ITUPublications International Telecommunication Union

ITU-T Technical Report

(12/2015)

QSTR-COUNTERFEIT
Counterfeit ICT equipment

Technical Report ITU-T QSTR-COUNTERFEIT

Counterfeit ICT equipment

Summary

Counterfeiting is widely recognized as a significant and growing socio-economic problem. This Technical Report provides background information on the nature of the issues related to the counterfeiting of information and communication technology (ICT) equipment, a review of the international conventions covering this type of infringement of intellectual property rights and the activities of organizations in the enforcement of these rights, and a description of a range of means to combat the trade in counterfeit products. In addition, a number of national and regional initiatives to combat the counterfeiting of mobile devices are described in Annex A.

Change log

This is version 2 of the ITU-T Technical Report on "*Counterfeit ICT Equipment*" approved at the ITU-T Study Group 11 meeting held in Geneva, 2-11December 2015.

Editor: Keith Mainwaring
UNIS
E-mail: keith.mainwaring@ukrainesystems.com

Keywords

Counterfeit, substandard.

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.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

Technical Report ITU-T QSTR-COUNTERFEIT

Counterfeit ICT equipment

1. Introduction: counterfeiting products – a growing problem

Although very difficult to measure, there is evidence accumulating that the distribution of counterfeit products is a growing problem, both in magnitude and in the range of products affected. In 2008, OECD [60] published a report that estimated, on the basis of customs seizures, the total international trade in counterfeit and pirated goods (not including digital products or those produced and consumed domestically) to be more than USD 200 billion in 2005. This estimate was updated on the basis of the growth and changing composition of international trade from just over USD 100 billion in 2000 to USD 250 billion for the year 2007, accounting for 1.95% of world trade [1]. Some estimates are even higher, the International Chamber of Commerce (ICC) Counterfeit Intelligence Bureau estimates that counterfeiting accounts for 5 - 7% of world trade to the value of USD 600 billion per annum [2].

The ICC Business Action to Stop Counterfeiting and Piracy (BASCAP) group commissioned a study [45] to complete the picture of the economic and social impacts of counterfeiting and piracy given by OECD. This report presents an estimation of the total global economic value of counterfeit and pirated products to be as much as USD 650 billion per year, of which international trade accounts for more than half (USD 285 billion to USD 360 billion), domestic production and consumption between USD 140 billion and USD 215 billion and digital content (music, movies and software) between USD 30 billion and USD 75 billion. In addition, it is estimated that counterfeiting and piracy cost G20 governments and consumers over USD 125 billion each year (due to factors such as decreased tax revenues and increased spending on counter-measure enforcement and health care) and the loss of approximately 2.5 million potential jobs.

The European Union's (EU) national customs authorities have registered that counterfeit goods entering the EU have tripled between 2005 and 2010. The statistics published by the European Commission in July 2011 show a tremendous upward trend in the number of shipments suspected of violating intellectual property rights (IPRs). Customs authorities registered around 80,000 cases in 2010, a figure that has almost doubled since 2009. More than 103 million fake products were detained at the EU external border.

http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf

An extremely wide range of products is counterfeited - food and drinks, pharmaceutical products, electrical and automotive components, all manners of consumer products and even a whole store. Computer components (monitors, casing, hard drives), computer equipment, routers, webcams, remote controls, mobile phones, televisions (TVs), compact discs (CDs) and digital versatile disc (DVD) players, loudspeakers, cameras, headsets, universal serial bus (USB) adaptors, software, certificates, certification marks and data (such as biometric data) are all counterfeited.

In addition, the Internet has been used increasingly for digital piracy and also as a marketplace for counterfeit goods. All of the factors which make the Internet an attractive resource for retailers, especially those retailers aiming at thin markets (global market reach, ease of establishing, moving and closing websites that can be made to look very attractive and convincing, and cheapness of sending e-mail) coupled with the possibility to remain anonymous, make it attractive for those selling counterfeit goods. And the huge number of sites on the Internet make it very difficult for intellectual property rights owners and enforcement agencies to identify illegal operations. E-mail solicitations, e-commerce and auction sites are all used in attempts to sell counterfeit goods.

As far as the ICT industry is concerned, a KPMG and AGMA report estimated that 8% to 10% of all goods in the information technology (IT) industry sold worldwide were counterfeit, and counterfeiting

led to a loss in revenue of USD 100 billion to the IT industry in 2007. Hewlett-Packard alone performed over 4,620 investigations in 55 countries between 2005 and 2009 resulting in the seizure of counterfeit printing supplies worth more than USD 795 million [3]. Consumer electronics accounted for 22% of US Customs seizures in 2011 with the value of goods increasing by 16% over 2010. About a third of the goods in this category were mobile phones [53].

In 2011, there was an estimated global market of 250.4 million counterfeit mobile phones. http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline. This corresponds to about 16% of the 1,546 million handsets sold in 2011 [48]. This is a similar estimate of the extent of the penetration of counterfeits in the mobile phone market as that in the study on internationalization and fragmentation of value chains and security of supply, prepared in 2011 for the European Commission, according to which counterfeit mobile phones constitute 15%-20% of the global market in terms of units sold and about USD 9 billion in revenue.

In addition to the production of counterfeit devices, counterfeit electronic components are being introduced in legitimate product supply chains. The use of counterfeit electronic components in the US military equipment hit the headlines in the fall of 2011 when a hearing was held of the Senate Armed Services Committee on counterfeit electronic components in the Department of Defence supply chains [5]. A study conducted by the Department of Commerce's Bureau of Industry and Security [42] estimated that there were some 1,800 cases of counterfeit electronic components being introduced in defence contract supply chains, involving more than a million components. The number of incidents was also found to be rising from 3,868 in 2005 to 9,356 in 2008. As a result of this hearing, the 2012 National Defence Authorisation Act (NDAA) includes guidance on dealing with counterfeit components, including the performance of additional inspections of imported electronic components, and assigns full responsibility to contractors for detecting fake components and rectifying any case in which fake components have found their way into products [33].

The 2008 OECD study found that most counterfeit products originate in one country in Asia (accounting for 69.7% of counterfeit product seizures).

This Technical Report sets out to provide background information on the problem of counterfeiting and how it is being tackled with emphasis on the counterfeiting of ICT equipment and on the ICT tools that could be used to mitigate this problem.

In addition to counterfeit devices, there is also a proliferation of ICT equipment and accessories which are commonly referred to as "substandard" or "unauthorized". Although there is no universal standard definition of these terms, these devices often use inferior components and, in most cases, do not comply with applicable national legal requirements regarding the certification, approval, distribution and sale of mobile devices. These devices do not, in every case, involve the infringement of intellectual property rights of device manufacturers, and therefore do not fall within the accepted definition of "counterfeit"; consequently, they do not fall within the scope of this Technical Report, which is concentrated on counterfeit devices. "Substandard" devices constitute and present a distinct set of problems and remedies that require separate consideration.

2. What is counterfeiting?

The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement) defines counterfeit trademark goods as "any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation" (footnote 14 to Article 51). The term "counterfeit" is therefore used in the TRIPS Agreement only in the trademark area. It refers to infringing goods which are defined more precisely

than ordinary trademark infringements on the basis that the trademark is identical to or essentially indistinguishable from the original. This text does not touch on the intention behind the use of the counterfeit trademark. It defines a counterfeit product in terms of the closeness of the mark used to a registered product and applies to cases where the goods are the same as for which the trademark is registered. In practice, such infringing goods would typically include cases where a mark is slavishly copied, deliberately to give the impression of identifying a genuine product. This would usually involve intent to defraud since the confusion between the genuine product and the copy is deliberate.

The same footnote in the TRIPS Agreement defines pirated copyright goods as "any goods which are copies made without the consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation". The term "piracy" thus relates to infringement of copyright and related rights in the TRIPS Agreement.

3. Impacts of counterfeit ICT equipment and components

There are unique impacts on society related to counterfeit ICT equipment that may not exist for other types of intellectual property rights violations. Counterfeit products, for example, will not usually have been formally tested, nor approved according to any regulatory requirements that may be applicable. The use of counterfeit products can be extremely dangerous. For example, there are reports of deaths due to the explosion of counterfeit batteries, cases of electrocution and fires caused by chargers, and documented instances of these devices containing high levels of hazardous substances such as lead and cadmium.

The 2008 OECD report included assessments of the socio-economic effects and the effects on rights holders, consumers and governments:

– Considering the socio-economic effects, counterfeiting may well have a negative effect on innovation, levels of foreign direct investment, growth in the economy and levels of employment and may also redirect resources into organized criminal networks.
– Counterfeiting is likely to have an economic impact on rights holders as sale volumes and royalties, prices, brand value and reputation, costs and scope of operations may be affected.
– Consumers may find that the quality of counterfeit goods is substandard and also be presented with serious health and safety risks.
– Governments will not receive as much in taxation, and will possibly face issues of corruption and also need to expend additional resources in combating counterfeiting activities.

3.1. Counterfeit ICT equipment examples

The following are key examples of the impact of counterfeit ICT equipment:

3.1.1. Mobile phones

Counterfeit mobile phone and accessories negatively impact society by, among other things:[1]

– lowering the quality of service of mobile telecommunication services, thus impacting the experience of consumers and businesses;
– creating a safety hazard for consumers due to use of defective or inadequate components or materials;
– raising cybersecurity-related threats;
– jeopardizing consumer privacy;

[1] The following is based on the MMF Counterfeit/Substandard – A Resource Guide for Governments. http://spotafakephone.com//docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf

– impairing the safety of digital transactions;
– evading applicable taxes and duties and hence negatively impacting government tax coffers;
– hurting the most financially vulnerable consumers by failing to provide any warranties to the consumer and otherwise violating consumer law requirements;
– creating risks to the environment and consumer health due to the use of hazardous substances in the manufacturing of these devices;
– facilitating the drug trade, terrorism, and other local and international criminal activity;
– causing economic harm given the market distortion caused by the unfair competition and deceptive practices; and
– damaging the trademarks of companies who manufacture the original products.

A study by the Instituto Nokia de Tecnologia (INdT), an independent research and development entity based in Brazil, confirmed the poor quality of counterfeit phones and the potential negative impact it had on consumers, telecommunications carriers and local economies. The study examined 44 counterfeit and substandard cell phones, comparing them with genuine and homologated equipment. The study shows that the counterfeit phones failed in 26% of call attempts and 24% of established calls were dropped. Additionally, in places where a genuine phone could work perfectly, counterfeit phones would not be usable because of their lower quality of transmission when compared to original phones. There were also issues with cell handover (the ability to maintain the call while moving between cells) with handover time being 41% longer than original phones and 34% of calls dropped during the handover. See Figures in Annex 1 of Mobile Manufacturers Forum's (MMF) Counterfeit/Substandard mobile phone - Resource guide for Governments.
http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf.

Counterfeit mobile phones also pose significant health and safety risks. Such devices may contain levels of chemicals that exceed established safety standards and they are more difficult to collect through e-waste management programmes. This has an impact especially in developing countries which have limited or no environmentally sound recycling capabilities and with large volumes of counterfeit mobile devices. Tackling the counterfeit device issue by disabling these devices further compounds this problem for developing countries.

Counterfeit products, because of their poor assembly and use of poor quality components, contain hazardous substances that are banned in many countries under the restriction of hazardous substances (RoHS) or national equivalent legislation.

Another recent study conducted by the Nokia Institute of Technology in Brazil (INdT) on hazardous substances illustrates the potential dangers from counterfeit phones. Specifically, the objective was to evaluate whether counterfeit phones were compliant with RoHS, and the EU Directive on the restriction of use of certain hazardous substances in electrical and electronic equipment. This directive restricts the use of six hazardous materials in various types of electrical and electronic equipment.

The study, using the IEC 62321 [IEC 62321:2008] standard test method, involved testing five counterfeit phones and 158 parts including the covers, displays, integrated circuits (IC), keyboard and other surface-mounted device (SMD) components. The INdT study revealed the presence of two hazardous substances (lead and cadmium) in both internal and external components at concentrations much higher than the maximum values permitted by RoHS. Figure A: Hazardous Substances Chemical Analysis in MMF's Counterfeit/Substandard mobile phone - Resource guide for Governments http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf illustrates the excessive level of lead and cadmium found on internal and external components of the tested mobile phones.

Other studies conducted in other countries have confirmed the existence of hazardous substances in counterfeit mobile phones. The Centre for Materials for Electronics Technology (C-MET), in Hyderabad, India, undertook a study to test RoHS compliance of mobile handsets being put on the Indian market. For this study, C-MET selected 15 widely available mobile phone models for testing.

The phones were chosen based on their popularity and availability in the Indian market and the tests were also undertaken using IEC 62321 (2008) procedures.

The results were that all of the counterfeit mobile phones were found to contain alarmingly high proportions of hazardous substances, especially lead (Pb). In some cases, the values were 35-40 times higher than the globally acceptable limits for Pb. Many of the critical components like the memory card slot, subscriber identity module (SIM) slot, camera, etc., that come in direct physical touch with consumers fared the worst in terms of hazardous material content, which obviously increases the risk for consumers than if the components were inside the device. In contrast, mobile phones tested from global and other recognized brands were found to be within the RoHS limits and therefore safe for consumer use. Figure B in MMF's Counterfeit/Substandard mobile phone - Resource guide for Governments http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf summarizes the results of this study, while Figure C in MMF's Counterfeit/Substandard mobile phone - Resource guide for Governments http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf demonstrates visually the areas where high concentrations of lead were found.

In addition, the use of phones with duplicate/fake/missing international mobile equipment identity (IMEI) numbers can present threats to national and personal security as they are difficult to trace on the network.

Finally, as an example of the revenues that may be lost due to the trade in counterfeit mobile devices, the Kenyan Anti-Counterfeit Authority claims that the country lost about USD 38.5 million due to this market in counterfeit mobiles [25]. The installation of the Automated Information System for Mobile Terminal Registration in Ukraine (AISMTRU) in 2009 resulted in an additional USD 500 million in revenue between 2010 and 2012 derived from the payment of customs import duties on mobile terminals. Prior to the implementation of this system in 2009, only 5%-7% of mobile devices in use in the Ukraine were legally imported, whereas today 92% – 95% are imported legally [39].

3.1.2. Accessories and components for ICT products

Often, it is the accessories of ICT products that are sold which are counterfeit. In the case of mobile phones, as well as other ICT products, it is the batteries, chargers, and headphones. In the case of printers, it is often the ink cartridges which are counterfeit. In the case of digital cameras, fake lenses which register correctly with the camera body are available amongst other fake accessories such as cables and memory cards. These fake components even go down to the chipset level. Accidental or deliberate replacement with fake electronic components could cause severe issues for users when used in medical equipment or other safety-critical ICT products. In 2013, unauthorized MIFARE contactless clones were seized at the CarteS conference in Paris.

http://www.mifare.net/files/6114/2295/3702/NXP_Whitepaper_Protect_your_reputation_with_genuine_MIFARE_products_2015.pdf

Counterfeit batteries are widespread across the world and are of particular concern. Counterfeit batteries are responsible for a number of fires. The types of counterfeit batteries range from Alkaline AA batteries to Lithium-ion rechargeable batteries which are included in many different types of product, most notably mobile phones.

Counterfeit batteries have been reported as causing deaths. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aLWvmmrHx9F0. In connection with that report, it was noted that counterfeit batteries are widespread in poorer areas given that there is a higher level use of the handset and hence a need to replace batteries more often.

Similar incidents have been seen in countries around the world. There is increasing concern about such batteries causing issues on aircraft after a number of reported incidents. In February 2014, the UK Civil Aviation Authority's Geoff Leach said that he was worried about "cheap, copycat batteries bought from dubious sources online, batteries that could develop a fault with dramatic consequences".

http://www.bbc.co.uk/news/business-25733346

In 2004, in testimony before the Committee on the Judiciary, United States Senate, a representative of Gillette explained that in a one-week operation they had seized one million fake Duracell batteries amongst many other counterfeit products.

http://www.judiciary.senate.gov/meetings/counterfeiting-and-theft-of-tangible-intellectual-property-challenges-and-solutions &

http://www.judiciary.senate.gov/imo/media/doc/Willard%20Testimony%20032304.pdf

Headphones are a concern because the poor quality of counterfeit headphones can not only potentially affect the ears but also represent a potential fire risk. In 2013, it was reported that officials seized GBP 15 million worth of fake headphones.

http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods

3.1.3. Two-way radios

Motorola Solutions Inc. has cautioned customers on purchasing counterfeit two-way radios that have been found in Vietnam in 2013. These counterfeit two-way radios may be hazardous for users; they are not only copies of Motorola's two-way radio designs, but they also carry unauthorized use of the Motorola logo and model numbers making it difficult for customers to differentiate them.

http://uk.reuters.com/article/2013/07/09/motorola-solutions-idUSnBw085384a+100+BSW20130709

3.1.4. Digital cameras

Digital cameras are part of the long list of ICT products that are subject to being counterfeited. As with other products, they are very difficult to identify and vendors, retailers and helpful users sometimes provide guides to help consumers identify the fakes.

http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html

The security and privacy risks of counterfeit devices such as webcams can be high for users. The software in these products is not only of poor or defective quality initially, but the user will also get no security updates or support afterwards, making them exposed to cyber risks.

3.1.5. Personal computers and tablets

The popularity of certain types of computers and tablets have resulted in widespread counterfeiting. In some cases, these products were actually "decoys" and did not even contain a circuit board. http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/. For the ones that do include electronics, these products have in some cases been pre-installed with malware included in counterfeited versions of operating systems.

http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware

3.1.6. Electronic children's toys

In 2014, most children's toys contain electronics of some sort. From fake games consoles and hand-held gaming devices, through to baby toys, all have the potential to cause physical harm to children. Examples of safety risks include non-earthed power supplies which pose an electrocution risk.

http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys

4. Intellectual property rights (IPRs) conventions

A number of international agreements and conventions set out substantive standards for the protection of IPRs under national laws, as well as permissible exceptions and limitations, and define the necessary procedures that national governments undertake to make available to enable the right holder to take effective action against any infringing acts.

4.1. The Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works

The World Intellectual Property Organization (WIPO) administers multilateral treaties concerning intellectual property. The fundamental treaties are the Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works.

The Paris Convention was concluded in 1883 and has been subsequently revised on a number of occasions. Its aim is to protect "patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations of origin, and the repression of unfair competition" [8]. As regards counterfeiting, this convention requires contracting states to take measures against "direct or indirect use of a false indication of the source of the goods or the identity of the producer, manufacturer or merchant".

4.2. World Trade Organization (WTO) Trade-Related Aspects of Intellectual Property Rights (TRIPS)

The World Trade Organization (WTO) administers the TRIPS Agreement which sets minimum standards to be applied by all WTO Members both with respect to the substantive protection and the enforcement of IPRs. The TRIPS Agreement thus introduces for the first time a comprehensive set of enforcement provisions into a multilateral agreement. Any disputes among WTO Members in this regard are to be settled under the WTO's Dispute Settlement Understanding.

TRIPS provisions on enforcement have two basic objectives, i.e. to make effective means of enforcement available to right holders and to ensure that enforcement procedures are balanced and proportionate and do not impede legitimate trade. They are divided into five sections. The first section lays down general obligations that all enforcement procedures must meet. These are notably aimed at ensuring their effectiveness and that certain basic principles of due process are met. The following sections deal with civil and administrative procedures and remedies, provisional measures, special requirements related to border measures and criminal procedures.

The Agreement makes a distinction between infringing activities in general, in respect of which civil or administrative procedures and remedies must be available, and counterfeiting and piracy – the more blatant and egregious forms of infringing activity – in respect of which certain additional procedures and remedies are mandatory, namely border measures and criminal procedures. For this purpose, counterfeit goods are in essence defined as goods involving slavish copying of trademarks, and pirated goods as goods which violate a reproduction right under copyright or a related right.

In detail, the obligations of WTO Members are as follows:

a) **Civil and administrative procedures**: The right holder must be able to initiate civil, judicial or, on an optional basis, administrative procedures against an IPR infringer. Those procedures must be fair and equitable. Certain rules on evidence are established. Furthermore, Members are required to provide judicial authorities with the authority to award three types of remedies: injunctions, damages and other remedies. As part of the safeguards against abuse, the obligations also extend to the indemnification of the defendant where enforcement procedures have been abused by the right holder.

b) **Provisional measures**: Temporary injunctions constitute an important tool pending the solution of a dispute at a trial. Therefore, judicial authorities must have the authority to order prompt and effective provisional measures to take action against alleged infringements. Those measures aim to prevent an IPR infringement from occurring and to preserve relevant evidence concerning the alleged infringement. Like in other sections on enforcement, certain procedural requirements and safeguards against abuse are provided for.

c) **Border measures**: Enable the right holder to obtain the co-operation of customs administrations to intercept infringing goods at the border and to prevent the release of such

goods into circulation. They are mandatory for counterfeit trademark and pirated copyright goods, while Members may also make them available for infringement of other IPRs, infringing goods destined for exportation, goods in transit, de minimis imports and parallel imports. Border measures are subject to certain procedural requirements and safeguards against abuse, similar to those applying to provisional measures. As regards remedies, the competent authorities must be empowered to order the destruction or disposal outside the channels of commerce of infringing goods.

d) **Criminal procedures**: These must be put in place to address cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Their application to other cases of IPR infringement is optional. In terms of remedies, the agreement stipulates that sanctions must include imprisonment and/or monetary fines, and, in appropriate cases, also seizure, forfeiture and destruction of the infringing goods and of materials and equipment used to produce them.

Least developed country WTO Members currently benefit from transitional arrangements that exempt them from the obligation to apply the protection and enforcement standards set by the TRIPS Agreement in general until July 2021, as well as to comply with the provisions regarding the protection and enforcement of patents and undisclosed data in the pharmaceutical sector until January 2016. Among others, the objective is to enable them to create a viable technological basis.

5. IPR enforcement

Although international treaties concerning the protection of intellectual property rights have been in place for well over a century, it is only recently that enforcement has been addressed in international forums. This is due to foundations provided by the TRIPS Agreement and also to the growing socio-economic impacts of IPR infringements. IPR enforcement is now on the agendas of many international organizations, such as the WIPO, the World Customs Organization (WCO) and Interpol, in the European Union and in many nations.

5.1. World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO) established an Advisory Committee on Enforcement (ACE) in 2002 with the aims of co-ordination with other international organizations and the private sector to combat counterfeiting and piracy. It provides training programmes and technical assistance.

