution may also assist in:

– blocking the illegal import of these devices and therefore ensuring that mobile devices have been imported and sold legally and thus may increase the payments of customs duties and value-added tax;

– combating handset theft by registering the IMEI codes of stolen terminals in the "black list" upon lawful request, which makes theft of terminals useless (the same procedure may be applied to the terminal lock-out upon the request of the owners of the lost mobile devices);

– blocking the use of equipment that is not type approved by the regulator, ensuring the consumer protection against use of low quality mobile terminals, which could be unauthorized or dangerous for human health or which do not ensure adequate quality of mobile communication services (protection is ensured by implementing the tool for easy verification of the legality of a mobile phone prior to its purchase).

It is important to keep a nationally coordinated approach, since counterfeit ICT devices could be present in more than one network and the detection process should attend efficiently in the actions to be taken in order to avoid multiple user's impacts, duplicated efforts or conflicts across the different mobile operators.

Early stages of diagnosis (sizing of the problem of identifiers invalids, cloned, etc.) planning of the process to detect and control, resources required (money, staff, time) and impact analysis to reduce affecting end users should be conducted and discussed with all stakeholders to implement such solutions.

It should also be considered that in some cases such mechanisms can cause issues for legitimate users, including travellers and tourists, such as:

– A foreign visitor travelling into a country, then using a local subscriber identification module (SIM) card in their device may be caught in a white listing trap where they are unable to use their device at all.

– A roaming visitor who continues to use his device for a few months may also be unfairly penalized by local white listing after a period of usage.

– A registration message may be sent to a visitor to a country who is using a local SIM, however they may not speak the local language and so cannot understand the message.

They consequently do not act on the registration and their device is blacklisted. This either: i) causes disconnection of the visitor from the local network or; ii) causes the visitor's legitimate device to be blacklisted in other countries because of sharing arrangements, despite the device being entirely legitimate.

As such these mechanisms if poorly implemented can cause issues and these scenarios should be avoided by design. Finally, this functionality must not be used to arbitrarily disconnect users from networks for other reasons**.**

Appendix I

Other industry solutions

(This appendix does not form an integral part of this Recommendation.)

Industry has invested in multiple efforts to address the problem of counterfeit equipment and to improve the trustworthiness of equipment and companies. These are industry-driven efforts to develop voluntary solutions to enhance security of the supply chain. Counterfeit equipment is one aspect of these efforts, but not the only one. Industry must also work with governments, specifically law enforcement and customs for enforcement. It is best to think of the outcomes of these efforts as a toolkit that companies can draw from depending on need and specific circumstance (e.g., product, market, etc.).

Note that industry activities on counterfeit products cover a very wide range of products with varied supply chains, some with different needs. This is a complex interaction with multiple participants. In addition to these external activities companies carry out highly sensitive and confidential research and development to develop ways to combat counterfeiting.

Below is a non-exhaustive overview of some efforts to enhance device security that can contribute towards making counterfeiting more difficult.

- **GSMA IMEI database**

The IMEI is a 15-digit number that is used to identify a device on a mobile network. The type allocation code (TAC) is the first 8 digits of the IMEI that identify a specific model.

The Global System for Mobile communications Association (GSMA) maintains a global database which contains information on specific TACs that are assigned to 3GPP compliant devices. This database is known as the IMEI database.

This database could be used in the following ways:

– Identification of counterfeit ICT devices can be accomplished in collaboration with the genuine manufacturer who can be identified using the GSMA TAC database list.

– The GSMA TAC database can be made available to government entities, such as ministries, regulators, customs and law enforcement, as a source of information about the provenance and specification of mobile devices. This information can be used to identify anomalies and identify the device producer who cannot confirm whether the device is genuine.

– The authenticity of mobile device producers and their IMEI can be verified using the GSMA TAC database. Customs and law enforcement agencies can use the GSMA helpdesk to verify the TAC certificate serial number submitted by the producer. This is a second serial number associated with each TAC. A mismatch between these identifiers indicates some form of identifier falsification.

– Regulators can use the GSMA TAC database to ensure that mobile devices being tested on the conformance assessment match the description of the model listed on the database.

GSMA IMEI Database: https://imeidb.gsma.com/imei/index

GSMA IMEI Services: https://www.gsma.com/services/tac-allocation/the-imei-database/

- **Device Identification, Registration and Blocking System**

The Device Identification, Registration and Blocking System (DIRBS) is a server-based software platform intended to address counterfeit, illegal and stolen mobile devices in a country. The DIRBS software platform is available as open source to assist governments, regulators and others in their efforts to combat the improper use of counterfeit, illegal and stolen devices on cellular networks.

The platform is consistent with the International Telecommunication Union's recommendations for addressing illegal and non-type approved devices in a country.