WIPO is also collaborating with the United Nations Environment Programme (UNEP) and other organizations such as the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) to raise awareness of the challenge of recycling and disposal of the growing volumes of counterfeit products.

http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx

http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods

5.2. World Trade Organization – Council for TRIPS

The Council for TRIPS is one of the three sectoral Councils operating under the WTO's General Council. It is responsible for the administration of the TRIPS Agreement and, in particular, for monitoring the operation of the Agreement and Members' compliance with their obligations under the TRIPS Agreement. The Council has formal meetings in Geneva three times per year, as well as informal meetings as required. The meetings constitute a forum for discussion and consultation on any matter related to the TRIPS Agreement, as well as for clarifying or interpreting provisions of the

Agreement. IPR enforcement has been discussed on an ad hoc basis in the TRIPS Council on several occasions, most lately 2012.

5.3. UN Office of Drugs and Crime (UNODC)

UNODC is the custodian of the United Nations Convention against Transnational Organized Crime that is the worldwide platform for co-operation in tackling all forms of organized crime. Currently, 167 countries are party to the Convention and have committed themselves to fighting organized crime through collaboration and ensuring that domestic laws are suitably structured.

UNODC holds biannual meetings of the Parties to the United Nations Convention against Transnational Organized Crime. These meetings bring together governments from across the world to promote and review the implementation of the Convention in order to ensure better approaches to tackling transnational organized crime. The last meeting was in October 2012.

The UN Office of Drugs and Crime has focused on the linkage between the trade in counterfeit goods and transnational organized crime http://www.unodc.org/counterfeit/. UNODC launched the "Counterfeit: Don't Buy into Organized Crime" campaign in January 2014 to raise consumer awareness of the USD 250 billion a year of illicit trafficking of counterfeit goods. The campaign – "Counterfeit: Don't buy into organized crime" - informs consumers that buying counterfeit goods could be funding organized criminal groups, puts consumer health and safety at risk and contributes to other ethical and environmental concerns.

UNODC also works to counter the flow of illicit goods such as counterfeit products and drugs by means of technical assistance programmes. UNODC and the World Customs Organization launched the Container Control Programme (CCP) in 2006. The programme has resulted in the seizure of 487 containers of fraudulent and contraband goods alongside a further 195 containers of drugs.

https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html

https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html

5.4. World Customs Organization (WCO)

WCO is an intergovernmental organization comprised of 179 Customs administrations that provides leadership, guidance and support to its Members to secure and facilitate legitimate trade, realize revenues, protect society and build capacity. As Customs administrations are responsible for protecting national borders from the illegal flow of counterfeit and pirated goods, WCO leads discussions on global efforts to fight such crimes. This entails bolstering efforts to combat counterfeiting and piracy by improving enforcement methods and promoting the exchange of information between Customs as well as between Customs and the private sector.

Capturing the attention of Customs officers and industries worldwide and ensuring their vigilance with regards to counterfeit products is at the heart of the WCO IPR and Health and Safety Programme. With the protection of consumer health and safety as a key priority, WCO is extremely active in delivering extensive capacity building actions and developing various enforcement tools.

Conscious of the importance of collaborating with the private sector, WCO works very closely with industry members and associations in order to assess their needs and difficulties when tackling this phenomenon. WCO regularly invites rights holders to participate in its various anti-counterfeiting activities, such as field operations, regional or national seminars and has developed an online tool, interface public-members (IPM), to arm Customs officers with the means to detect counterfeit and pirated products and to communicate with economic players in real time.

Large scale Operations are a vital part of the WCO anti-counterfeit initiatives in which multiple numbers of Customs administrations simultaneously raise their level of enforcement on counterfeit items to quantify and qualify the impact of global counterfeiting activities. In 2013 alone, over 1.1 billion counterfeit items were intercepted by Customs Administrations in an Operation in the African region and an Operation in the Latin American region.

WCO has also developed a global online detection tool, IPM, aimed at frontline Customs officers to facilitate the distinction between genuine products and their fake reproductions. Since its launch in 2010, IPM has become a real communication hub between Customs officers on the ground and the private sector by allowing them to exchange crucial information in real time in order to intercept counterfeit goods.

With the recent launch of IPM mobile, field Customs officers can now access IPM via their mobile devices and retrieve all relevant information contained in the database. This new version offers the possibility to use mobile devices to scan industry standard GS1 barcodes found on millions of products, enabling to search the products database in a more time-efficient manner. Furthermore, scanning the barcodes will enable automatic connection to any authentication services linked to the product controlled. This new feature is known as IPM Connected - a global network of security features providers (SFPs) interfaced with IPM. With this growing network of SFP, the number of rights holders to join IPM is also seeing a boost with over 700 brands currently in the system, covering a wide-range of industry sectors from pharmaceutical, foodstuff, pesticides, to fast-moving goods and luxury items [63].

5.5. European Union

At the level of the EU a series of public consultations have been carried out since 2011 regarding Directive 2004/48/EC on the enforcement of intellectual property rights. The previous public consultation on the efficiency of IP civil enforcement systems in EU Member States closed in March 2013. The European Commission published a summary of the replies in July 2013.

The Commission adopted on 1st July a Communication "Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan" – COM (2014)932.

The ten actions listed in the Action Plan focus on commercial scale infringements (the so-called "follow the money" approach) and aim at improving prevention, increasing cross-border cooperation between Member States and prioritising IP enforcement policy on the basis of objective data.

The European Observatory on Counterfeiting and Piracy was created in 2009 as part of the European Commission. Regulation No 386/2012 of the European Parliament and of the Council renamed it the European Observatory on Infringements of Intellectual Property Rights and fully entrusted it to the Office of Harmonisation of the Internal Market on 5 June 2012. The Observatory serves as a platform for private and public actors allowing them to share best practices and experiences on IPR enforcement, to raise public awareness and to collaborate on collecting and monitoring data.

The European Commission promoted at EU level a Memorandum of Understanding on the sale of counterfeit goods via the Internet (MoU). It was signed in May 2011 between internet platforms, brand owners and trade associations. The MoU established a code of practice in the fight against the sale of counterfeit goods over the internet and enhanced collaboration between its signatories.

Customs

The Council Regulation No 1383/2003 of 22 July 2003 on customs actions against goods suspected of infringing certain intellectual property rights was replaced by Regulation 608/2013.

5.6. Interpol

Interpol, the international police organization with 190 member countries, started an Intellectual Property Crime Action Group in 2002. This group supports regional and global operations to seize counterfeit goods, organizes training courses through the International IP Crime Investigators College (IIPCIC), and has created a database on international intellectual property crime.

5.7. United Nations Economic Commission for Europe (UNECE)

The UNECE Working Party on Regulatory Cooperation and Standardisation Policies (WP.6) has established an advisory group on market surveillance (MARS group) that aims to encourage member states to coordinate their efforts to contain the problem of counterfeit goods. They have produced Recommendation M. on the "Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods" [8].

5.8. National Initiatives (a few examples)

5.8.1. France

The CNAC (*Comité National Anti Contrefaçon*) is the French national anti-counterfeiting committee http://www.industrie.gouv.fr/enjeux/pi/cnac.php
and the INPI (*Institut National pour la Propriété Industrielle*) is the national institute for industrial property http://www.inpi.fr/fr/accueil.html . The finance ministry (*Ministère de l'économie et des finances*) is also involved in anti-counterfeiting activities. http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet

5.8.2. UK Intellectual Property Office

The UK government Intellectual Property Office created the intellectual property (IP) Crime Group in 2004. It produces an annual IP crime report and has also published a supply chain toolkit [9]. The UK has also a Minister for Intellectual Property.

5.8.3. Kenya Anti-Counterfeit Agency

The Kenya Parliament passed the Anti-Counterfeit Act (No.13) in 2008. This act prohibits trade in counterfeit goods and also established the Anti-Counterfeit Agency [10].

5.8.4. US - China Joint Commission on Commerce and Trade

The US and China have established a Joint Commission on Commerce and Trade. At their 24th meeting in December 2013, China's National Leading Group on Combating IPR infringement and the Manufacture and Sales of Counterfeit and Substandard Goods committed to adopting an action plan in 2014 that includes raising public awareness, requirements for compliance with all laws and regulations concerning IPR protection and enforcement actions. www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet

6. Industry anti-counterfeiting forums

Businesses have reacted to the problem of counterfeiting by establishing forums to represent their interests. These forums provide information about the extent of the problem, suggest ways of mitigating the effects of counterfeiting and lobby governments and international organizations to take action to combat counterfeiting.

6.1. International Chamber of Commerce (ICC)

ICC represents the world's business organizations. Thousands of companies and associations in about 120 countries are members. It acts on behalf of business in making representations to governments and intergovernmental organizations. ICC was founded in 1919 and itself established the ICC International Court of Arbitration in 1923.

ICC created a Counterfeiting Intelligence Bureau in 1985 and, more recently, the Business Action to Stop Counterfeiting and Piracy (BASCAP) group.

The ICC Counterfeiting Intelligence Bureau maintains a case study database and also provides investigative services.

BASCAP continued the study of the economic and social impacts of counterfeiting and piracy begun by OECD [45] and has developed an information clearing house which provides information by country [11] and sector [12] and also brand protection [13] and worldwide contact directories [14].

ICC also publishes an Intellectual Property Roadmap [15].

6.2. International Anti-Counterfeiting Coalition (IACC)

IACC [16] was founded in 1979 and has members from all branches of industry. It aims to combat counterfeiting and piracy by promoting anti-counterfeiting regulations.

6.3. Mobile Manufacturers Forum (MMF)

The Mobile Manufacturers Forum maintains a website (spotafakephone.com) that provides information on counterfeit mobiles and batteries.

6.4. Association of Service and Computer Dealers International and North American Association of Telecommunications Dealers (AscdiNatd)

The AscdiNatd has developed an anti-counterfeit program that includes an anti-counterfeit policy for adoption by member companies and counterfeit information resources, including information from HP and Cisco [17].

6.5. Alliance for Gray Market and Counterfeit Abatement (AGMA)

AGMA was formed in 2001 by 3Com, Cisco Systems, Hewlett-Packard, Nortel and Xerox with the aim of combating trade in counterfeit high-technology products.

6.6. British Electrotechnical and Allied Manufacturers Association (BEAMA) Anti-counterfeit Working Group

BEAMA is the independent expert knowledge base and forum for the electrotechnical industry for the UK and across Europe. It represents over 300 manufacturing companies in the electrotechnical sector, and it has significant influence internationally as well as in the UK's political, standardization and commercial policy.

The BEAMA Anti-Counterfeiting Working Group (ACWG) was formed in 2000. Its objective is to take action against counterfeiters manufacturing counterfeit electrical installation products, and the traders who distribute them into many international markets, including those in Europe, the Middle East and Africa. As well as BEAMA members, the WG comprising many of the leading industry associations from the installer, distributor, test and certification and law enforcement sectors. It has achieved global recognition for its proactive work and receives co-operation from trade associations and law enforcement bodies around the world.

A database of counterfeiters for use by the electrical installation industry has been created, which is passed to authorities worldwide for them to follow up in the local markets.

The Working Groups' activities are publicized through trade magazine articles, presentations, participation in conferences and the production of guides and posters to raise awareness of this rapidly growing, potentially damaging threat to consumer safety and business integrity.

This Working Group is responsible for managing anti-counterfeiting action projects, collecting and disseminating information on IPR issues, and responding to government and others on behalf of the association. It also offers advice and information to any company or association which has a problem with IPR issues.

Current activities include projects in China, UAE, UK, Nigeria and Iraq, plus comprehensive web and port watch programmes.

In the UK, BEAMA are working with many of the leading industry bodies to raise awareness and fight counterfeit and non-compliant products – the industry portal www.counterfeit-kills.co.uk has been launched specifically for this purpose.

6.7. UKEA (United Kingdom Electronics Alliance)

UKEA is a consortium of UK trading associations representing the electronics sector. It aims to coordinate the discussion of issues within the sector and communicate with the government. UKEA has established an Anti-Counterfeiting Forum [18] that publishes information on the problem of counterfeit electronic components, potential solution providers and best practices.

6.8. Anti-Counterfeiting Group (ACG)

ACG is a UK trade association that was created in 1980 with members mainly in the automotive industry but now represents most sectors of industry.

6.9. UNIFAB - *Union des Fabricants*

The *Union des Fabricants* is a French organization dedicated to combating counterfeiting by increasing public awareness (by opening a Museum of Counterfeiting in addition to other activities), providing information to businesses and lobbying. http://www.unifab.com/en/

6.10. International Electronics Manufacturing Initiative (iNEMI)

The iNEMI has defined a project on "Counterfeit Components – Assessment Methodology and Metric Development".
http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf

7. Measures to combat counterfeit equipment

7.1. Introduction

Counterfeiting equipment can be combated by marking products in some way so that they can be authenticated by strictly controlling the product life cycles. Labels that are difficult to forge can be attached to products and serial numbers assigned which can be used to authenticate that the item is genuine (by accessing a database, for example).

Individual items may be assigned unique identifiers. An example of a system that is used to combat counterfeiting is mPedigree which is used to counter pharmaceutical counterfeiting in Africa. This system allows consumers to check whether medicines are genuine or counterfeit and potentially dangerous by sending a (free) short message service (SMS) to a registry of pharmaceutical products.

Strict control of supply chains, and possibly of complete product life cycles, is required with testing, evaluation and certification as necessary to ensure the security of the product and that appropriate quality is maintained. In addition, customs officials need to be given the tools to identify counterfeit products, and market surveillance mechanisms may be employed.

Identifiers can be made on an object in clear text or can be encoded on an "identification (ID) tag" such as a barcode, a radio frequency identification (RFID) tag, smartcard or an infrared tag so that they can be read automatically. Three levels can be distinguished in the identification of an object. First, there is a pure identifier level at which objects are uniquely identified, for example, by an electronic product code (EPC). The second level is an encoding level as the pure identifiers can be encoded in different formats, and finally there is a physical realization, when the encoded identity is written onto an RFID tag, for example.

To ensure that identifiers are globally unique for specific applications, they must be managed in an organized fashion, with some form of allocation procedure. For example, the GSM Association (GSMA) manages the international mobile equipment identities (IMEIs) for the global system for mobile communications (GSM), the universal mobile telecommunications system (UMTS) and the long-term evolution (LTE) devices; the Telecommunications Industry Association allocates the mobile equipment identifiers (MEIDs) for the code division multiple access (CDMA) devices, and GS1 manages barcode identifiers. ISO manages a number of identifier domains and also acts as a top-level authority incorporating the identifier schemes of other organizations such as GS1.

Another example is that of the marking of equipment to indicate that it has been approved to be marketed within a country. For example, Anatel requires mobile phone chargers and batteries to carry a secured label defined by their Resolution 481/2007[2]. See Figure 1.

Figure 1 — Example of Anatel's required secured label defined by their Resolution 481/2007

This approach has been used in the telecommunication equipment industry for many years and was successfully implemented by some countries/regions[3] (e.g. FCC[4], Anatel[5], EU[6]).

2 https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=

3 By usage of some conformance assessment system, that may require certification, declaration of conformity and/or benefiting from the usage of Mutual Recognition Agreements (MRAs).

Customs officials need to be able to identify counterfeit products and market surveillance and other enforcement measures which may be employed. In addition, importers with a track record of ignoring import controls can be identified and put on a special list. When shipments of ICT equipment are being imported by rogue importers, regulatory authorities can be notified so that a decision can be made to carry out inspections, and enforcement should then be warranted. See Figure 2.

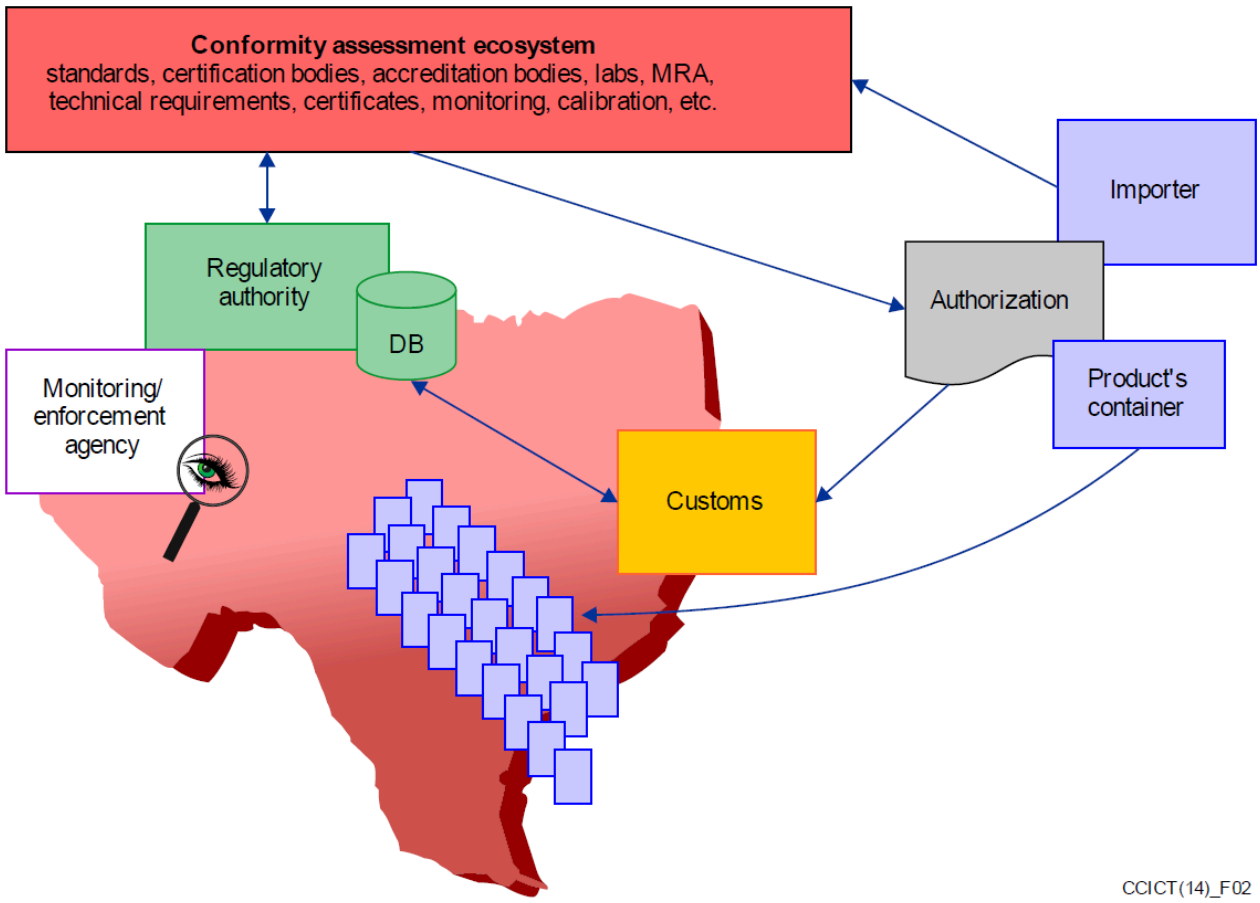

Figure 2 — Conformity assessment ecosystem

It is to be noted that counterfeit products could in fact conform with specified requirements, interoperate with genuine products, and hence pass the conformance and interoperability test. As such, product evaluation by trademark holder may be required to accurately identify counterfeit products and distinguish them from genuine products.

The ICT sector is marked by a large presence of international competitors that promote constant innovation. While this is a desirable condition, the market is, at the same time, exposed to manufacturers/vendors that are not committed to following established international, regional or national rules.

The problem of asymmetric information is more marked in developing countries, where there is little or no development of technologies and conformity assessment procedures. The typical problems commonly faced when managing a conformity assessment system are the lack of trusted and traceable

4 https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P

5 http://www.anatel.gov.br/grandeseventos/en/frequently-asked-questions-faqs

6 http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en

information, as in the following cases: i) identification of the origin or the juridically responsible agent for the products; ii) manufacturing plant sites; iii) certification bodies; and iv) qualified laboratories with legitimated accreditation certificate. In some cases, importers without any technical knowledge and capability to provide assistance can represent foreign companies that have outsourced their engineering and manufacturing units displaced in other countries (e.g. outsourcing schemes). Although such processes may represent savings in the production process, quality and accountability in the manufacturing telecommunication/ICT equipment are weakened.

One could further contend that vested interest, greed, consumer demand, lack of standards and/or poor enforcement are conducive to low-quality equipment. In some cases the same brand or model, because of the lack of a proper conformance process in a specific target market, is fitted and sold with different electronic components, some good, some bad, and shipped to selected destinations according to their relative laxity on quality. A procedure known as tropicalização (Portuguese for tropicalization) springs to mind as an example of such tampering with equipment meant for sales south of the Equator. See Figure 3.

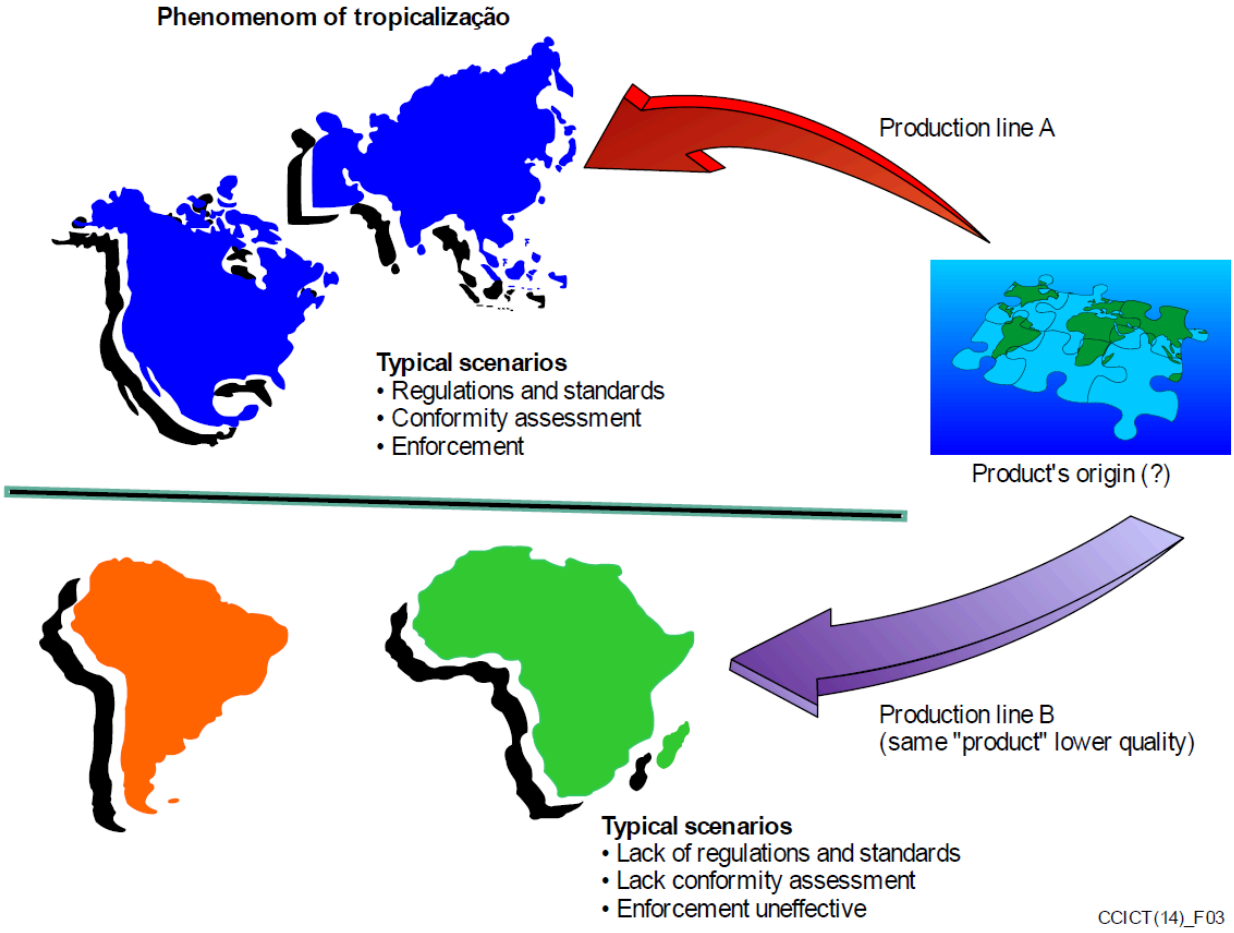

Figure 3 — Procedure known as tropicalização (Portuguese for tropicalization)

7.2. Abuse of identifiers and type approval logos

All identifiers that are created by authentic manufacturers of goods can and are abused 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. 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 from genuine ones, even before considering the product itself.