DIRBS consists of a country-level device database that interfaces at different levels of detail with operators, local manufacturers, importers, consumers, customs, law enforcement and the global GSMA IMEI database. The DIRBS platform consists of an analysis engine and associated subsystems that provide information to enable blocking of counterfeit and fraudulent devices; actual blocking is determined by country-specific governing rules and performed via operator's equipment identity register (EIR) mechanisms.

More information can be found at: www.qualcomm.com/dirbs

- **Trusted Computing Group**

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.

Among other areas, the TCG has developed a specification for a trusted platform module (TPM) relevant to this topic:

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

As mentioned at the above-mentioned web site, TPM is a computer chip (microcontroller) that can securely store artefacts used to authenticate the platform (your PC or laptop). These artefacts can include passwords, certificates, or encryption keys

This mechanism allows for both local and remote attestation that helps establish trust that the equipment is authentic.

The TCG has also started an Embedded Systems working group to address the security of embedded systems, including Internet of things (IoT):

http://www.trustedcomputinggroup.org/developers/embedded_systems

- **Global Platform**

Global Platform has developed the standards for the trusted execution environment (TEE) which has been adopted in modern mobile devices as a method of securely storing and executing sensitive security code and assets.

More information can be found at: https://www.globalplatform.org/specificationsdevice.asp

- **ISO/IEC JTC1/SC27**

The scope of SC27 is important to the industry's activities related to security and mitigating counterfeit and the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and protection of personal information.

Among its other work SC27 has published standards relevant to counterfeit equipment, such as:

– [b-ISO/IEC 15408]: *Information technology – Security techniques – Evaluation criteria for IT security" (Common Criteria)*;

– [b-ISO/IEC 27034] *Information Technology – Security Techniques – Application Security*;

– [b-ISO/IEC 27036-3]: *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*;

– [b-ISO/IEC 20243]: *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

More information can be found at: http://www.din.de/en/meta/jtc1sc27

- **The Open Group Trusted Technology Forum**

The Open Group Trusted Technology Forum (OTTF) leads the development of a global supply chain integrity program and framework in order to provide buyers of IT products with a choice of accredited technology partners and vendors. Note that the [b-ISO/IEC 20243] listed above was first developed by The Open Group.

More information can be found at: http://www.opengroup.org/getinvolved/forums/trusted

- **Institute of Electrical and Electronics Engineers**

The Institute of Electrical and Electronics Engineers (IEEE) has developed a standard for secure device identity and a method for cryptographically binding the identity to the device, such as the IEEE 802.1ar – "Standard for Local and Metropolitan Area Networks: Secure Device Identity".

As pointed on the IEEE website: This standard specifies secure device identifiers (DevIDs) designed to be used as interoperable secure device authentication credentials with extensible authentication protocol (EAP) and other industry standard authentication and provisioning protocols. A standardized device identity facilitates interoperable secure device authentication and simplifies secure device deployment and management.

More information can be found at: http://www.ieee802.org/1/pages/802.1ar.html

- **Other industry activities related to counterfeit include**

ICC – Counterfeiting Intelligence Bureau

http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

ICC – Business Action to Stop Counterfeiting and Piracy (BASCAP)

http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/

Bibliography

[b-ITU-T-CI-Portal] ITU C&I Portal under Pillar 4 keeps updated information on country's C&I regulatory framework http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

[b-ITU-T TR-Counterfeit] Technical Report on Counterfeit ICT device (2015).

[b-IEEE 802.1] IEEE 802.1 (2009), *Standard for Local and Metropolitan Area Networks: Secure Device Identity.* – http://www.ieee802.org/1/pages/802.1ar.html

[b-ISO/IEC 15408-1] ISO/IEC 15408-1:2009, *Information technology - Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/IEC 17000] ISO/IEC 17000:2004, *Conformity assessment – Vocabulary and general principles*.

[b-ISO/IEC 20243] ISO/IEC 20243:2015, *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

[b-ISO/IEC 27034] ISO/IEC 27034:2011, *Information technology – Security techniques – Application security*.

[b-ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[b-EC-Regulation] Market Surveillance Regulation EC no. 765/2008.

[b-Gartner] https://www.gartner.com/it-glossary/gray-market

[b-ITU-D-CI-Guidelines] ITU Guidelines on Establishing conformity and interoperability regimes: Complete Guidelines (2015), ITU http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf

[b-ITU-D-Rep] Final Report for the Question 4/2 – Question 4/2: Assistance to developing countries for implementing conformance and interoperability programmes, ITU-D Study Groups, 2017, https://www.itu.int/pub/D-STG-SG02.04.1-2017

[b-OECD] 2017 OECD report "Trade in Counterfeit ICT Goods".

[b-TRIPS Agreement] Trade-Related Aspects of Intellectual Property Rights; annex of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.

[b-UNECE] Recommendation M. on the: Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[b-WCO-IPM] World Customs Organization IPM – http://www.wcoipm.org/

[b-WTO-TBT] World Trade Organization – WTO Agreement on Technical Barriers to Trade.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019