7.3. International mobile equipment identity (IMEI)

As already noted, mobile phones have been a particularly attractive target for counterfeiters and, in response, the Mobile Manufacturers Forum (MMF) has created a website giving information for consumers on how to spot counterfeit phones and batteries. http://spotafakephone.com. They advise that one should get to know the appearance, capabilities, availability and price of the genuine articles and also check the international mobile equipment identity (IMEI) number. IMEI is a unique identifier for each mobile phone and counterfeits often do not have an IMEI or have a fake number. One problem for manufacturers, network operators and the authorities is that counterfeiters have evolved their manufacturing in such a way that they sometimes steal legitimate ranges from existing manufacturers as part of their counterfeiting strategy. This can be used as one method to evade systems for checking IMEIs.

The allocation of IMEIs is managed by GSMA so as to ensure that they are unique. The allocation scheme is hierarchical with the GSMA assigning 2-digit identifiers to Reporting Bodies that then allocate IMEI and the serial number of the equipment. The Reporting Bodies currently authorized to allocate IMEIs are the CTIA – The Wireless Association, BABT (British Approvals Board for Telecommunications), TAF (Telecommunications Terminal Testing and Approval Forum) (China), and MSAI (Mobile Standards Alliance of India).

The format of IMEI valid from 1 January 2003 is to be found in Table 1, as follows [51]:

Table 1 — IMEI format

Type allocation code (TAC)	Serial number	Check digit
NNXXXX YY	ZZZZZZ	A
TAC	Type allocation code, formerly known as type approval code.	
NN	Reporting Body identifier.	
XXXXYY	Mobile equipment (ME) type identifier defined by Reporting Body.	
ZZZZZZ	Allocated by the Reporting Body but assigned per ME by the manufacturer.	
A	Check digit, defined as a function of all other IMEI digits.	

GSMA registers additional information such as the manufacturer name and model number and the technical capabilities, such as the frequency bands supported and the power class, for each device identified by its IMEI.

GSMA maintains the IMEI DB (IMEI Database) [24], previously known as the central equipment identity register (CEIR). The IMEI DB contains a "white list" of equipment that is considered to be suitable for use worldwide, and a "black list" of IMEIs related to devices that are not considered suitable for use due to their being lost, stolen, or faulty and posing a threat to network integrity. It should be noted that the IMEI DB white list is a list of TACs rather than full IMEIs and the data is freely available to eligible parties including national regulators, law enforcement agencies and customs agencies. In addition to the IMEI DB, individual network operators may implement their own equipment identity registers (EIR), to which they can download the "white list", and these allow operators to control which devices can access their networks.

http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/

The primary use of the IMEI DB is for operators to be able to identify the devices, and their characteristics, being used on their networks and for the blocking of stolen handsets. The IMEI DB can also be used to detect counterfeit devices, which helps prevent device laundering, deter crime and support prosecutions.

There have been problems, however, with the implementation of IMEI. Cases have been reported of equipment with no IMEI, with an all-zero IMEI, duplicate IMEIs and IMEIs allocated by unauthorized organizations. Some of these devices with invalid or non-unique IMEIs are counterfeits but others are genuine but not in compliance with the GSMA IMEI allocation procedure due to misunderstandings on the part of the manufacturers. For example, there were estimated to be 30 million GSM handsets in India with no IMEI, and MSAI was authorized by GSMA to offer a temporary amnesty programme involving the implantation of genuine IMEIs (genuine IMEI implant (GII) programme) in order to be able to uniquely identify each device.

As an example of duplicate IMEIs, 6,500 handsets with the IMEI 135790246811220 have been detected in Australia. As for unregistered IMEIs, a network operator in Uganda reported that the number of TACs on its network that are not registered in the IMEI DB is greater than the number allocated by GSMA and that are registered in the IMEI DB.

There is therefore good reason to ensure that the use of IMEI is mandated and that IMEIs are allocated in accordance with the GSMA process. The IMEI DB is one tool for detecting counterfeit mobiles and, to give one example, Kenya denied access to mobiles with invalid IMEIs from the end of September 2012 as there were estimated to be 2.3 million subscribers using fake handsets. Further information on these examples and other cases in which IMEIs have been used as the basis of identifying counterfeit mobiles is provided in Annex A. As several national efforts aimed at addressing the issue of counterfeit mobile devices rely on the use of IMEI, it is essential that the IMEI allocation procedure and database is secure and reliable, and that IMEI is securely encoded within the devices.

One option is that operators be required to block devices with duplicate and invalid IMEI's as these devices must be authenticated on a network in order to work. Blocking these devices when first connected is probably the most effective tool to address the problem at this time.

However, there are several constraints to blocking IMEIs. One is that GSMA does not maintain a full IMEI white list but rather a white list of TAC codes only. Secondly, IMEIs from legitimate devices have been cloned onto counterfeit and substandard devices complicating the blocking process, and finally, any blocking solution must prevent or prohibit other cloned IMEIs from being copied to the devices in question.

While there are challenges with blocking, solutions are available on the market. At the same time, it is important to avoid a patchwork of unique national solutions that will simply shift the problem across national borders. Given that IMEIs are allocated by GSMA and that IMEI DB is maintained by GSMA, it would seem logical that they should be involved in some way in national initiatives in order to utilize the full suite of available lists and other technical measures.

However, considering that the estimated number of counterfeit devices is simply enormous, just blocking operational terminals would cause heavy and unexpected impacts to networks and end users. This fact cannot be ignored.

In this regard, it is important to take into consideration the fact that in developing countries, with low social and economic conditions, mobile phones are the main gateway to communicate and participate

in the information society[7]. Sadly, this happens using a considerable number of cheaper counterfeit devices.

For this reason, the entire society has to be prepared for such a change. Best approaches must be studied, considered and planned. For instance, the motives (of safety risks, lower quality of service and consequently increase in complaints, interference hazards, and IPR infringement, etc.) for not allowing counterfeit devices must be clearly explained to consumers.

In this sense, if regulators and governments choose to put in force terminal blocking actions, it is important to adopt transition policies, 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 since the estimated life cycle of a mobile terminal is 18 months[8].

7.4. Unique identifiers

Electronic product codes (EPCs) were first developed by the Massachusetts Institute of Technology Auto-ID Centre that was created in 1999 and are today managed by EPCglobal, a subsidiary of GS1 which has defined the most widely used specifications for global supply chain systems. The International Organization for Standardization (ISO) and the Ubiquitous ID Centre (Japan) have also defined identifiers for a number of applications.

GS1 defines nine "identification keys" for the identification of items, locations, shipping containers, assets, services, document types, shipments and consignments, as follows:

– GTIN - global trade item number
– GLN - global location number
– SSCC – serial shipping container code
– GRAI – global returnable asset identifier
– GIAI – global individual asset identifier
– GSRN – global service relation number
– GDTI – global document type identifier
– GSIN – global shipment identification number
– GINC – global identification number for consignment

GTIN is used to identify categories of objects whereas GLN, SSCC, GIAI and GSRN identify individual objects; GRAI and GDTI can be used to identify either categories of objects or individual items depending upon the absence or presence of a serial number. GINC and GSIN identify logical groupings rather physical objects. These identification keys are intended for realization using barcodes. There is a correspondence between these codes and EPCs defined by EPCglobal for use with RFID. GTIN is extended in the EPC scheme by the addition of a serial number so as to uniquely identify an object. The other keys that are used to identify individual objects have a direct EPC equivalent. The following EPCs are defined [46]:

– General identifier (GID)
  • urn:epc:id:gid:*ManagerNumber.ObjectClass.SerialNumber*
– Serialized global trade item number (SGTIN)
  • urn:epc:id:sgtin:*CompanyPrefix.ItemReference.SerialNumber*
– Serial shipping container code (SSCC)
  • urn:epc:id:sscc:*CompanyPrefix.SerialReference*

---

[7] ITU's m-Powering Development Initiative: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx

[8] http://www3.epa.gov/epawaste/education/quest/pdfs/unit1/chap2/u1-2_product-life.pdf : "Cell phones are only used for an average of 18 months before being replaced—even though they can function for much, much longer."

– Global location number with or without extension (SGLN)
  • urn:epc:id:sgln:*CompanyPrefix.LocationReference.Extension*
– Global returnable asset identifier (GRAI)
  • urn:epc:id:grai:*CompanyPrefix.AssetType.SerialNumber*
– Global individual asset identifier (GIAI)
  • urn:epc:id:giai:*CompanyPrefix.IndividulAssetReference*
– Global document type identifier (GDTI)
  • urn:epc:id:gdti:*CompanyPrefix.DocumentType.SerialNumber*
– Global service relation number (GSRN)
  • urn:epc:id:gsrn:*CompanyPrefix.ServiceReference*
– US Department of Defense (DoD)
  • urn:epc:id:usdod:*CAGEOrDODAAC.SerialNumber*
– Aerospace and defence identifier (ADI)
  • urn:epc:id:adi:*CAGEOrDODAAC.OriginalPartNumber.Serial*

ISO/IEC 15459 [ISO/IEC 15459] defines unique identifiers for supply chain tracking that can be represented in automatic identification and data capture (AIDC) media such as barcodes and RFID.

Parts 1, 4, 5, 6 and 8 of ISO/IEC 15459 specify the unique string of characters to identify transport units, individual items, returnable transport units, product groupings and transport units, respectively. In each case, the unique identifier is structured into classes so as to facilitate the efficient management of the identifiers for that class of object.

Part 2 specifies the procedural requirements for allocating unique identifiers for item management applications and describes the obligations of the Registration Authority and Issuing Agencies. These procedures do not apply to those items for which ISO has already designated Maintenance Agencies or Registration Authorities to provide identification schemes. It therefore does not apply to:
– freight containers, as their unique coding is specified in ISO 6346 [ISO 6346:1995];
– vehicles, as their unique identification is specified in ISO 3779 [ISO 3779:2009];
– car radios, because their unique identification is specified in ISO 10486 [ISO 10486:1992]; and
– ISBN [ISO 2108:2005] and ISSN [ISO 3297:2007] schemes.

Part 3 specifies the common rules that apply to unique identifiers for item management that are required to ensure full compatibility across classes of unique identifiers.

ISO Technical Committee 246 is chartered to produce standard anti-counterfeiting tools. This committee is developing a standard on the performance criteria for authentication solutions for combating the production of counterfeit goods [ISO 12931:2012].

In addition to ISO and EPCglobal, the Ubiquitous ID Centre in Japan has defined a generic identifier called an "ucode" [26], which is not only intended to identify physical objects but also may be used to identify places and digital information, see Table 2. Basic ucodes are 128 bits in length (but can be extended in multiples of 128 bits) and may embed other identifiers such as ISBNs, Internet protocol (IP) addresses or ITU-T E.164 telephone numbers [ITU-T E.164]. The ucode is basically a number that needs to be assigned a meaning in a relational database. Any individual or organization can obtain ucodes from the Ubiquitous ID Centre, which acts as the registration authority for these numbers.

Table 2 — Ucode format

Version (4 bits)	TLDc (16 bits)	cc (4 bits)	SLDc (variable)	ic (variable)
TLDc		top level domain code (assigned by the Ubiquitous ID Centre)		

cc	class code (indicating the boundary between the SLDc and ic)
SLDc	second level domain code
ic	identification code for individual objects

ITU-T is working on systems for accessing multimedia information triggered by the tag-based identification of things. As part of this work, a description of the various ID schemes that could be used for such identification is being produced. The Ubiquitous ID Centre has submitted their ucode scheme such that the ucode would be assigned an object identifier (OID) registered under the branch {joint-iso-itu-t(2) tag-based(27)} in compliance with Recommendation ITU-T X.668 [ITU-T X.668]. The ISO/IEC Unique ID scheme described earlier is assigned an object identifier under the branch {iso(1)} of the Object Identifier tree. This results in the ISO/IEC (including EPCglobal) and Ubiquitous ID Centre identifier schemes being assigned object identifiers either under the {iso} branch (ISO and EPCglobal) or {joint-iso-itu-t} branch (Ubiquitous ID Centre) and allows the coexistence of the various identification schemes that have different registration authorities. For RFID tags, the object identifier (OID) and ID would be encoded as defined in ISO/IEC 15962 [ISO/IEC 15962:2013].

NOTE – The term "object" of "object identifier" is not being used here to refer to a "thing" in general but rather it is used in accordance with the definition given in ISO/IEC 15961 [ISO/IEC 15961:2004] as: "a well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication". An object identifier unambiguously identifies such an object. Object identifiers are hierarchically organized with the roots of the tree or top 'arcs" indicating the organization that is responsible for the definition of the information. The top arcs represent ITU-T, ISO and Joint ISO - ITU-T. They are given the numeric values 0, 1 and 2, respectively. The "tag-based" arc in the joint ISO – ITU-T tree is given the numeric value 27.

Data associated with an object may be stored on a tag along with the identifier if the tag has sufficient memory. However, another possible means to find information associated with an identifier is to use an identifier resolution mechanism.

A very wide variety of services and applications for RFID can be envisaged, once it becomes possible to provide information associated with a tag identifier in different forms (text, audio or image). For example, in a museum, an identifier on a tag attached to a painting could be used to find further information on the painting and the artist. In a grocery store, an identifier on a food package could be used to check that the food is safe to eat and not one of a sample that has been found to be contaminated in some way. Identifier-triggered information access could be valuable in medicine/pharmaceuticals, agriculture, libraries, the retail trade and supply chain management. Such mechanisms could also be employed to combat counterfeiting. Recommendation ITU-T F.771 [ISO 15394:2009] describes a number of services that could be based on the use of information associated with tagged objects and the requirements for these services.

A model for accessing the information associated with a tagged object is specified in Recommendation ITU-T H.621 [ITU-T Y.4405] (see Figure 4). Within this model, a multimedia information discovery function can send the identifier obtained from an ID tag reader to an ID resolution function, thereby obtaining a pointer (such as a uniform resource locator (URL)) to the appropriate multimedia information manager. As a result, it becomes possible to access the information associated with the tag ID. As the number of identifiers is expected to be very large, the ID resolution function is likely to be distributed in a tree structure.

The ID resolution function could be based on the use of the Internet domain name system (DNS) that usually provides the Internet protocol (IP) address corresponding to a uniform resource locator (URL). The object naming service (ONS) described by EPCglobal uses DNS mechanisms to find information associated with electronic product codes.

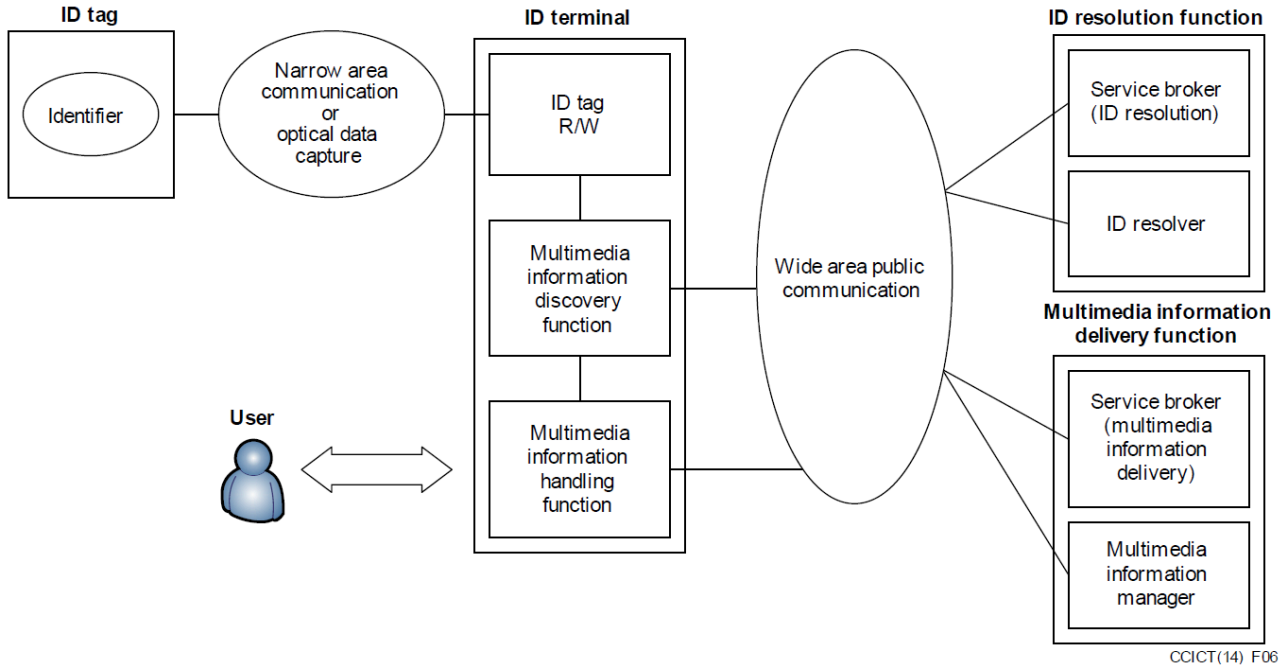

Figure 4 — Functional architecture for multimedia information access triggered by tag-based identification (Recommendation ITU-T H.621)

In addition, Recommendation ITU-T X.1255 [ITU-T X.1255] https://www.itu.int/rec/T-REC-X.1255-201309-I/en provides a framework for the discovery of identity management information that is recognized in the ITU Plenipotentiary Resolution on Combating counterfeit telecommunication/information and communication technology devices.

7.5. Automatic identification and data capture (AIDC)

7.5.1. Barcodes

Barcodes are often used to identify products. They take a variety of forms from the universal product code (UPC) barcodes that are familiar in supermarkets to matrix (2D) barcodes. They can easily be faked and copied by counterfeiters.

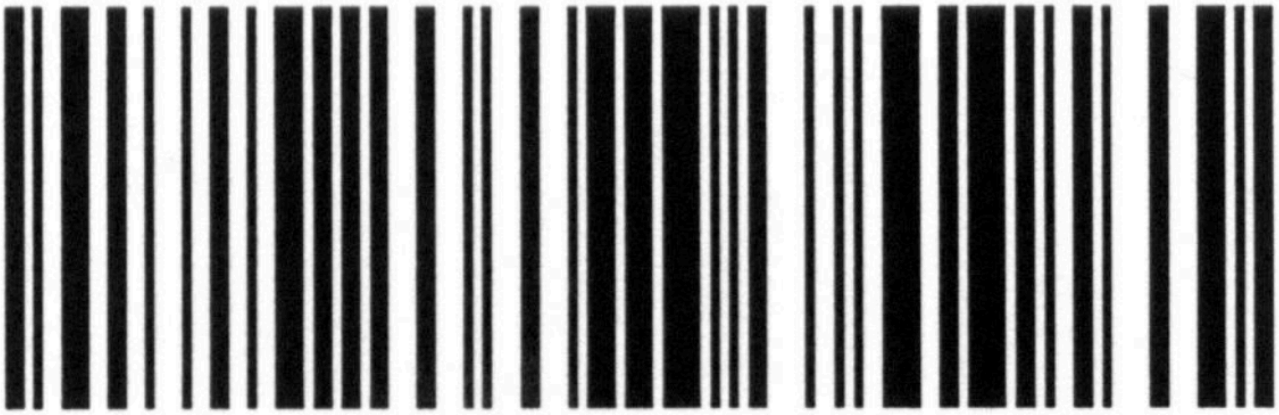

Figure 5 — Examples of linear barcodes

For examples of linear barcodes, see Figure 5:
UPC ISO/IEC 15420 [ISO/IEC 15420:2009]
Barcode Code 39 ISO/IEC 16388 [ISO/IEC 16388:2007]
Barcode Code 128 ISO/IEC 15417 [ISO/IEC 15417:2007]

Figure 6 — Examples of matrix (2-dimentional) barcodes

For examples of matrix (2-dimentional) barcodes, see Figure 6:
Codablock F ISO/IEC 15417+
PDF 417 ISO/IEC 15438 [ISO/IEC 15438:2006]
Maxicode ISO/IEC 16023 [ISO/IEC 16023:2000]
QR code ISO/IEC 18004 [ISO/IEC 18004:2006]
Data matrix ISO/IEC 16022 [ISO/IEC 16022:2006]

Barcodes can be used to encode a serial number. For example, DIN 66401 [41] defines a unique identification mark (UIM) consisting of a matrix symbol (ISO/IEC 16022 or ISO/IEC 18004) and a unique data identifier (in accordance with ANSI MH10.8.2 [36] and "+" symbol according to ANSI/HIBC 2.3 [37]). This is an application standard for marking small items in the fields of electronics and health care for example. They are especially suitable for direct marking using inkjet or laser marking and also for label printing.

The requirements for item labelling and direct product marking with linear and 2D barcodes are specified in ISO 28219 [ISO 28219:2009]. The requirements for the design of linear and 2D barcode labels for product packaging are specified in ISO 22742 [ISO 22742:2010] and those for shipping, transport and receiving labels in ISO 15394 [ISO 15394:2009].

7.5.2. RFID

RFID enables objects to be tagged and the information stored on these tags to be read using short-range wireless technology. The specifications for RFID cover the identification of objects, air interface characteristics and data communication protocols.

ISO/IEC 15963 [ISO/IEC 15963:2009] specifies how radio frequency (RF) tags are assigned unique identifiers. RF tags have an identifier allocated by the integrated circuit manufacturer – the tag ID. The tag ID (TID) may be used as the unique item identifier (UII) when the tag is attached to some item or UII may be stored in a separate part of memory on the tag. UII in this case could be an EPC as specified by EPCglobal.

Table 3 shows the ISO/IEC 15963 tag ID format.

Table 3 — ISO/IEC 15963 tag ID format

Allocation class (AC)	TID issuer registration number	Serial number
8 bits	Size defined by AC value	Size defined by AC and TID issuer value

The allocation class indicates the authority assigning the numbers – the TID issuer. Integrated-circuit card manufactures can be registered to assign unique identifiers under the ISO/IEC 7816-6 [ISO/IEC 7816-6:2004] scheme or the American National Standards Institute INCITS (International Committee for Information Technology Standards) scheme, as can the manufacturers of tags for freight containers and transport applications following the procedures of ISO 14816 [ISO 14816:2005]. EPCglobal identifiers are accommodated within the ISO/IEC 15963 scheme as the GS1 class.

The five classes of TID issuer are shown in Table 4:

Table 4 — Classes of unique TID issuers

AC value	Class	TID issuer identifier size	Serial number size	Registration authority (of TID issuer registration number)
000xxxxx	INCITS 256	See ANSI INCITS 256 [34] & 371.1 [35]	See ANSI INCITS 256 and 371.1	autoid.org
11100000	ISO/IEC 7816-6	8 bits	48 bits	APACS (UK Payments Administration)
11100001	ISO 14816	See NEN	See NEN	NEN (Netherlands
				Standardization Institute)
11100010	GS1	See ISO/IEC 18000-6 Type C [ISO/IEC 18000-6:2013] & ISO/IEC 18000-3 Mode 3 [ISO/IEC 18000-3:2010]	See ISO/IEC 18000-6 Type C & 18000-3 Mode 3	GS1
11100011	ISO/IEC 7816-6	8 bits	48 bits	APACS (includes memory size and extended TID header)
All other values	Reserved			Reserved

An early application of RFID was for the identification of animals. ISO completed a standard in 1994 that defines the structure of an RFID identification code for animals (ISO 11784 [ISO 11784:1996]). The complementary ISO 11785 [ISO 11785:1996] describes how this tag information is read.

ISO has proceeded to define a complete set of specifications for item management: ISO/IEC standards 15961 through 15963 describe the common data protocol and identifier formats applicable to the ISO/IEC 18000 series of standards [ISO/IEC 18000] that describe the air interfaces at various frequencies. Separate specifications are required for the different frequency bands because the frequency of operation determines the characteristics of the communication capability, e.g. the range of operation or whether transmission is affected by the presence of water.

ISO/IEC 29167-1 [ISO/IEC 29167-1:2014] defines the architecture for security and file management for the ISO/IEC 18000 air interface standards. Application-dependent security mechanisms are defined and a tag may support all or a subset of these. An RFID tag interrogator can access information about the security mechanisms supported by a tag as well as further information such as the encryption algorithm and key length employed.

Implementation guidelines for system designers to assess the potential threats to the security of the data on the tag and tag-to-reader communication, along with descriptions of the appropriate countermeasures to ensure tag data security, are given in ISO/IEC TR 24729-4 [ISO/IEC TR 24729-4:2009].

Supply chain applications of RFID (with parts applicable to freight containers, returnable transport items, transport units, product packaging and product tagging) are specified in ISO 17363 to 17367 [ISO 17363:2013] to [ISO 17367:2013]; ISO 18185 [ISO 18185] describes how RFID can be used to track the movements of freight containers. ISO has also produced performance and conformance test specifications.

The RFID emblem specified in ISO/IEC 29160 [ISO/IEC 29160:2012] can be used as a label on products to indicate that it has an RFID tag. See Figure 7.

Figure 7 — Example of RFID emblem specified in ISO/IEC 29160

EPCglobal is the GS1 subsidiary developing specifications for the use of electronic product codes with RFID. EPCglobal has produced a suite of standards including specifications for tag data encoding, air interface protocols, reader protocols, and information and object name services. An overview of the EPCglobal suite of standards is provided in Figure 8.

The main elements of the EPCglobal suite of standards are as follows:

– The EPC Tag Data Standard (TDS) defines a number of identification schemes and describes how this data is encoded on tags and also how it is encoded in a form suitable for use within the EPC systems network.
– A machine-readable version of the EPC data formats is given in the EPC Tag Data Translation (TDT) standard. This can be used for validating EPC identifiers and translating between various representations of the data.
– The tag protocols are RFID air interfaces. On the "Gen 2" interface, a reader sends information to a tag by modulating a radio frequency signal in the 860 – 960 MHz range. Tags are passive, in the sense that they receive energy from the signal transmitted by the reader. This air interface protocol has been included in the ISO/IEC 18000 series of specifications as Type C in Part

6. The high frequency air interface operates at 13.65 MHz. This specification is backwards compatible with ISO/IEC 15693 [ISO/IEC 15693].

- The low level reader protocol (LLRP) is used by a client to control a reader at the level of operation of the air protocol and provides an interface between application software and readers (the reader protocol (RP)).
- Readers discover clients using the procedures specified in the Discovery, Configuration and Initialisation (DCI) standard.
- The Reader Management (RM) standard is used to monitor the operating status of RFID readers. It is based on the use of the simple network management protocol (SNMP) defined by the Internet Engineering Task Force (IETF).
- The Application Layer Events (ALE) standard provides a means for clients to obtain filtered EPC data. This interface provides independence between the infrastructure components that obtain the raw EPC data, the components that process that data and the applications that make use of the data.
- The EPC Information Services (EPCIS) standard allows the sharing of EPC data within and between enterprises.
- The core business vocabulary (CBV) is intended to ensure that all parties exchanging EPCIS data will have a common understanding of the meaning of that data.
- The Object Naming Service (ONS) standard describes how the domain name system (DNS) can be used to obtain information associated with a specific EPC.
- The EPCglobal certificate profile standard describes how entities within the EPC global network can be authenticated. Use is made of the ITU-T X.509 [ITU X.509] authentication framework and the Internet public key infrastructure profiles defined in IETF RFC 3280 [IETF RFC 3280] and IETF RFC 3279 [IETF RFC 3279].
- The Pedigree standard specifies the means of handling electronic drug "pedigree" documents for use in pharmaceutical supply chain applications.

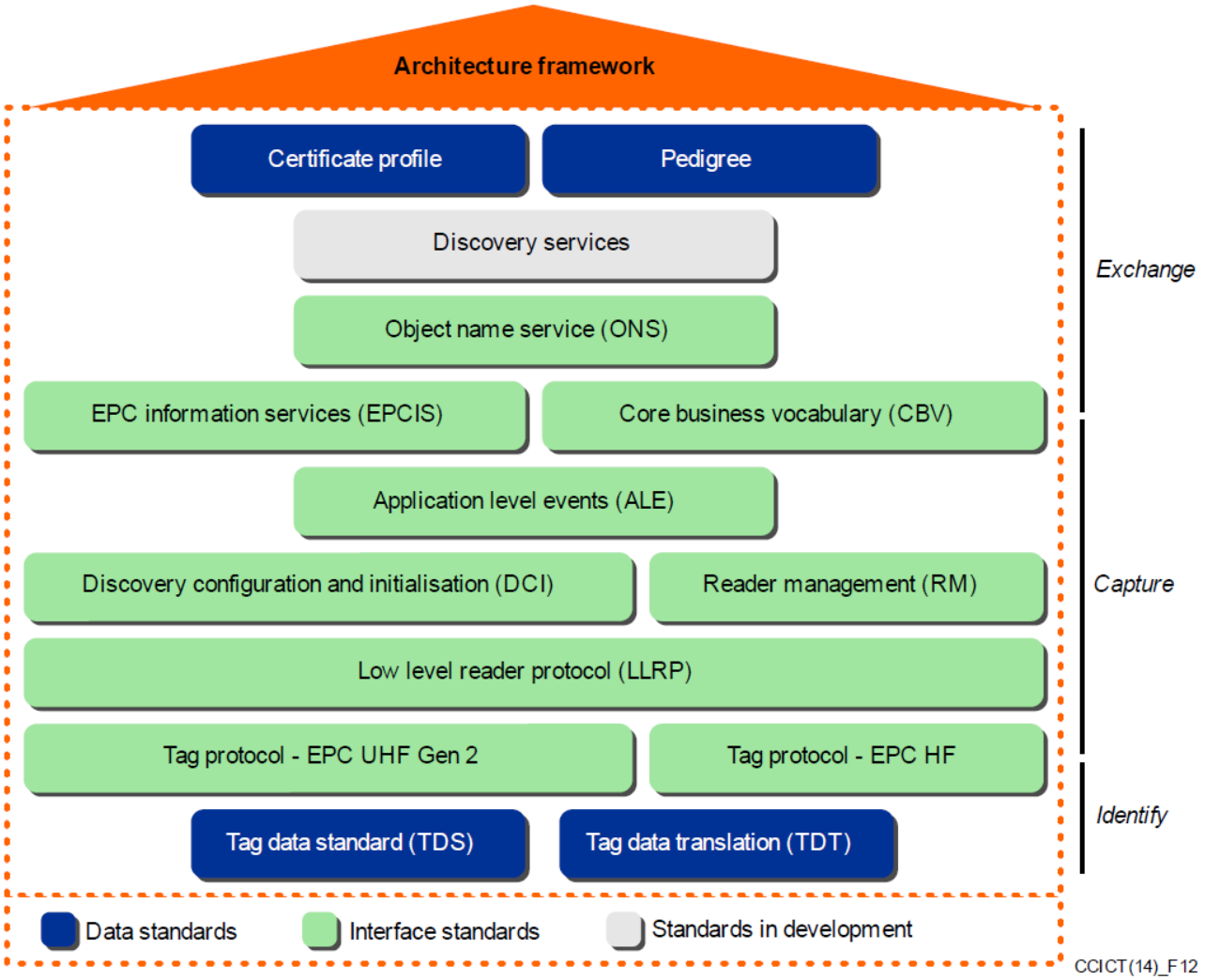

Figure 8 — EPCglobal standards overview [27]

7.6. Secure printing and hologram labels

Secure printing techniques can be used to create tamper-evident labels, and labels may also be complemented with hologram images that are difficult to forge. It should be noted, however, that such mechanisms are widely abused and copied by counterfeiters.

7.7. Supply chain management

Maintaining the security of supply chains is very important to combat counterfeiting activities. The ISO 28000 series of International Standards specify the requirements for the secure management of supply chains. These standards are applicable to organizations of any size involved in manufacturing, service, storage or transportation by air, rail, road and sea at any stage of the production or supply process. The following standards are available:

– ISO 28000:2007, *Specification for security management systems for the supply chain*. [ISO 28000:2007]
– ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance*. [ISO 28001:2007]
– ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*. [ISO 28003:2007]

– ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*. [ISO 28004-1:2007]
– ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements*. <<iso28005-2011>

ISO 28000 requires organizations to assess the security environment in which they operate and to determine if adequate security measures have been implemented. The elements of a security management system are shown in Figure 9.

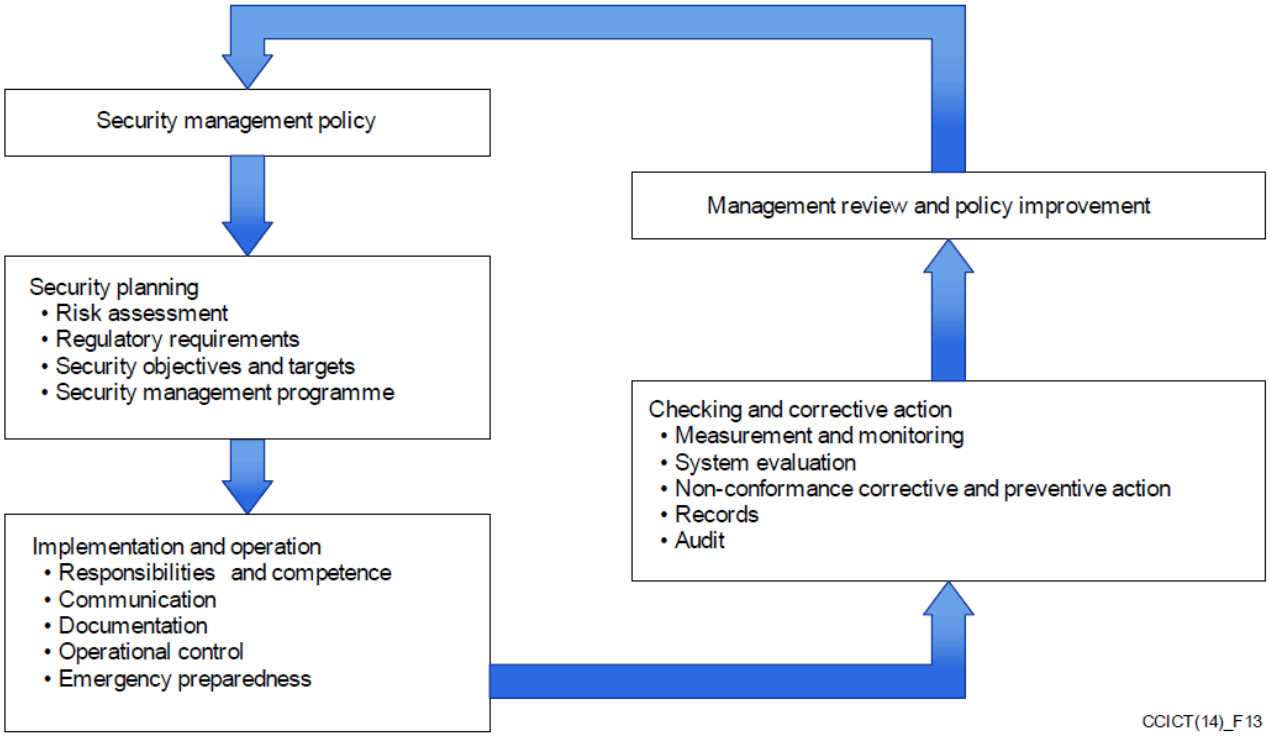

Figure 9 — ISO 28000 security management system elements

The World Customs Organization (WCO) SAFE Framework of Standards [28] is intended to ensure the security of global supply chains and includes a handbook describing the factors indicating that shipments have a high-risk of containing counterfeit goods. The SAFE Framework is based on customs-to-customs agreements and also customs-to-business partnerships with benefits being given to businesses that meet supply chain security standards.

IEC TC 107, whose field of activity is process management for the avionics industry, has produced a specification concerned with the avoidance of use of counterfeit, fraudulent and recycled electronic components [IEC TS 62668-1]. This committee is also currently working on a specification for managing electronic components from non-franchised sources to prevent counterfeit components entering the supply chain [IEC TS 62668-2].

SAE International (originally the Society for Automotive Engineers) has developed a number of specifications specifically intended to avoid counterfeit electronic components being introduced in the supply chains of the aerospace and automotive industries that are widely referred to in the electronics industry. SAE has produced two documents that are intended for the use of those making purchasing decisions:

SAE AS5553 [57] "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation"; and

SAE ARP6178 [56] "Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors"; and a specification intended for use by distributors: SAE AS6081 [58]: "Counterfeit Electronic Parts; Avoidance Protocol, Distributors". SAE has

also produced a specification on testing: SAE AS6171 [59]: "Test Methods Standard; Counterfeit Electronic Parts".

IEC TC 107 works closely with SAE International on SAE AS5553 through a liaison arrangement.

Most of the forums concerned with the problem of counterfeit goods mentioned earlier offer advice or guidelines on supply chain management. In general, there are requirements for product traceability, inspection and testing (performed by a 1st, 2nd or 3rd party).The UK IP Crime Group has produced a Supply Chain Toolkit in 2011.

7.8. Testing

The International Electrotechnical Commission (IEC) operates the following conformity assessment schemes http://www.iec.ch/about/activities/conformity.htm:

- IECEE – IEC System of conformity assessment schemes for electrotechnical equipment and components;
- IECEx – IEC system for certification to standards relating to equipment for use in explosive atmospheres;
- IECQ – IEC quality assessment system for electronic components.

These IEC CA schemes are based on 3rd party certification and employ online systems to provide information on certificates that can be used in the effort to identify counterfeit products.

The IECEE operates the certification body (CB) scheme that is based on the principle of mutual recognition by its members of the test results for obtaining certification or approval at the national level. The CB Bulletin http://members.iecee.org/iecee/ieceemembers.nsf/cb_bulletin?OpenForm is a database for users of the CB scheme that provides information on:

- The standards accepted for use in the scheme;
- The participating National Certification Bodies including product categories and the standards for which they have been recognized; and
- National differences of each member country for each standard.

IECEE CBTC Online is an online test certificate registration system for national certification bodies that also allow public access.

The IECEE has established a Task Force to study measures to combat counterfeiting (CMC-WG 23 "Counterfeit").

The IECEx international certification system consists of the following components:

IECEx Certified Equipment Scheme;
IECEx Certified Service Facilities Scheme;
IECEx Conformity Mark Licensing System;
IECEx Certification of Personnel Competencies (CoPC).

The IECEx CoC Online provides information on certificates and licenses issued in accordance with these schemes.

The IECQ operates the IECQ Electronic Components Management Plan (ECMP) for avionics systems and the IECQ Hazardous Substances Process Management (HSPM) scheme. Certificates are available online.

7.9. Databases

Databases of known counterfeits are provided for the use of enforcement agencies, such as those operated by WCO and Interpol, and also consumers. The ICC Counterfeiting Intelligence Bureau maintains a case study database.

7.10. Market surveillance

Market surveillance consists of the "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" [38].

Counterfeit goods may be identified during market surveillance activities, and market surveillance authorities could be involved in the effort to combat the trade in counterfeit goods. 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 [54].

Some countries require the registration of products for them to be marketed. For example, the Standards Organization of Nigeria has recently introduced an e-product registration scheme in an attempt to limit the sale of counterfeit products.

8. Standards organizations

The main international standardization organizations addressing topics relevant to combating counterfeiting are the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO created a technical committee to produce specifications of anti-counterfeiting tools (ISO TC 246) in 2009. This committee developed a specification of the performance criteria for authentication solutions used to combat the counterfeiting of material goods (ISO 12931) [ISO 12931:2012]. This specification aims to increase consumer confidence, make supply chains more secure and help public authorities create preventive, deterrent and punitive policies. ISO TC 246 is no longer active but work in this area will continue under ISO TC 247.

Standardization in the field of the detection, prevention and control of identity, financial, product and other forms of social and economic fraud is within the scope of ISO TC 247: "Fraud countermeasures and controls". This committee has developed an ISO guidance standard on the interoperability of object identifiers for anti-counterfeiting – ISO 16678 [ISO 16678:2014]: "Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade". This new project concerns the use of mass serialization to identify products against a database to ascertain a level of authenticity. This International Standard intends to enable reliable and safe object identification to deter introduction of illegal objects to the market. The serial numbered products can be authenticated throughout the manufacturing and distribution chain including the consumer.

ISO recognized that counterfeiting and piracy affects a huge assortment of consumer goods including apparel and footwear, medicines, autos and auto parts, food and beverages, cosmetics, movies and music, electrical products, safety devices and aircraft parts. Specific consumer concerns include safety and health risks, performance aspects, usability/fitness for purpose, accessibility, data protection, job losses, economic harm and links to organized crime.

http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf

The joint ISO/IEC technical committee ISO/IEC JTC 1/ SC 31 is working on automatic identification and data capture techniques. This committee has seven working groups on the following topics:

- WG1 Data carrier;
- WG2 Data structure;
- WG4 Radio frequency identification for item management;
- WG5 Real time locating systems;
- WG6 Mobile item identification and management (MIIM);
- WG7 Security for item management;

The European Committee for Standardization (CEN) is also working on AIDC technologies in TC 225.

Many national standardization organizations have established committees equivalent to those in ISO/IEC. To give just one example, The German standardization institute (DIN) has created DIN NA 043-01-31 to work on automatic identification and data capture techniques [29] and DIN NA 043-01-31-04 UA on Radio-frequency Identification for Item Management.

IEC TC 107 on process management for avionics is working on counterfeit prevention.

In addition, SAE International is producing specifications to avoid the use of counterfeit electronic components in high-technology industries, and GS1 has produced a suite of specifications on item identification and supply chain management.

9. Guidelines for combating counterfeiting

Guidelines for combating counterfeiting have been presented by a number of organizations from different perspectives – from the vantage points of manufacturers and distributors, governments and their enforcement agencies, and consumers.

The Anti-Counterfeiting Forum suggests best practices for OEMs (Original Equipment Manufacturers), distributors and component manufacturers [30]. These guidelines include:

- sourcing directly from the manufacturer or an authorized distributor or, if not possible, from a locally-established grey market source;
- insistence upon documentary evidence of authenticity if grey market sources are used;
- greater co-ordination of product and component life cycle management;
- ensuring that scrap and faulty products are disposed of beyond use; and
- improvement of product traceability by use of unique identifiers and control of documentation.

The Components Technology Institute Inc. (CTI) has developed a Counterfeit Components Avoidance Program (CCAP-101) [62] for the certification of independent distributors of electronic components. Requirements are specified for distributors to detect and avoid the delivery of counterfeit components to their customers. Electrical testing may be performed. This certification program is intended to meet the objectives of the SAE AS5553 specification.

Similarly, the Independent Distributors of Electronics Association (IDEA) has produced a specification for counterfeit mitigation and inspection (IDEA-STD-1010A) [50] and also a quality management specification (IDEA-QMS-9090) [49].

The ICC IP Roadmap includes recommendations for business and government actions on all aspects of intellectual property protection, including combating counterfeiting and piracy. In particular, ICC urges governments to do more to enforce IPR regulations as "government resources allocated to combating piracy and counterfeiting are often woefully inadequate compared to the scale of the problem".

The OECD observed that the market for counterfeit and pirated products can be divided into a "primary market" in which consumers believe the products to be genuine, and a "secondary market" in which the purchasers knowingly buy counterfeit or pirated products in their search for a bargain. A person who has no scruples about buying a counterfeit shirt or handbag may well not wish to purchase counterfeit medicine or electrical equipment. Different strategies are required to combat counterfeiting in these two markets, and it is therefore necessary to know in which market a particular product is traded.

It may be possible to combat the counterfeiting of products in the primary market effectively, for example, with information campaigns pointing out the dangers of purchasing counterfeit products, whereas for products in the secondary market it may be necessary to impose more severe penalties.

The UK IP Crime Group Supply Chain Toolkit [31] aims to raise awareness of the problem of counterfeit goods entering legitimate business supply chains, and offers guidance on how to protect

intellectual property assets. An outline of the process by which a company can reduce the risks of counterfeit goods entering its supply chain is given in Figure 10.

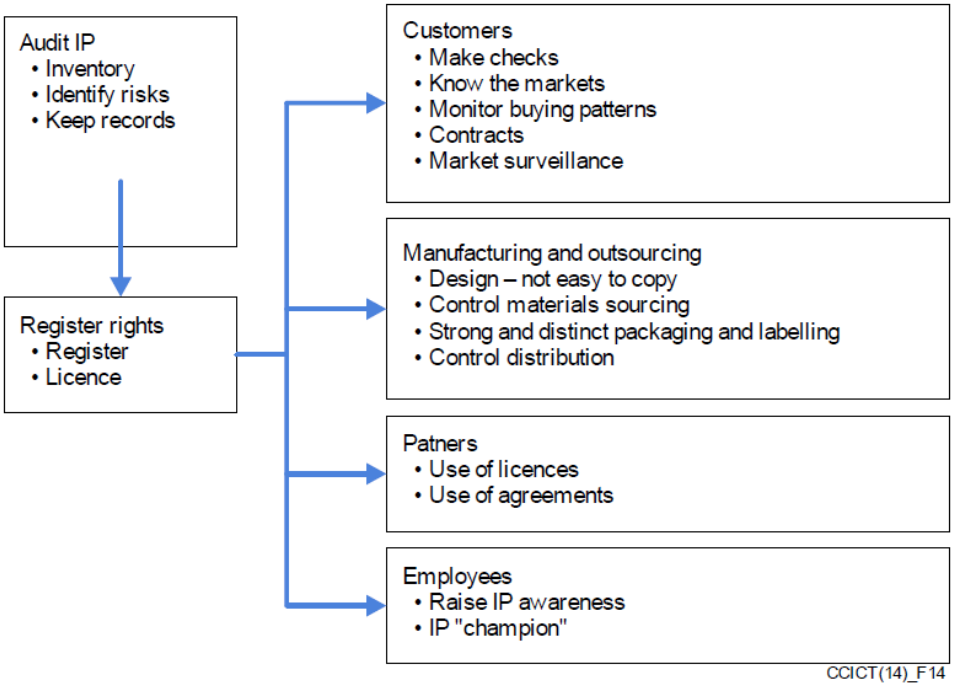

Figure 10 — Protecting intellectual property rights (adapted from UK IP Crime Group Toolkit [31])

MMF has developed a Resource Guide for Governments that proposes a range of measures, including:

– adoption of changes in legal and regulatory frameworks so as to restrict the activation of counterfeit devices on telecommunications networks;
– restrictions on the importation of mobile devices and accessories that are not compliant to industry standards or approved/compliant with a country's legislative and regulatory framework;
– establishment of necessary global industry and authority alliances and solutions for validation of original products by authorities, consumers, and the sales channel;
– development of harmonized and innovative technological solutions that limit the possibility of counterfeit mobile devices from being activated on telecommunications networks; and
– support of standards that lead to enhanced security features (such as unique individual identification numbers) that deter the manufacture of counterfeit and other illegal products.

This approach necessarily moves beyond reliance on traditional enforcement action alone moving instead towards blocking these devices from operating on networks. That said, enforcement, awareness campaigns and market surveillance will remain important, and mobile phone manufacturers will continue to work with national authorities wherever possible.

10. Conclusions

Counterfeiting is a growing problem that is affecting an ever wider range of products. In the ICT sector, mobile phones are especially targeted with some 250 million counterfeits sold annually constituting some 15%-20% of the global market. Apart from clear economic impacts on the manufacturers of the genuine products (brand devaluation, loss of revenue, copyright and trademark infringement, unfair competition), on authorized dealers and governments (as tax payments are avoided, additional costs in ensuring compliance with applicable national legislation, the need to react to public security dangers, and lost labour opportunities), there are also dangers to the health, safety and privacy of consumers, public safety aspects and negative effects on network operators (due to lower quality of

service (QoS) delivery, potential interference and electromagnetic compatibility (EMC) problems, and network disruption). The majority of these counterfeit mobile phones are produced in one country in Asia, and it is in this country that the majority of counterfeit electronic components originate as the result of recycling in the informal sector of e-waste from developed countries as identified by the US Senate Armed Services Committee hearing on counterfeit electronic parts in the defence systems supply chain [5]. It is clear that much more work needs to be done to identify and deal with the sources of counterfeit equipment before it is exported around the world.

The legal instruments to combat counterfeiting are largely in place but enforcement is still weak. The 2008 OECD report concluded that the "magnitude and effects of counterfeiting and piracy are of such significance that they compel strong and sustained action from governments, business and consumers. More effective enforcement is critical in this regard, as is the need to build public support to combat the counterfeiting and piracy. Increased co-operation between governments, and with industry, would be beneficial, as would better data collection."

Governments have become more engaged in this issue and many are conducting awareness campaigns, offering advice and more rigorously pursuing offenders, as can be seen in China recently. Governments not only need to enforce IPR regulations but also implement the Basel Convention to ensure that used and end-of-life equipment is handled in an environmentally sound manner, rather than contributing to the informal counterfeiting economy. Ethical recycling practices should be adopted worldwide.

Government may also wish to link market surveillance activities to those of the customs authorities to improve the capabilities of detecting counterfeit products. Seized counterfeit ICT equipment should be considered as e-waste and handled in accordance with environmentally sound waste management schemes.

The companies and industries impacted by counterfeiting have organized information campaigns and lobbied in support of their interests. There does though appear to be a need for greater awareness of the issues of counterfeiting. In the USA, the 2012 National Defence Authorisation Act (NDAA) assigns full responsibility to contractors for detecting fake components and rectifying any case in which fake components have found their way into products.

Consumers also need to be aware of the dangers of purchasing counterfeit equipment and that counterfeits may not be safe to use and may not perform as well as the genuine articles. It is evident that many national and international bodies, as well as manufacturers, retailers and the media, regularly highlight the issues presented by counterfeit products to consumers. It remains the case, however, that consumers often make an active decision to purchase counterfeit goods, whatever the potential consequences, seemingly on the basis of price.

Counterfeiting could also potentially be combated by equipment life cycle management, not only of the supply chain but also of the return, reuse and recycling phases of the complete life cycle of the equipment. Life cycle management requires means to identify and authenticate items and the processes to securely track them. Tracking though should be appropriate and sufficient for its purpose as automatic identification and data capture (AIDC) technologies, such as RFID, do present significant privacy issues as objects could potentially be linked with their owners. Care should be taken in the standards process to respect the privacy of consumers and not facilitate the oppression of users of ICT products via identifier registration mechanisms. Consumers should also be protected from arbitrary disconnection from networks.

AIDC technology and supply chain management standards, as reviewed earlier, can be applied to combat counterfeiting.

Combating counterfeiting requires co-operation across industry sectors. Enforcers such as customs authorities could be supported by some generic tools (such as those for detecting fake passports and

bank notes) as well as an array of sector and product specific mechanisms and targeted actions with the co-operation of the public and private sectors.

In the mobile phone sector today, there are a number of systems based on IMEI registration, which are operated or planned by individual administrations and regulatory authorities to identify genuine and legally imported mobile terminals. There are also a number of regional initiatives for the exchange of information on mobile terminal devices of illegal origin. Such mechanisms can cause issues for legitimate users too. For example, a foreign user travelling into a country, then using a local SIM card in their device may be caught in a white listing trap where they are unable to use their device. Such mechanisms can cause issues with the free movement of goods. In other ICT sectors, such mechanisms do not exist due to the nature of the products and structure of the industries.

Even though some countries have deployed successful solutions relying on IMEI to deter the spread of counterfeit mobile phones; others, especially developing countries, still face significant challenges in finding effective solutions to combat counterfeit devices. At present, the available solutions in some countries are based on blocking the mobile phones with invalid IMEI numbers on their networks, blocking the use of equipment that is not type approved by the regulator, or blocking the illegal import of these devices, or by performing other actions on consumer awareness, enforcement measures and appropriate legislation changes on the national level.

The main international standardization organizations have addressed topics relevant to combating counterfeiting. There is currently no ITU Recommendation available, for example, to compare the different existing systems for combating counterfeiting, describe a relevant framework, and consider performance and interoperability on a global level. ITU and other relevant stakeholders have key roles to play in fostering co-ordination between the parties concerned to identify ways of dealing with counterfeit devices internationally and regionally. In addition, ITU is instructed to assist the membership in taking the necessary actions to prevent or detect the tampering with and/or duplication of unique device identifiers.

This Technical Report addresses topics relevant to combating counterfeiting only, such as what counterfeiting is, its impact, the IPR conventions and its enforcement, industry anti-counterfeiting forums, measures to combat counterfeiting and organizations involved in counterfeiting. To assist regulatory authorities in protecting consumers, operators and governments from the negative effects of counterfeit devices, ITU should study this issue further.

11. ITU engagement

Resolution 177 of the ITU 2010 Plenipotentiary Conference (PP-10) "*invites Member States and Sector Members* to bear in mind the legal and regulatory frameworks of other countries concerning equipment that negatively affects the quality of their telecommunication infrastructure, in particular recognizing the concerns of developing countries with respect to counterfeit equipment" [32].

WTDC-14 Resolution 79: "The role of telecommunication/information and communication technologies in combating and dealing with counterfeit telecommunication/information and communication devices" and PP-14 Resolution COM5/4 on "Combatting counterfeit telecommunication /information and communication technology devices" mandate ITU to address the issue of counterfeit ICT equipment.

Study Group 11 (SG11) Question 8 is studying this issue, and ITU held a workshop on "combating counterfeit and substandard ICT equipment" in Geneva in November 2014.

http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx

ITU-T Study Groups 16 and 17 have produced Recommendations relevant to the identification and authentication of objects.

ITU-T Study Group 5 (SG5) is responsible for studying design methodologies to reduce the environmental impacts of the use of ICT by such means as recycling.

The Director of TSB has established an Ad-hoc Group (AHG) on IPR: http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx to study patent policy, software copyright and marks guidelines, and other related issues. This Group has been meeting since 1998. Symposia have also been arranged jointly by ITU and WIPO such as those on multilingual domain names in 2001 and on "dispute resolution at the crossroads of information and communications technologies and intellectual property" in 2009: http://www.wipo.int/amc/en/events/workshops/2009/itu/index.html. ITU also organized a Patents Roundtable in 2012 to provide a neutral venue for industry, standards bodies and regulators to discuss whether current patent policies and existing industry practices adequately respond to the needs of the various stakeholders. http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx. To date, this Group has not addressed the counterfeiting issue.

ITU has a role to play in addressing the problem of counterfeit ICT equipment.

The ITU Telecommunication Development Sector (ITU-D) SG1 Report on Regulation and Consumer Protection in a Converging Environment (March 2013), prepared in the framework of Resolution 64 of the ITU World Telecommunication Development Conference (Hyderabad, 2010), cited the protection of innovators, creators and consumers from counterfeiting and piracy associated with the online (and increasingly cross-border) distribution of goods and services as a challenge for regulatory authorities.

According to the guidelines for developing countries on establishing conformity assessment test labs in different regions, published by the ITU Telecommunication Development Sector in May 2012, Member States indicated that counterfeit equipment is aggravating conformance and interoperability problems http://www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf It is noted that "suspicion of dumping of sub-standard products in the marketplace which have failed testing in other countries is a further cause of concern as is the importation and deployment of counterfeit products. A key component of the answer to such concerns is to have a robust type approval regime and test lab working from a set of technical standards, a testing regime and testing capability to approve and monitor communications technologies which are being deployed on the marketplace, backed up by surveillance, audit and enforcement. If there are no established technical requirements, type approval regime and test labs available to a country or region then the marketplace is left largely unprotected". Testing and interoperability can be severely constrained where multiple standards from different bodies are implemented within a product. It should be acknowledged that whilst seemingly attractive, a testing regime alone is unlikely to bring about any real change in situations for addressing counterfeits.

It should be noted that as counterfeiters become increasingly sophisticated, counterfeit products can conform to specified technical requirements and interoperate with genuine products. As such, counterfeit products can conform to a set of relevant technical standards and pass the conformance and interoperability test. In this case, only the trademark holder can accurately identify counterfeit products from genuine products by performing product evaluation.

The problem of counterfeit ICT equipment was addressed by the ITU Regional Workshop on Bridging the Standardization Gap (BSG) for the Arab and Africa Regions (Algeria, 26-28 September 2011), and a directive was produced to encourage the sharing of information at a regional level by establishing a database containing blacklisted counterfeit products.

http://www.itu.int/ITU-T/newslog/ITU+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx

The ITU-T Telecommunication Standardization Advisory Group (TSAG) Information Session on Conformance Assessment & Interoperability (Geneva, 13 January 2012) and the ITU Forum on

Conformance & Interoperability for the Arab & African Regions (Tunisia, 5-7 November 2012) highlighted the conclusion of the Arab Region that counterfeit equipment is a wearisome problem, especially in the mobile handsets market, as well as the need for a global co-operation in this regard. http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf], [http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00000E0005PPTE.pptx

The issue of mobile device theft, grey market and counterfeit devices and its impact on the industry, on operators, on governments and on users was considered by the Regulatory Associations meeting organized by the ITU Telecommunication Development Sector (Sri Lanka, Colombo, 1 October 2012) in accordance with Resolution 48 (Rev. Hyderabad, 2010) "Strengthening cooperation among telecommunication regulators", calling on ITU to organize, co-ordinate and facilitate activities that promote information sharing among regulators and regulatory associations on key regulatory issues at the international and regional level. Representatives of 10 regional regulatory associations, including ARCTEL-CPLP, AREGNET, ARTAC, EMERG, FRATEL, REGULATEL, OCCUR, FTRA, SATRC and APT, outlined that regional actions can be highly beneficial in this concern, such as:

– sharing of GSM and CDMA blacklist databases through the signature of bilateral or multilateral agreements;
– industry compliance with the security recommendations against the reprogramming of the duplication of IMEI or the manufacturer's electronic serial identification number;
– establishment of regulatory fiscal and/or customs mechanisms that ensure greater control be applicable to imported handsets, preventing the exit or re-export of stolen mobile terminal devices and/or their parts;
– conduction of campaigns to raise public awareness of the importance of reporting the theft and loss of their mobile terminal devices.

Many regional associations described their experiences on this matter and recognized that it is a crucial problem that needs to be addressed in co-operation with the industry and the operators. The regulatory associations' meeting adopted a recommendation that ITU in collaboration with the GSM Association conduct studies on the issue of mobile theft, grey market and counterfeit devices and provide guidelines and recommendations. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf

12. Glossary

AC	Allocation Class
ADI	Aerospace and Defence Identifier
AIDC	Automatic Identification and Data Capture
ALE	Application Layer Event
AWP	Automated Working Place
CB	Certification Body
CBV	Core Business Vocabulary
cc	class code
CD	Compact Disc
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CEIR	Central Equipment Identity Register

CIPS	Comprehensive Information Protection System
CoPC	Certification of Personnel Competencies
DB	DataBase
DCI	Discovery, Configuration and Initialisation
DNS	Domain Name System
DVD	Digital Versatile Disc
EIR	Equipment Identity Register
EMC	Electromagnetic Compatibility
EPC	Electronic Product Code
EPCIS	EPC Information Service
GDTI	Global Document Type Identifier
GIAI	Global Individual Asset Identifier
GID	General Identifier
GII	Genuine IMEI Implant programme
GINC	Global Identification Number for Consignment
GLN	Global Location Number
GRAI	Global Returnable Asset Identifier
GSIN	Global Shipment Identification Number
GSM	Global System for Mobile communications
GSRN	Global Service Relation Number
GTIN	Global Trade Item Number
HF	High Frequency
ic	identification code
IC	Integrated Circuit
ICT	Information and Communication Technology
ID	Identification
IMEI	International Mobile Equipment Identity
IP	Intellectual Property
IP	Internet Protocol
IPM	Interface Public-Members
IPR	Intellectual Property Rights
ISBN	International Standard Book Number
ISSN	International Standard Serial Number
IT	Information Technology
LLRP	Low Level Reader Protocol

LTE	Long-Term Evolution
ME	Mobile Equipment
MEID	Mobile Equipment Identity
MIIM	Mobile Item Identification and Management
MRA	Mutual Recognition Agreement MS::C Mobile Switching Centre
MSISDN	Mobile Subscriber Integrated Services Digital Network
NIR	Non-Ionizing Radiation
OID	Object Identifier
ONS	Object Naming Service
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RM	Reader Management
RoHS	Restriction of Hazardous Substances
RP	Reader Protocol
RUIM	Removable User Identity Module
SFP	Security Features Provider
SGLN	Global Location Number with or without Extension
SGTIN	Serialized Global Trade Item Number
SIM	Subscriber Identity Module
SLDc	Second Level Domain code
SMD	Surface-Mounted Device
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SS7	Signalling System No. 7
SSCC	Serial Shipping Container Code
TAC	Type Allocation Code
TC	Technical Committee
TDS	Tag Data Standard
TDT	Tag Data Translation
TID	Tag ID
TLDc	Top Level Domain code
TV	TeleVision
UHF	Ultra High Frequency
UII	Unique Item Identifier

UIM	Unique Identification Mark
UMTS	Universal Mobile Telecommunications System
UPC	Universal Product Code
URL	Uniform Resource Locator
USB	Universal Serial Bus
WG	Working Group

Annex A

Systems for identifying counterfeit mobile devices

(This annex forms an integral part of this Technical Report.)

As described earlier in this Technical Report, counterfeit mobile devices have been of particular concern and a number of initiatives have been taken to limit the spread of counterfeit mobile devices. Some of these schemes were initially intended to ensure that mobile devices were imported in accordance with legal procedures (i.e. that they were not contraband) and were subsequently assessed to be useful to give confidence that the devices were not counterfeit. These schemes also share many characteristics with initiatives that were specifically designed to address the problem of counterfeiting, such as being based on the authentication of a unique identifier (the IMEI).

The following sections present examples of measures being taken by national authorities and on a regional level.

A.1. Examples of measures taken by national administrations and regulators

A.1.1. Azerbaijan

The Mobile Devices Registration System (MDRS) http://www.rabita.az/en/c-media/news/details/134 was established in the Information Computer Centre (ICC) of the Ministry of Communications and Information Technologies in accordance with the "Rules of Mobile Devices Registration" approved by decision No. 212, dated 28 December 2011 of the Cabinet of Ministers of the Republic of Azerbaijan.

The purpose of mobile device registration is to prevent the import of low-quality devices of unknown origin that do not meet the required technical standards, such as those limiting the emission of harmful electromagnetic radiation, and to increase the recognition and competitiveness of manufacturing companies. The registration system prevents the use of lost/stolen mobile devices and those illegally imported into the country.

Since 1 March 2013, mobile operators enter the IMEI-numbers of the mobile devices used in Azerbaijan into a central database system on a daily basis. The Ministry of Communications and Information Technologies reported that over 12 million GSM devices were registered after the launch of the MDRS. Some 300,000 devices that do not meet the standards are allowed to continue functioning with their current mobile phone numbers but any new devices that do not meet the standards will not work in the country. http://www.mincom.gov.az/media-en/news-2/details/1840

The IMEI-numbers of all mobile devices used in the network prior to 1 May 2013 were considered as registered and therefore operate freely in the networks. After the launch of the Registration System, the IMEI-number of each mobile device imported into the country for private use (with a SIM-card by one of the country's mobile operators) should be registered within 30 days of the date of its connection to the network. This rule is not applied to roaming mobile devices using SIM-cards provided by foreign operators.

Subscribers are able to determine the legitimacy of their devices on the basis of their IMEI-numbers by using a special webpage (imei.az) or by use of SMS messages. The central database system was created in the Information Computer Centre (ICC) of the Ministry of Communications and Information Technologies and, at the same time, mobile operators installed the appropriate equipment that is synchronized with the central database. The software for the MDRS was developed by local specialists.

A.1.2. Brazil

SIGA - Devices Management Integrated System

The Brazilian National Telecommunications Agency – Anatel mobile service regulation determines that operators should only allow on their network and that user should only use devices that have been certified by Anatel (Article 8, IV and Article 10, V of the Mobile Service Regulation, approved by Resolution 477/2007[9]). Based on that, Anatel enforced that the Brazilian mobile operators should implement jointly a technological solution to curb the use of mobile devices that are not certified, tampered with or cloned IMEI.

The established action plan submitted by the operators to fulfil this obligation defined the outline of the technological solution to be implemented, the possible criteria based on real users in order to minimize the impacts on the population, and the criteria to be implemented for new users after the solution goes live so that only devices that comply with Anatel's regulation can access the network, the criteria to be implemented for mobile users in order to avoid inconvenience to users or foreign users, awareness campaigns on the mobile network users, among other things.

The action plan was approved by Anatel in 2012 considering the technical and regulatory aspects. The solution was called SIGA - Devices Management Integrated System, and is being developed based on the following technical premises:

- centralized solution and built jointly by all Brazilian mobile operators;
- integrated solution with operators of mobile platforms;
- automated solution, allowing the input of information with low human intervention;
- scalable and expandable based growth and complexity;
- dynamic and flexible, with rules that may be adjusted over time;
- composed of multiple sources of information such as call detail records (CDRs) and management systems operators, including the use of international databases, as appropriate, among others;
- Efficient to allow actions to be taken to be able to curb the use of illicit devices;
- able to minimize potential impacts on regular end users;
- reliable and secure.

Today the technical operation of SIGA is done by ABR Telecom[10], a technical association created as a joint venture of most Brazilian telecom operators to develop, deploy and operate centralized technical solutions for the Brazilian telecom market.

In this project, there is a strong interaction with all other parties involved to ensure the success of SIGA, such as Anatel, customs authorities, Association of Operators (SindiTelebrasil), Operators, Equipment Manufacturers, Union of Manufacturers (ABINEE) and ABR Telecom. Besides, the issue is complex because it involves all areas of an operator, several market players as well as the end user; a thorough discussion of all actions is being required.

SIGA is active on the operators' network since March 2014, collecting the required information to diagnose the market size of the devices that do not comply with Brazilian regulation, so that all the involved parties can define the necessary actions to guarantee that these counterfeit, substandard and unauthorized devices are removed from the network with minimum consumer impact.

One of the possible actions in discussion to fulfil this premise is to create a legacy database that contains all the cases (unique relation of a terminal and its users) that are allowed to continue to

9 http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477

10 http://www.abrtelecom.com.br

operate on the network but block any new irregular terminal access to the network. In this sense, the impact to the user is considerably reduced and the legacy database should disappear with the turnover of the devices.

In addition, it is important to include in the discussion entities representing the user, and to have a strong communication plan implemented before any actions that impact directly the user are taken (such as blocking or suspending the device).

In this sense, SIGA communication plan is being developed by the Operators, Anatel, and the Union of Manufactures together; the plan should be deployed by all these entities in a co-ordinated effort on all the consumer channels (such as publicity ads, operators bills and call-centres) showing the users the advantages to buy legal and certified terminals and the risk they take when using counterfeit and substandard terminals in the Brazilian scenario.

More detailed information on the technical aspect of this project can be obtained directly with National Telecommunications Agency – Anatel of the Brazilian administration.[11]

A.1.3. Colombia

In 2011, the Ministry of Information and Communication Technologies issued Decree 1630 for the purpose of establishing mechanisms aimed at controlling the marketing and sale of both new and used terminal devices and creating two types of centralized databases: one that has a registry of the IMEI numbers of terminal devices reported stolen or lost and prevent their use or activation, and another database with a registry of a record of the IMEI numbers for terminal devices legally imported or manufactured in the country and associated with an identification number of the owner or subscriber.

Law 1453 of 24 June 2011 on Citizen Security makes a provision for sentences of from 6 to 8 years imprisonment for those who tamper with, reprogram, relabel, or modify the IMEI of a mobile device and for those who activate devices reported stolen. In addition, altered equipment is confiscated. http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf

These initiatives have been taken to control the sale and use of stolen mobile devices but are also likely to have an impact on the use of counterfeit products.

A.1.4. Egypt

In 2008, the National Telecommunication Regulatory Authority (NTRA) established a market surveillance department to support its type approval activities. A system was adopted in Egypt in 2010 to combat the use of counterfeit mobile terminal equipment. This system makes use of the GSMA IMEI DB to provide a weekly update of the IMEI TAC white list and a central equipment identity register (EIR) – IMEI database. This solution was aimed at curbing the use of handsets with illegal, fake, null and cloned IMEIs, combating handset thefts, and addressing health and safety concerns.

11 prre@anatel.gov.br

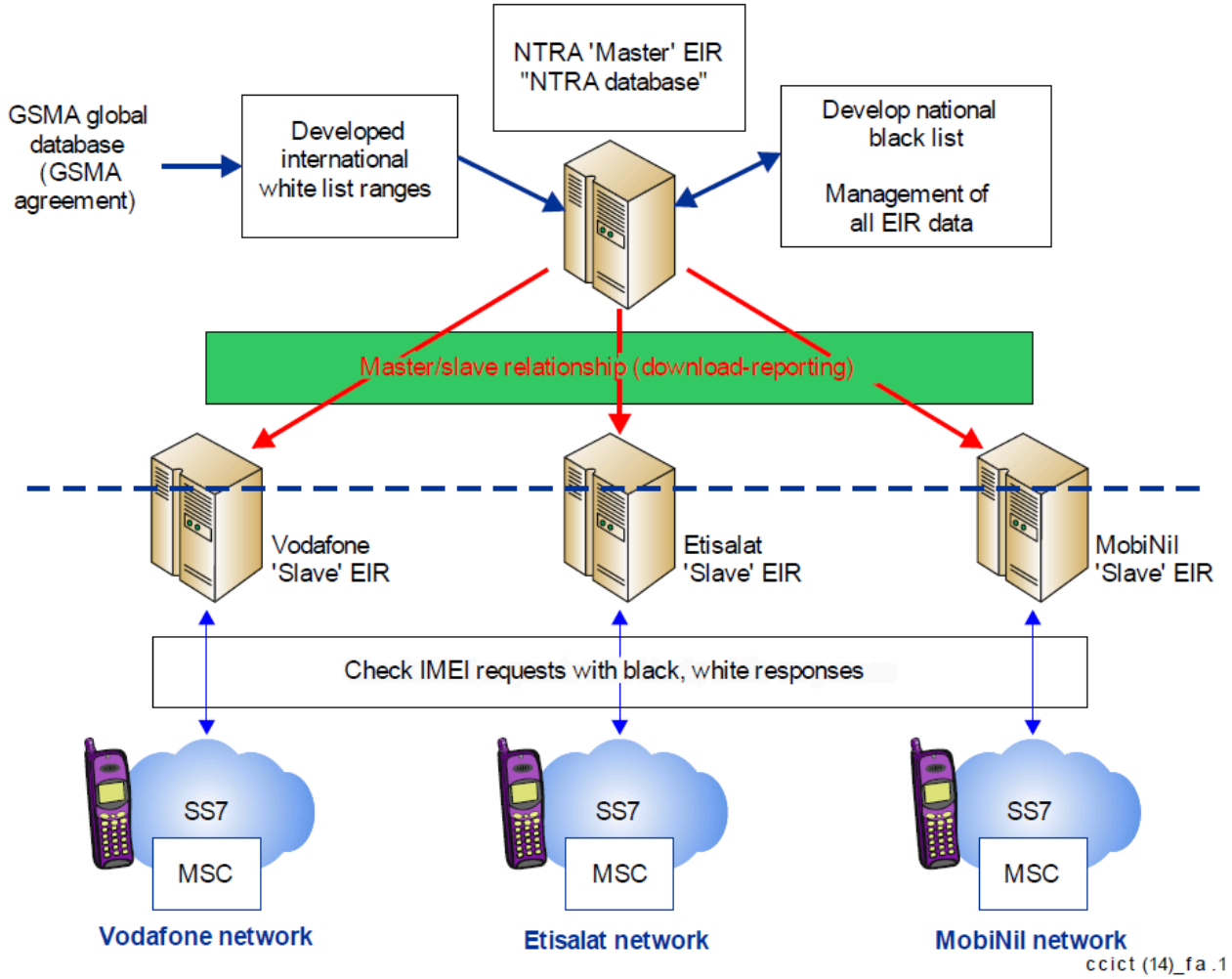

Figure A.1 — Central EIR IMEI database solution in Egypt

According to the NTRA, there were 3.5 million mobile handsets with the illegal IMEI code 13579024681122, 250,000 handsets with cloned IMEIs, 500,000 handsets with fake IMEIs, 350,000 with all zeros IMEI, and 100,000 without an IMEI code. http://www.itu.int/ITUD/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf

In February 2010, NTRA announced that the country's three mobile operators will block services to all anonymous users and cell phones without an IMEI (http://www.cellular-news.com/tags/imei/) in the Egyptian market. http://www.cellular-news.com/story/42911.php

A.1.5. Indonesia

The conditions for the importation of cellular phones into Indonesia were tightened in January 2013 through the imposition of technical procedures and standards requirements, distribution and port restrictions, pre-shipment controls and an obligation to pre-register IMEI numbers before importation. These requirements are specified in the Industry Minister Decree No 81/2012 and Trade Minister Decree No 82/2012.http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf

A.1.6. Kenya

A.1.6.1. Introduction

According to the Anti-Counterfeit Agency (ACA) of Kenya, unfair competition between counterfeits and genuine products cost the business community (local manufacturers, investors and innovators) an estimated Sh.50b (approximately, USD 596 million) in revenue loss annually, thereby threatening the closure and/or relocation of many industries. The loss to government and the economy from

counterfeiting is estimated over Sh.19 billion (approximately, USD 227 million) annually through tax evasion.http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471

The most affected items are medicinal drugs, electronics, CDs and pirated software, alcoholic drinks, mobile phones and farm inputs.

The Communications Commission of Kenya was established by the Kenya Information and Communications Act, Cap 411A, to license and regulate information and communications services. Section 25 of the said Act mandates the Commission to license the operation and provision of telecommunications systems and services, respectively, subject to requisite conditions. One of the license requirements is to type approve communications equipment to ascertain their compatibility with the public communications networks. It is in this context that Regulation 3 of the Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010, requires that all mobile phone handsets are type approved by the Commission before connection to public networks. http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf

The essence of the type approval process is primarily to safeguard the public against the undesirable effects brought about by substandard and/or counterfeit mobile phone devices which include technical, economic, health, and security concerns. Additional information on the challenges associated with counterfeit handset in the ICT industry is indicated below in clause A.1.6.2. A mobile handset that has no proper international mobile equipment identity (IMEI) cannot be type approved.

It is for the above reasons that the usage of counterfeit mobile phone devices must of necessity be phased out. This is, however, being done with due consideration to the interests of all the stakeholders, hence the phased activities leading to the switch off date of 30 September 2012.

With a view to ensuring that the interest and concerns of the stakeholders are taken on board, the Commission has since October 2011 hosted a series of open consultations between the ICT industry players, various government agencies and other stakeholders on the issue of counterfeit mobile handsets with the aim of addressing the challenges they bring about in the industry and the economy at large. Through these consultations, specific action points were agreed in relation to the subject matter.

Among the actions agreed is the running of a public awareness campaign by the Commission to ensure that subscribers are made aware of the negative effects of counterfeit devices; the establishment of a system that will be used by the public to determine whether the handsets they have are genuine; the establishment of systems for blocking counterfeit handsets within the mobile networks; and the provision of customer related support services.

Another significant action is the stepping up of surveillance and crackdown on counterfeit mobile devices by all relevant government agencies. A handset verification system with access to the GSMA database was established to enable subscribers to verify the validity of their phones through the submitted IMEI. Furthermore, a system for blocking counterfeit handsets within the mobile networks was implemented.

As a result of the above activities, 1.89 million counterfeit mobile phones were phased out in Kenya after 30 September 2012.

A.1.6.2. Phasing out of counterfeit mobile phone handsets

a) Background

1) Implementation of equipment identity register (EIR) system

Mobile use in Kenya is today a necessity as opposed to a luxury. This is seen in the increasing subscribers in the country currently placed at about 29.2 million. However, one challenge associated with the introduction of mobile communications

services is mobile phone theft as well as the increasing rate of crimes committed with the help of mobile phones, which pose a great security risk.

In the wake of these threats, the Commission in 2001 embarked on a series of consultations with the existing licensed mobile operators with a view to finding a lasting solution to the problem. Meanwhile, the East African Communications Organization (EACO) has adopted a resolution which *inter alia* required regulators and operators in the region to consult on the best way to check the theft of mobile handsets within the region.

During these consultations, it was noted that an inherent feature in the mobile networks dubbed the equipment identity register (EIR) provides a mechanism to address the issue of mobile phone theft. EIR is able to check the unique international mobile equipment identity (IMEI) of each phone that accesses the mobile network and keeps records of the same. Such information would then be availed to the extent possible where the authorities require it.

To this end, a Memorandum of Understanding (MoU) has been entered into among all the mobile operators on the implementation of the EIR system that will also pave the way for the implementation of the system at the regional level. It was also noted that the existence of counterfeit mobile handsets, which in most cases either have duplicated and/or fake IMEIs, would lead to a situation where when one such illegally acquired handset is tracked and deactivated using the EIR system. Several other handsets with similar IMEIs are likely to also get deactivated.

In this context, the reason to address the presence of counterfeit handsets in the market prior to the full implementation of the EIR system emerged as its success shall depend on the eradication of counterfeit handsets as advocated internationally.

2) Implementation of the legal/regulatory framework with regard to mobile handsets

   i) Legal/regulatory framework

   From the communications industry perspective, the relevant legal/regulatory framework governing handsets is provided for under Section 25 of the Kenya Information and Communications Act, Cap 4II A. The licenses granted under this Act have a condition which requires licensees to only offer services to those using a type approved apparatus.

   In addition, the Kenya Information and Communications (import, type approval and distribution of communications equipment) Regulations, 2010, explicitly requires all handsets to be type approved. It is important to note that in accordance with the Commission's type approval requirements, a GSM handset that has no proper IMEI or a tampered IMEI cannot be type approved. Consequently all handsets without a proper IMEI or with a cloned IMEI are in essence illegal and their use would therefore be in contravention of the above mentioned Act.

   ii) Recent Directive by the Commission and the operators' response

   In May 2011, the Commission gave notice to all mobile network operators to phase out counterfeit handsets on their networks by 30 September 2011. This directive was consonant to the spirit and letter of the statutes governing the communications sector.

b) Industry consultations

Upon receipt of the directive, the mobile industry players reverted with requests to review the directive citing a large number of subscribers using phones with the same or faulty IMEI. In addition, the operators feared that the disconnection of an estimate of over two million counterfeit handsets in use would have adverse implications on their revenue.

To ensure the implementation of the directive with minimal service interruptions, the Commission set up an open committee, made up primarily of representatives of mobile operators, relevant government ministries and agencies, equipment manufacturers, vendors and civil society.
The series of consultations between the ICT industry players and various government agencies is also aimed at addressing the challenges brought about by counterfeit mobile handsets in the industry and the economy at large. The GSM Association (GSMA) noted that Kenya is one of the countries with a rather large market for phones that have been stolen in Europe or outright counterfeit. Drawing from their experience in handling the matter at an international level, GSMA has equally made significant advisory contributions to support the process in Kenya through various technical interventions.
The consultations have so far resolved to take specific actions in support of the initiative. Key among these include the running of a public awareness campaign by the Commission to ensure that subscribers are aware of the negative effects of counterfeit devices, and mobile handset manufacturers commitment to the establishment of a system that will be used by the public to determine whether their handsets arc genuine or not. In addition, the network operators established systems to block counterfeit handsets in their networks and to provide subscriber-related support services, and government agencies to step up surveillance and to crack down on counterfeit handsets.
Establishment of a handset verification system with access to the GSMA database to enable subscribers verify the validity of their phones through a submitted IMEI was developed to go hand in hand with the consumer awareness campaign. http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf

A.1.7. Rwanda

The Rwanda Utilities Regulatory Agency (RURA) announced a plan to ban the importation of counterfeit mobile devices into the country in 2013 while not blocking those already in use. http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print. Rwanda is also facing a challenge of counterfeit phones which re-route calls made to the EACO harmonized short codes 100 (customer service), 101 (recharge in Tanzania) and 102 (check balance in Tanzania) to 112 (emergency, police). This forced RURA to reassign a different short code for customer information service on a temporary basis. http://www.eaco.int/docs/19_congress_report.pdf

A.1.8. Sri Lanka

In March 2013, the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) requested expressions of interest to "Design, Develop, and Install Central Equipment Identity Register (CEIR) for Mobile Networks in Sri Lanka". http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf

With the aim to curtail the counterfeit mobile phone market, discourage mobile phone theft and protect consumer interests, TRCSL intends to implement a central equipment identify register (CEIR) that connects to the EIRs of all the mobile operators. CEIR acts as a central system for all network operators to share blacklisted mobile terminals so that devices blacklisted in one network will not work on other networks even if the subscriber identity module (SIM) card in the device is changed.

According to the TRCSL's requirements, CEIR shall ensure the following functions:

a) CEIR shall have a capability to maintain the database of IMEIs of all the devices registered on the mobile networks.
b) CEIR shall be able to identify IMEIs such as:
   1) IMEIs which are not allocated;
   2) IMEIs which are null, duplicate or all zero.
c) CEIR database shall contain the following information of the devices that registered with all mobile networks in Sri Lanka:

1) IMEIs;
2) IMEI status (white, grey, black);
3) Date of record creation;
4) Date of last record update;
5) Device model number;
6) IMEI status reason (invalid, stolen, cloned, valid).

d) CEIR shall be able to block services to subscribers with registered devices with invalid or blacklisted IMEIs.
e) CEIR shall be able to identify the device model, version and other information.
f) CEIR shall allow the creation of a new record in the database containing the IMEIs whenever a new subscriber account is activated.
g) CEIR shall make available the operators' updated local black/white/grey list database information so as to prevent cloning across networks and to keep the database information up to date.
h) CEIR shall update periodically the IMEI database with the latest information on valid IMEI assignments by the most efficient methods available.
i) CEIR shall have a capability to identify counterfeit IMEIs by comparing IMEIs provided by GSMA.
j) CEIR shall be interoperable with all the appropriate network elements and interfaces of mobile operators.
k) CEIR database shall support a flexible method of input (via manual entry of data, flat files containing IMEI range updates).
l) CEIR shall perform a check on the IMEI format to verify if it is of a valid format and range.

A.1.9. Turkey

In 2006, the Information and Communication Technologies Authority (ICTA) of Turkey established a central equipment identity register (CEIR) in order to prevent the usage of non-registered mobile phones, tax loss, unfair competition in the sector, hijacking as well as automating the importation processes. The infrastructure was established to curtail illegally imported devices and disconnect the smuggled, lost and stolen devices or the ones with cloned IMEI numbers from wireless network.

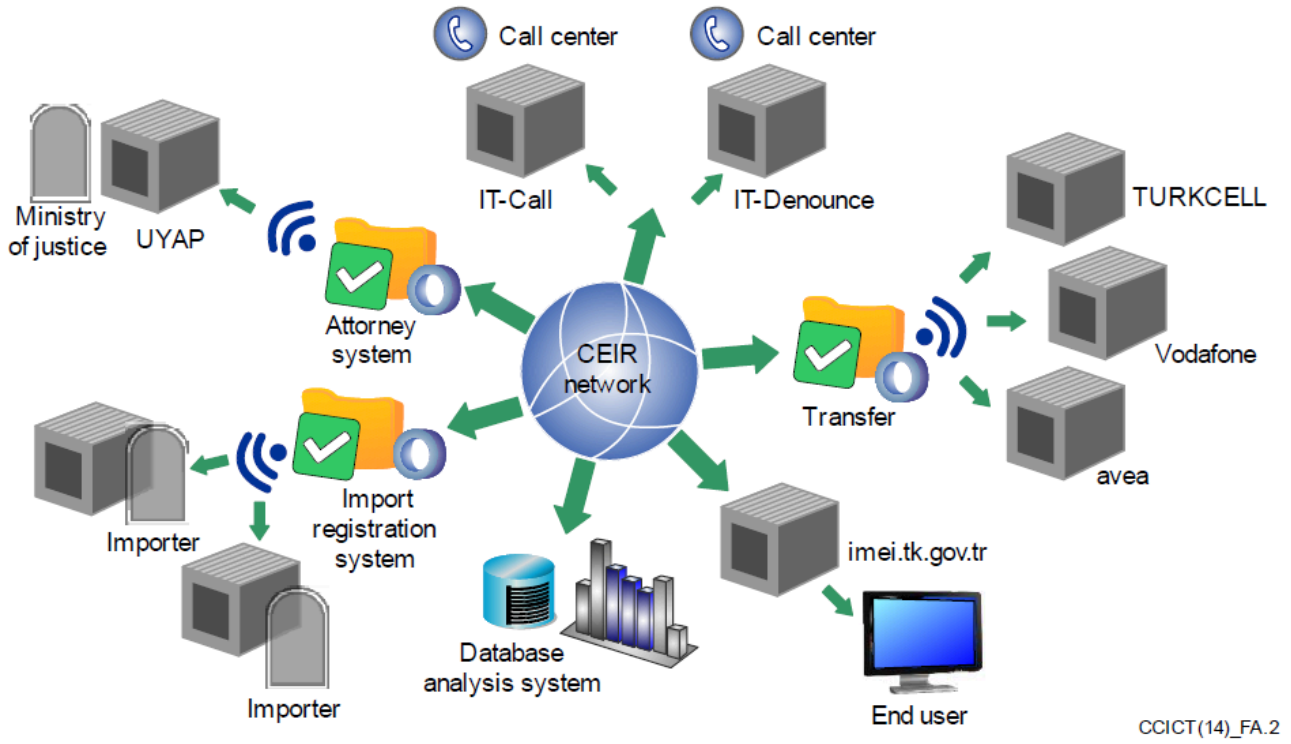

Figure A.2 — Central equipment identity registry structure

Key:

https://www.icta.mu/mediaoffice/publi.htm

The Radio Communication Law has categorized IMEI numbers as follows:

– White list: consists of IMEI numbers of devices which are registered and their electronic identity information has not been changed.
– Black list: consists of IMEI numbers that belong to the missing and stolen category of devices and their electronic identity information has been changed. Telecom operators are given the mandate to cut off wireless communication from such devices.
– Grey list: consists of IMEI numbers which do not belong to either the white or black list, and for which wireless communication is allowed. Telecom operators are required to analyse the call details from such devices and notify ICTA. Telecom operators are also required to notify such device users through a text message that their device is not included in the white list.
– Matched white list: consists of IMEI numbers that are a clone of the mobile subscriber integrated services digital network (MSISDN) number devices of users who have deposited a registration fee. It also consists of devices that entered into a subscription contract with a telecom operator, and were in Turkey for a temporary period with the MSISDN number.

According to the ICTA 2010 Annual Report, there were 131,836,847 IMEI numbers which are legally registered and 14,308,239 IMEI numbers which were included in the black list due to being lost, smuggled, stolen and cloned as of the end of 2010. https://www.icta.mu/mediaoffice/publi.htm

A.1.10. Uganda

The Uganda Communications Commission (UCC) has embarked on the implementation of a project http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html that aims at the gradual elimination of counterfeit mobile phones from the Ugandan market. A study certified by the UCC indicates that about 30% of mobile phones on the Ugandan market are fake. The survey also indicates that the government loses about Schilling 15 billion (~5400 million USD as of November 2014) in tax revenue to fake or counterfeit mobile phone dealers.

http://www.monitor.co.ug/Business/Commodities/Survey+finds+30of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html++

In December 2012, a consultative document "Timeline and distribution of tasks for the elimination of counterfeit mobile phones" was published by UCC http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf defining the project and four implementation phases as follows:

PHASE 1: Verification of mobile phones:

During this phase, consumers will be able to check the status of their phones using one or both of the Internet and SMS applications.

Consumers are advised to immediately verify the legitimacy of their mobile phones using the above two avenues.

PHASE 2: Denial of service to new counterfeit phones:

During this phase, new counterfeit mobile phones that have previously not subscribed to any network shall be denied access to all networks. The proposed date for the implementation of this phase was 31 January 2013.

PHASE 3: Disconnection of all counterfeit mobile phones:

During this phase, all counterfeit mobile phones, including the ones that have already subscribed to a network, shall be disconnected. The proposed date for the implementation of this step was 1 July 2013.

PHASE 4: Consolidating the project:

During this phase, the Commission shall review the outcomes of the project relating to the implementation of the project and issues to do with e-waste management and cloning of IMEIs. Proposals for the handling of various issues in this phase are still under consideration.

A.1.11. Ukraine

A.1.11.1. Introduction

In 2008, the immediate and most pressing problem that needed to be addressed was the import of contraband mobile terminals which constituted 93%-95% of the market. A considerable part of these handsets of unknown origin did not meet the Ukrainian standards either in their technical characteristics or in their safety. The National Commission for the State Regulation of Communications and Informatization (NCCIR) was empowered by the Law of Ukraine "On the Radio Frequency Resource of Ukraine" to impose additional measures to protect the Ukrainian market against low quality, unauthorized or illegally imported mobile terminals.

NCCIR defined a regulatory procedure for the import of mobile terminals. As a technical implementation of the import procedure, the Automated Information System for Mobile Terminal Registration in Ukraine (AISMTRU) was created and put into operation by the Ukrainian State Centre of Radio Frequencies (UCRF) in 2009. Consequently, illegal imports of mobile terminals decreased dramatically, constituting no more than 5%-7% of the market in 2010 and continuing to decrease in the following years.

IMEIs are used in the Ukraine to create a database of those devices that have been legally imported into the Ukraine. The following lists are maintained: a "white list" of those devices that have been legally imported, a "grey list" of devices of unconfirmed status and a "black list" of devices that will be denied service. Access is provided to the regulatory and customs authorities, network operators and the general public with appropriate levels of access privileges.

AISMTRU performs the following functions:

- automation of processing the applications of importers to complete the regulatory procedures for registration and use of terminal equipment within telecommunication networks;
- prevention of illegal "grey" import of mobile terminals to the territory of Ukraine;
- combat handset theft;
- automation of the UCRF workflow and increase in the working efficiency between UCRF and the terminal market players;
- determination of the 'cloned' IMEI codes and blocking the terminals with 'cloned' IMEI codes.

Detailed information on AISMTRU follows in clause A.1.11.2.

The Ukrainian legislation prohibits the selling of mobile terminals with IMEI codes that are not registered with AISMTRU. The main part of AISMTRU is the general database, which maintains "white", "grey" and "black" lists of IMEI codes of mobile terminals. With the first connection and registration of a terminal with any operator network, the IMEI code of the terminal is automatically forwarded by the mobile operator to the general database. AISMTRU reveals the IMEI codes which are not available in the "white" list, identifies the counterfeit mobile telephones and registers the corresponding IMEI codes in the "grey" list. All owners of the respective terminals receive a SMS notice and have to confirm the terminal's legal origin within 90 days of the date of entering the "grey" list.

The IMEI codes of stolen terminals are registered in the "black" list upon request of a law-enforcement authority, which makes theft of terminals useless. The same procedure is applied to the terminal lock-out upon the request of the owners of the lost telephones. The "black" list terminals are not served by network operators.

The objective of consumer protection is achieved by implementing the tool for easy verification of the legality of a mobile terminal prior to its purchase. Any customer may verify the status of the IMEI code of the terminal by sending an SMS with this code to the nationwide number "307" or by using the Internet-portal of UCRF. The time required for verification does not exceed 10 seconds.

AISMTRU implementation ensures a legal terminal market in Ukraine and has decreased abruptly the "grey" (illegal) import of mobile terminals in Ukraine. The share of illegally imported mobile terminals has decreased from 93%-95% in 2008 to 5%-7% in 2010 and the following years. A revenue of more than USD 500 million was transferred to the State Budget of Ukraine over the period 2010-2012 from customs duties on the import of mobile terminals, compared with USD 30 million over the preceding three years. The Ukrainian mobile terminal market consists mainly of mobile terminals which meet the technical characteristic requirements for use in Ukraine.

A.1.11.2. Automated Information System for Mobile Terminal Registration in Ukraine (AISMTRU)

A.1.11.2.1. Background

The rapid development of mobile (cellular) communications services provided by operators and the significant prevalence of this type of telecommunication service in Ukraine have led to the rapid growth of the mobile terminals market in Ukraine and, as a consequence, to an increase of the importation of these products.

A "mobile terminal" means a mobile handset or any other telecommunication network end user equipment, which has an international identifier (IMEI code) and may be identified within the network by using this code.

In 2008, a critical situation existed on the mobile terminals market in Ukraine: 93%-95% products on the market were "grey imports" or, simply speaking, smuggled goods. Moreover, a major part of these products was represented by copies of branded handsets of unknown origin, which did not meet

the Ukrainian standards either in their technical or safety characteristics. Various market regulation measures were not able to change this situation and terminals were not manufactured in Ukraine.

Then the independent regulatory authority — the National Commission for the State Regulation of Communications and Informatization (NCCIR) — was empowered by the Law of Ukraine "On the Radio Frequency Resource of Ukraine" to impose additional measures to protect the Ukrainian market against low quality, unauthorized or illegally imported mobile terminals.

A.1.11.2.2. Objectives

To control the import, realization and use of terminals, NCCIR has defined the following objectives:

a) To protect the Ukrainian market against low quality mobile terminals, which could be unauthorized or dangerous for human health.
b) To ensure adequate quality of mobile communication services.
c) To resolve the social problem of handset theft, especially from children.
d) To combat illegal import and realization of mobile terminals on the Ukrainian market.

Procedures have been developed for the importation and realization of mobile equipment with due consideration of the above objectives. These procedures have been laid down in official acts — Procedure for import of radio electronic facilities and radiating devices and Procedure for realization of the electronic facilities and emitting devices in Ukraine.

A.1.11.2.3. Import procedures

Import of radio equipment to Ukraine is controlled by the customs authorities under the following conditions:

– availability of a document on radio equipment's conformity with technical regulations;
– conformity to the Register of radio electronic facilities and radiating devices, which are permitted to be used in Ukraine in the frequency bands of common usage;
– absence in the Register of radio electronic facilities and radiating devices, which are prohibited to be used in Ukraine in the frequency bands of common usage.

IMEI codes, submitted by the importer to UCRF, are processed and entered into the "white list" of the IMEI general database. For registration of international identifiers of terminal equipment, legally imported to Ukraine, the State Customs Service of Ukraine provides UCRF with the extract from the customs declaration (in electronic form) for the import of radio electronic facilities on a daily basis.

As a technical implementation of the above regulatory import procedure, the Automated Information System for Mobile Terminal Registration in Ukraine (AISMTRU) was created and put into operation by UCRF on 1 July 2009.

In accordance with the Law of Ukraine "On Confirmation of Conformity", the conformity of the terminal equipment has to be certified by the bodies, agreed by the Regulator (NCCIR).

A.1.11.2.4. AISMTRU functions

AISMTRU functions are as stated in clause A.1.11.1

– automation of processing the applications of importers;
– prevention of illegal "grey" import of mobile terminals to the territory of Ukraine;
– combat handset theft;
– automation of the UCRF workflow and increase in working efficiency between UCRF and the terminal market players;
– determination of the 'cloned' IMEI codes and blocking the terminals with 'cloned' IMEI codes.

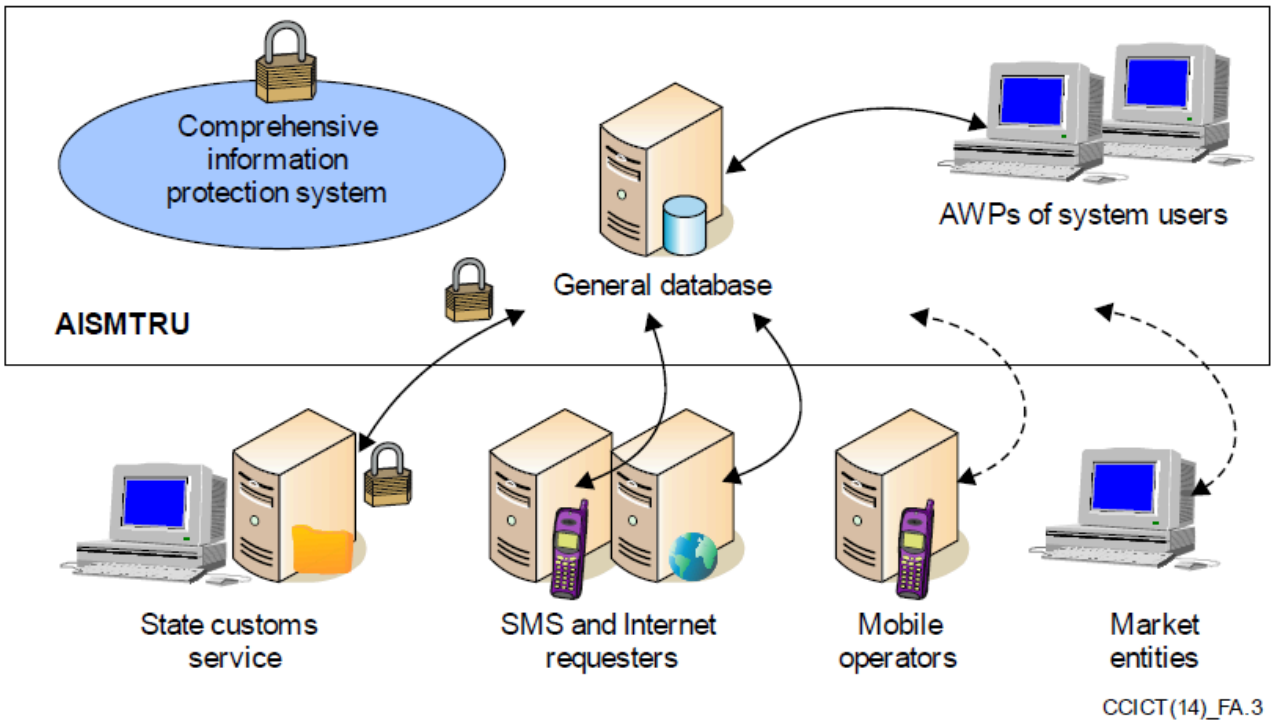

Figure A.3 — AISMTRU functions

A.1.11.2.5. Authorization

According to the current legislation, the following entities are authorized to use AISMTRU:
- Ukrainian State Centre of Radio Frequencies;
- National Commission for the State Regulation of Communications and Informatization;
- mobile operators;
- State Customs Service;
- Ministry of Internal Affairs;
- buyers and users of mobile terminals; and
- importers.

A.1.11.2.6. IMEI general database

The main part of AISMTRU is the IMEI general database, which maintains three lists conventionally called as:
- "White list": A register of the IMEI codes of the terminals legally imported or manufactured in Ukraine.
- "Grey list": A register of the general database with IMEI codes of the terminals not entered into the "white list" or "black list" at the moment of first registration in the telecommunication network.
- "Black list": A register of the IMEI codes of the terminals prohibited to be served in operator's networks (stolen or lost handsets, terminals with unconfirmed legal origin after 90 days from the date of entering the "grey list").

The maintenance subsystem of the IMEI general database gives the UCRF authorized users a tool for data entry into the "white list". The "grey" and "black" lists are automatically generated. The UCRF authorized users have a limited right to change the status of specific IMEI codes in the "grey" and "black" lists.

Each action of the UCRF authorized user is confirmed with an individual user's electronic digital signature.

The subsystem has a data import function to forward data from terminal importers and mobile operators to the IMEI Register.

By processing the data from the "white list" and data from operators, form the importers and the Customs Service, it is possible to form and maintain registers of the "grey" and "black" lists.

The first stage of bringing the system into operation solved two objectives:

a) Protection of the Ukrainian market against unauthorized mobile terminals with low quality that may be hazardous to a user's health.

b) Prevention of illegal import of mobile terminals and their realization on the Ukrainian market.

Subsequently, a system has been developed to ensure the solution of all objectives, including that of de-motivating the theft of mobile terminals, especially from children.

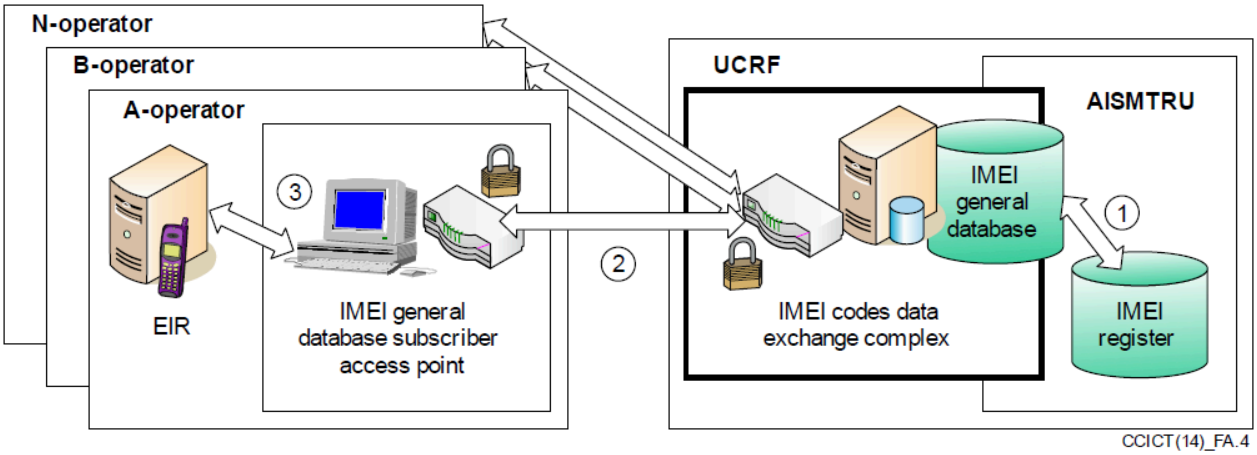

Figure A.4 — EIR and IMEI general database

As a second stage, a subsystem for exchanging the IMEI codes from the "white", "grey" and "black" lists between AISMTRU and the national mobile operators was implemented. At this stage, the exchange of IMEI codes was carried out in the 'manual' mode.

In addition, data exchange subsystems were implemented to inform the Ministry of Internal Affairs about the stolen/lost terminals and with the Customs Service to communicate information about the imported terminals.

To ensure active interaction with AISMTRU, operators and UCRF have provided:

– maintenance of the equipment identity register (EIR);
– IMEI general database subscriber access point (subscribers point);
– channel for interaction between the subscribers point and EIR;
– application of digital signature certificates for the authorized users.

The system, embedded in AISMTRU, synchronizes the work of the EIR of cellular (mobile) operators and the IMEI general database. This makes automatic exchange possible for the lists of IMEI codes between the EIRs of mobile operator networks and the IMEI general database. By doing so, the IMEI code of each terminal, after its registration in the operator network, appears in AISMTRU and is checked in the IMEI general database.

For today, the synchronization server supports both manual and automatic modes to connect to the EIR of operators.

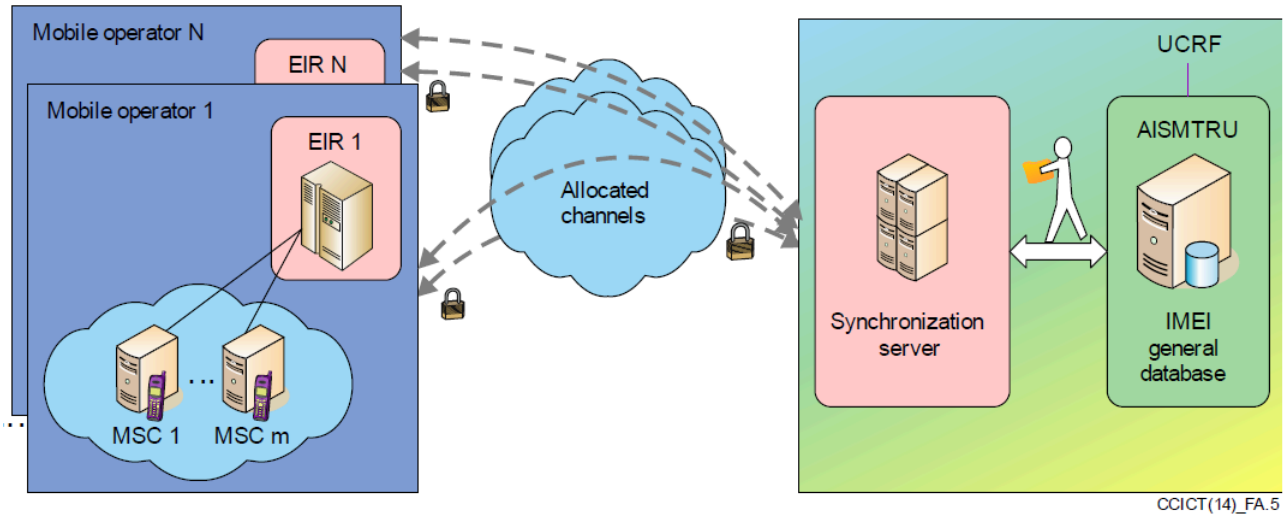

Figure A.5 — Synchronization server

A.1.11.2.7. Features

Features of the system include:
- use of industry standards for data storage and transfer (data exchange);
- ensured security of the data and the entire system;
- use of the national standard for digital signature to secure the integrity and non-repudiation at all stages of data processing in the system;
- modular structure of the system;
- operation mode 24x7.

A.1.11.2.8. Data security

The comprehensive information protection system (CIPS) of AISMTRU meets the requirements of the current legislation and is confirmed by the positive conclusion issued on the basis of the examination results by a competent governmental authority.

CIPS ensures:
- control of limited access to confidential information;
- identification of safety threats to the limited access information which is transferred, processed and stored in the system;
- protection of confidentiality, integrity and availability of the limited access information against unauthorized access;
- prevention of information leakage while passing an insecure environment;
- protection of technological information from unauthorized access, destruction, alteration or blocking.

Security and reliability are guaranteed by:
- use of reliable means of electronic digital signature to ensure authenticity and integrity of information, authorization and authentication of the authorized users;
- implementation of electronic digital signature in accordance with the national standards of Ukraine;
- availability of backup and recovery system;
- maintenance of secure log (logging any user action or event in the system).

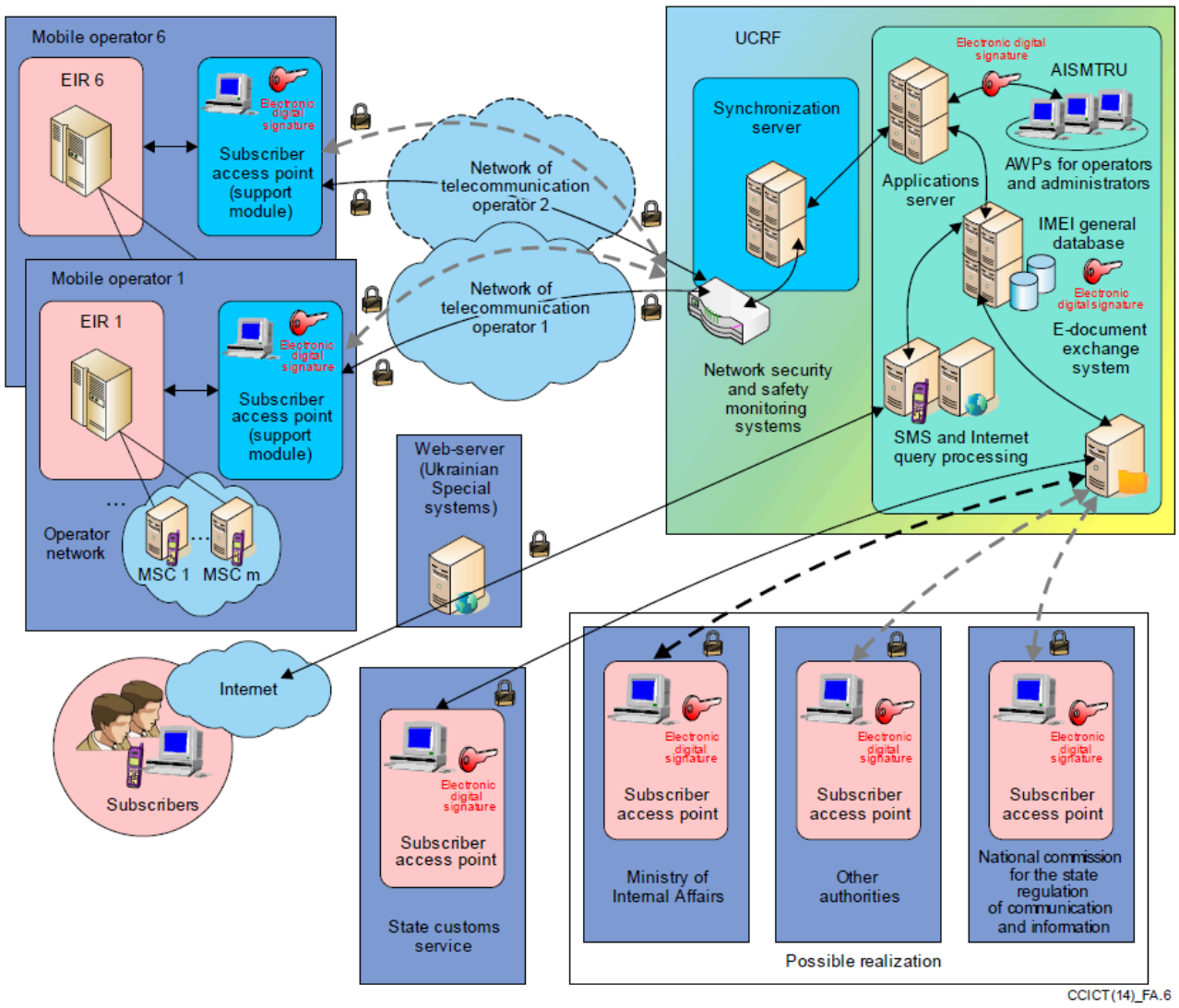

Figure A.6 — Comprehensive information protection system (CIPS) of AISMTRU

A.1.11.2.9. Effects of implementation

a) Consumer protection

Each buyer can verify the legality of a mobile terminal prior to its purchase in Ukraine. It can be done by use of the UCRF official website or by sending an SMS with a verified terminal IMEI code to number '307', which is common for all mobile operators. After a few seconds, a response gives the status of the requested IMEI code in the IMEI general database.

This protects the Ukrainian market from terminals which do not meet the usage requirements specified in Ukraine.

The current Ukrainian legislation prohibits the realization of mobile terminals with IMEI codes that are not registered in the IMEI general database.

b) Combat terminal theft

The IMEI codes of stolen terminals are registered in the "black list" upon request of a lawenforcement authority, thus rendering terminal theft pointless.

The same procedure is applied to terminal lock-out upon the request of the owners of lost handsets.

c) Suppression of illegal import

At first connection to any operator network, any terminal is immediately registered with the related network. The IMEI codes of terminals, served by an operator network (except

for those currently in international roaming), are automatically forwarded in due time (night-time) by the mobile operators to the AISMTRU IMEI general database.
AISMTRU reveals the IMEI codes which are not available in the "white list" of the IMEI general database. These IMEI codes are registered with the "grey list". All owners of the respective terminals receive an SMS warning of a possible lock-out of the terminals in 90 days.
After the 90-day period, the IMEI code is transferred from the "grey list" to the "black list". The "black list" terminals are not served by operators (refusal in network registration, with the exception of emergency calls to number '112'). A connection to any other operator network does not change the status of the "grey" or "black" terminal.
Having received the SMS warning of entering the "grey list" and the 90-day limited service period, the owner can apply to UCRF to present a confirmation of the legal importation of the terminal. The UCRF staff reviews the application of the owner and, in case the legality of importation is confirmed, transfers the IMEI code from the "grey" to the "white list". After this procedure, mobile operators start to serve the terminal without a time limit.
However, for the time being the "black list" terminals are not disconnected due to the absence of the required legal instrument.
UCRF runs a call centre to handle calls relating to requests from mobile terminal users on the IMEI code status and importation of terminals.

d) Legalization of the terminal market in Ukraine

- "Grey" (illegal) import of mobile terminals in Ukraine has decreased abruptly. The share of legally imported mobile terminals increased to 93%–95% in 2010 (versus 7.5% in 2008).
- A revenue of more than USD 500 million was transferred to the State Budget of Ukraine over the period 2010–2012 from customs duties on import of mobile terminals, compared with USD 30 million over the preceding three years.
- The Ukrainian mobile terminal market consists mainly of mobile terminals which meet technical characteristic requirements for use in Ukraine.
- There are 140,865,260 IMEI codes of mobile terminals registered in the AISMTRU IMEI general database as of 30 April 2013.
- AISMTRU paid its way in seven months solely at the expense of funds received by UCRF for the importers' payments.

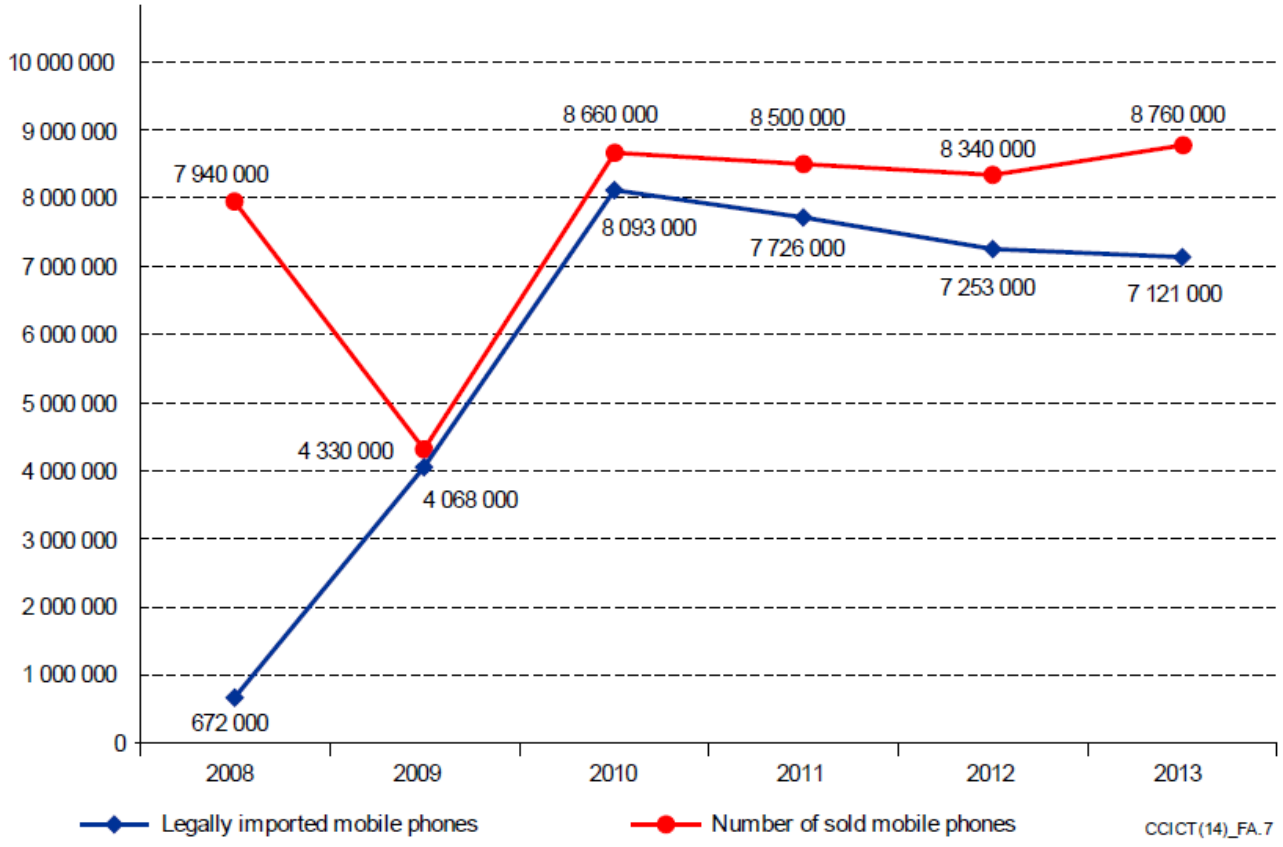

Figure A.7 — Effects of AISMTRU implementation in Ukraine

A.1.12. United Arab Emirates (UAE)

The UAE's telecoms laws prohibit the use, sale, purchase, distribution, and promotion of fake mobile devices. The Telecommunications Regulatory Authority (TRA) takes all the necessary steps to ensure there is a complete stop to the sale and usage of such devices in the UAE. Those involved in the sale of fake mobile phones are given a notice and a fine, while in some cases licenses could be withheld as a consequence of regulations not being met.

In 2011, TRA launched a new campaign http://www.uaeinteract.com/docs/TRA_urges_against_use_of_fake_cell_phones/47437.htm (to raise awareness and discourage the use of fake mobile phones in the UAE, and announced that as of 1 January 2012, all mobile phone devices with a fraudulent IMEI number would cease to work within the UAE's telecommunications mobile network. TRA took out advertisements in daily newspapers warning people of the impending ban on counterfeit phones.

While this measure aimed to render fraudulent mobile phone devices obsolete, service subscriptions were not affected and continued to function normally when using genuine mobile phone devices. By sending an SMS with the mobile device IMEI number to telephone number '8877', users may receive a reply from a service provider giving information on the status of the mobile device. Users of fake devices are immediately contacted by their service providers and all phones that are not type approved have to be disconnected from all telecom services, including calls, texts and Internet.

TRA announced that fraudulent mobile devices are potentially harmful to the user's health, and encouraged all users to take the proper precautions when purchasing the mobile devices and equipment. According to TRA, fake phones are especially prone to battery leaks and explosions, releasing highly corrosive or poisonous chemicals. The low quality assembly also means radiation levels go unchecked, the batteries tend to drain faster, and signal reception is usually much weaker.

An ultimate goal of TRA consisted in eliminating fake mobile devices in the UAE and educating the general public as well as retailers on the risks involved with their use. TRA recognized that the issues of counterfeiting and piracy had a tremendous impact on the economy and intellectual property rights, but fake mobile phones were also low quality devices that had been manufactured without proper tests and checks.

A.2. Examples of joint measures on regional levels

A.2.1. Inter-American Telecommunication Commission (CITEL)

CITEL was established by the Organisation of American States (OAS) General Assembly in 1994 with the aim of promoting the development of telecommunications/ICT in the Americas. All 35 states are members as well as more than 100 Associate Members from the ICT industry.

CITEL Permanent Consultative Committee I (Telecommunications) recommended in 2009 that member states "consider creating databases as part of an overall anti-counterfeit and fraud program" (Final Report of 15th Meeting of CITEL PCC.I 2, October 2009), and in December 2011 CITEL PCC.II (Radiocommunications including broadcasting) began the study of measures being taken by telecommunications administrations regarding the use of counterfeit mobile phones.

PCC.II decided to request Administrations to provide information "about the actions and regulatory and administrative measures taken or planned regarding the fake, counterfeit and substandard cellphones and their negative impacts to users and operators including interference, NIR levels and the use of hazardous or prohibited chemical components" (Final Report of 18th Meeting of CCITEL PCC.II, 22 December 2011, Decision 121).

CITEL has also considered the issue of mobile phone theft and both permanent consultative committees have agreed a number of resolutions related to this issue.

PCC.II agreed Resolution 73 in September 2011 on the "establishment of a regional partnership to combat the theft of mobile terminal equipment". This resolution asked PCC.I to consider "the promotion by CITEL of the establishment of joint measures by the member states to restrict, in any country of the region, the activation of this stolen mobile terminal equipment, and for it to adopt specific recommendations for operators so that they use the resources afforded by technology and do not permit the connection to their networks of equipment whose origin has not been fully identified, establishing a regional partnership to combat the theft of this equipment" (Final Report of 17th Meeting of PCC.II, 6 September 2011, Resolution 73).

PCC.I responded almost immediately by agreeing a resolution on "regional measures to combat the theft of mobile terminal devices" (Final Report of 19th Meeting of CITEL PCC.I, 20 September 2011, Resolution 189). This resolution notes the international nature of the problem as mobile devices are sent to other countries when an individual country takes measures against device theft and, therefore, the necessity of taking measures at the regional level. In addition to measures related to lost/ stolen handsets, Resolution 189 also invites member states to "consider including in their regulatory frameworks the prohibition of the activation and use of the IMEIs or manufacturer's electronic serial number of devices reported stolen, lost or *of unlawful origin* in regional or international databases" (editor's italics).

The Annex to Resolution 189 includes a number of complementary measures such as "to study the feasibility of implementing controls of the local marketing of mobile terminal devices and their connection to networks" and "to promote the establishment of regulatory fiscal, and/or customs mechanisms that ensure the import of mobile terminal devices and/or their parts [are] of lawful origin

and that are certified as in conformity with each Member State's regulatory framework, as well as customs controls preventing the exit or re-export of stolen mobile terminal devices and/or their parts".

PCC.I agreed a Recommendation on "regional measures for the exchange of information on mobile terminal devices reported stolen, lost or recovered" in 2012 (Final Report of 20th Meeting of CITEL PCC.I, 10 June 2012, Recommendation 16) which also included terminals of "illegal origin". Member states are invited "to implement national, regional and international actions and measures so that mobile telecommunication service providers exchange information on stolen, lost or illegal mobile terminal devices through the different existing and operational platforms for the different access technologies to combat informal markets, promoting cooperation among the countries and safeguarding the principles of citizen security and end users' rights". Member States are also advised to "give consideration to creating a database platform for information exchange on mobile terminal devices stolen, lost, or of illegal origin using the MEID (Mobile Equipment Identifier) number(s) used by the Code Division Multiple Access (CDMA), EV-DO and dual mode CDMA/4G and, in many networks, the RUIM (Removable User Identity Module)".

PCC.I has also agreed a "Technical Notebook" on "Stolen and/or lost mobile terminals" (Final Report of 23rd Meeting of CITEL PCC.I, 10 October 2013, Resolution 217).

In May 2014, CITEL approved Resolution 222 (XXIV-14) - "*Strengthening regional measures to combat the spread of counterfeit, substandard and unapproved mobile devices*".

As a result, a Correspondence Group was established to Discuss Regional Measures to Combat the Spread of Counterfeit, Substandard and Unapproved Mobile Devices in order to share information, experiences and technical and regulatory best practices with Member States related to this issue, with the aim of developing recommendations and guidelines that could be established within the Americas Region.

In August 2014, the work plan of this Correspondence Group was approved and included in the scope of the Rapporteurship on Fraud Control, Regulatory Non-compliance Practices in Telecommunications and Regional Measures against the Theft of Mobile Terminal Devices, with the following mandate:

a) To draw up a definition of what is meant by counterfeit, substandard, and unapproved mobile devices.
b) To evaluate the scope and nature of the counterfeit, substandard, and unapproved mobile devices problem.
c) To promote sharing of information and exchanging of experiences among CITEL Members regarding measures taken to fight the sale and use of counterfeit, substandard, and unapproved mobile devices.
d) To document best practices from around the world in fighting the sale and use of counterfeit, substandard, and unapproved mobile devices.
e) To propose the creation of technical notebooks, recommendations and/or resolutions of CITEL addressing technical and regulatory measures to fight the sale and use of counterfeit, substandard, and unapproved mobile devices in the Americas region.
f) To finish the work and report the results achieved to the Rapporteurship on Regulatory Non-compliance Practices and Fraud Control in Telecommunications.

A.2.2. East African Community (EAC)

East Africa loses over USD 500 million in revenue annually from product imitation http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products/. Cheap and substandard products supplied through foreign and local traders and manufacturers are illegally replicating well-known brand names and designs on their packages.

According to a Common Market Protocol, adopted by the EAC in 2010, counterfeit products and trade can only be defeated through collaboration.

The East African Communications Organization (EACO) is a regional body bringing together regulatory, postal, telecommunications and broadcasting organizations from the five member states of the EAC (Kenya, Tanzania, Rwanda, Burundi, and Uganda). EACO has considered the issue of counterfeit mobile phones flooding the region and agreed a corresponding common initiative in 2012.

The EACO Numbering Task Force (CCK-Kenya, TCRA-Tanzania, RURA-Rwanda, ARCT-Burundi, UCC-Uganda) recommended in May 2012 that a national database be developed and procedures adopted for the verification of handsets to protect consumers, businesses and networks from the effects of counterfeits (Report of EACO Numbering Task Force for 2011-2012).

The 19th EACO Congress in 2012 was informed of the status of the implementation of equipment identity registers (EIRs) in the region and some challenges that had been encountered were described in http://www.eaco.int/docs/19_congress_report.pdf. These were the:

– duplication and lack of international mobile equipment identity (IMEI);
– lack of consumer awareness of the dangers associated with counterfeit equipment and lack of knowledge on how to verify that the equipment is genuine;
– lack of local vendors'/resellers' awareness of the issues associated with selling cheap substandard equipment; and
– the high cost of implementation.

In order to overcome these challenges, the following solutions were proposed:

– implement awareness campaigns for consumers and local vendors;
– license all vendors/resellers;
– enhance type approval procedures;
– establish equipment databases; and
– require SIM card registration.

A.2.3. Association of the Communications and Telecommunications Regulators of the Community of Portuguese Speaking Countries (ARCTEL-CPLP)

The Association of the Communications and Telecommunications Regulators of the Community of Portuguese Speaking Countries Association (ARCTEL-CPLP) has members from Angola, Brazil, Cape Verde, Guinea-Bissau, Mozambique, Portugal, São Tomé and Príncipe and East Timor (http://www.arctel-cplp.org). A presentation was made by ARCTEL-CPLP at the ITU Global Symposium for Regulators in 2012 on regional approaches against mobile theft, grey market and counterfeit devices. https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf

ARCTEL-CPLP proposed the extension of the traditional solution (namely, national black list database systems) to the regional level by:

– sharing of the GSM and CDMA black list databases through bilateral or multilateral agreements;
– establishment of regulatory fiscal and/or customs mechanisms that ensure greater control of importing handsets and preventing the re-export;
– industry compliance with the security recommendations against reprogramming or duplication of the IMEI or manufacturer's electronic serial identification number;
– implementation of campaigns to raise public awareness of the importance of reporting theft and loss of mobile terminal devices.

Bibliography

[ISO 10486:1992] ISO 10486:1992 (1992), *Passenger cars — Car radio identification number (CRIN)*, First edition.

[ISO 11784:1996] ISO 11784:1996 (1996), *Radio frequency identification of animals — Code structure*, Second edition.

[ISO 11785:1996] ISO 11785:1996 (1996), *Radio frequency identification of animals — Technical concept*, First edition.

[ISO 12931:2012] ISO 12931:2012 (2012), *Performance criteria for authentication solutions used to combat counterfeiting of material goods*, First edition.

[ISO 14816:2005] ISO 14816:2005 (2005), *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*, First edition.

[ISO 15394:2009] ISO 15394:2009 (2009), *Packaging — Bar code and two-dimensional symbols for shipping, transport and receiving labels*, Second edition.

[ISO 16678:2014] ISO 16678:2014 (2014), *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*, First edition.

[ISO 17363:2013] ISO 17363:2013 (2013), *Supply chain applications of RFID — Freight containers*, Second edition.

[ISO 17364:2013] ISO 17364:2013 (2013), *Supply chain applications of RFID — Returnable transport items (RTIs) and returnable packaging items (RPIs)*, Second edition.

[ISO 17365:2013] ISO 17365:2013 (2013), *Supply chain applications of RFID — Transport units*, Second edition.

[ISO 17366:2013] ISO 17366:2013 (2013), *Supply chain applications of RFID — Product packaging*, Second edition.

[ISO 17367:2013] ISO 17367:2013 (2013), *Supply chain applications of RFID — Product tagging*, Second edition.

[ISO 18185 (all parts)] ISO 18185 (all parts) (2007), *Freight containers – Electronic seals*, First edition.

[ISO 2108:2005] ISO 2108:2005 (2005), *Information and documentation — International standard book number (ISBN)*, Fourth edition.

[ISO 22742:2010] ISO 22742:2010 (2010), *Packaging — Linear bar code and two-dimensional symbols for product packaging*, Second edition.

[ISO 28000:2007] ISO 28000:2007 (2007), *Specification for security management systems for the supply chain*, First edition.

[ISO 28001:2007] ISO 28001:2007 (2007), *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*, First edition.

[ISO 28003:2007] ISO 28003:2007 (2007), *Security management systems for the supply chain—Requirements for bodies providing audit and certification of supply chain security management systems*, First edition.

[ISO 28004-1:2007] ISO 28004-1:2007 (2007), *Security management systems for the supply chain—Guidelines for the implementation of ISO 28000—Part 1: General principles*, First edition.

[ISO 28005-2:2011] ISO 28005-2:2011 (2011), *Security management systems for the supply chain—Electronic port clearance (EPC)—Part 2: Core data elements*, First edition.

[ISO 28219:2009] ISO 28219:2009 (2009), *Packaging—Labelling and direct product marking with linear bar code and two-dimensional symbols*, First edition.

[ISO 3297:2007] ISO 3297:2007 (2007), *Information and documentation—International standard serial number (ISSN)*, Fourth edition.

[ISO 3779:2009] ISO 3779:2009 (2009), *Road vehicles—Vehicle identification number (VIN)—Content and structure*, Fourth edition.

[ISO 6346:1995] ISO 6346:1995 (1995), *Freight containers—Coding, identification and marking*, Third edition.

[ISO/IEC 15417:2007] ISO/IEC 15417:2007 (2007), *Information technology—Automatic identification and data capture techniques—Code 128 bar code symbology specification*, Second edition.

[ISO/IEC 15420:2009] ISO/IEC 15420:2009 (2009), *Information technology—Automatic identification and data capture techniques—EAN/UPC bar code symbology specification*, Second edition.

[ISO/IEC 15438:2006] ISO/IEC 15438:2006 (2006), *Information technology—Automatic identification and data capture techniques—PDF417 bar code symbology specification*, Second edition.

[ISO/IEC 15459-1:2014] ISO/IEC 15459-1:2014 (2014), *Information technology—Automatic identification and data capture techniques—Unique identification—Part 1: Individual transport units*, Third edition.

[ISO/IEC 15459-2:2006] ISO/IEC 15459-2:2006 (2006), *Information technology—Unique identifiers—Part 2: Registration procedures*, Second edition.

[ISO/IEC 15459-3:2014] ISO/IEC 15459-3:2014 (2014), *Information technology—Automatic identification and data capture techniques—Unique identification—Part 3: Common rules*, Second edition.

[ISO/IEC 15459-4:2014] ISO/IEC 15459-4:2014 (2014), *Information technology—Automatic identification and data capture techniques—Unique identification—Part 4: Individual products and product packages*, Third edition.

[ISO/IEC 15459-5:2014] ISO/IEC 15459-5:2014 (2014), *Information technology—Automatic identification and data capture techniques—Unique identification—Part 5: Individual returnable transport items (RTIs)*, Second edition.

[ISO/IEC 15459-6:2014] ISO/IEC 15459-6:2014 (2014), *Information technology — Automatic identification and data capture techniques — Unique identification — Part 6: Groupings*, Second edition.

[ISO/IEC 15459-8:2009] ISO/IEC 15459-8:2009 (2009), *Information technology — Unique identifiers — Part 8: Grouping of transport units*, First edition.

[ISO/IEC 15961:2004] ISO/IEC 15961:2004 (2004), *Information technology — Radio frequency identification (RFID) for item management — Data protocol: application interface*, First edition.

[ISO/IEC 15962:2013] ISO/IEC 15962:2013 (2013), *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*, Second edition.

[ISO/IEC 15963:2009] ISO/IEC 15963:2009 (2009), *Information technology — Radio frequency identification for item management — Unique identification for RF tags*, Second edition.

[ISO/IEC 16022:2006] ISO/IEC 16022:2006 (2006), *Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification*, Second edition.

[ISO/IEC 16023:2000] ISO/IEC 16023:2000 (2000), *Information technology — International symbology specification — MaxiCode*, First edition.

[ISO/IEC 16388:2007] ISO/IEC 16388:2007 (2007), *Information technology — Automatic identification and data capture techniques — Code 39 bar code symbology specification*, Second edition.

[ISO/IEC 18000 (all parts)] ISO/IEC 18000 (all parts) (2008), *Information technology – Radio frequency identification for item management*, Second edition.

[ISO/IEC 18000-3:2010] ISO/IEC 18000-3:2010 (2010), *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*, Third edition.

[ISO/IEC 18000-6:2013] ISO/IEC 18000-6:2013 (2013), *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*, Third edition.

[ISO/IEC 18004:2006] ISO/IEC 18004:2006 (2006), *Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification*, Second edition.

[ISO/IEC 29160:2012] ISO/IEC 29160:2012 (2012), *Information technology — Radio frequency identification for item management — RFID Emblem*, First edition.

[ISO/IEC 29167-1:2014] ISO/IEC 29167-1:2014 (2014), *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*, Second edition.

[ISO/IEC 7816-6:2004] ISO/IEC 7816-6:2004 (2004), *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*, Second edition.

[ISO/IEC TR 24729-4:2009] ISO/IEC TR 24729-4:2009 (2009), *Information technology — Radio frequency identification for item management — Implementation guidelines — Part 4: Tag data security*, First edition.

[IEC 62321:2008] IEC 62321:2008 (2008), *Electrotechnical products — Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers)*, First edition.

[IEC TS 62668-1] IEC TS 62668-1, *Process management for avionics — Counterfeit prevention — Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*, Third edition.

[IEC TS 62668-2] IEC TS 62668-2, *Process management for avionics — Counterfeit prevention — Part 2: Managing electronic components from non-franchised sources*, Second edition.

[IETF RFC 3279] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[ISO/IEC 15459] ISO/IEC 15459, *ISO/IEC 15459, Unique identifiers.*.

[ISO/IEC 15693] ISO/IEC 15693, *ISO/IEC 15693, Identification cards – Contactless integrated circuit cards – Vicinity cards.*.

[ITU X.509] Recommendation ITU X.509, Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T E.164] Recommendation ITU-T E.164, Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[ITU-T X.1255] Recommendation ITU-T X.1255, Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[ITU-T X.668] Recommendation ITU-T X.668, Recommendation ITU-T X.668 (2008) | ISO/IEC 9834-9:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*.

[ITU-T Y.4405] Recommendation ITU-T Y.4405, Recommendation ITU-T H.621 (2008), *Architecture of a system for multimedia information access triggered by tag-based identification*.

[ITU-T Y.4551] Recommendation ITU-T Y.4551, Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[1] http://www.oecd.org/sti/ind/44088872.pdf .

[2] http://www.icc-ccs.org/icc/cib .

[3] http://www.havocscope.com/counterfeit-hp-printing-supplies .

[4] http://www.spotafakephone.com/ .

[5] http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf .

[6] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html .

[7] http://www.wipo.int/treaties/en/ip/washington .

[8] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html .

[9] https://www.gov.uk/government/publications/annual-ip-crime-report-2013-to-2014 .

[10] http://www.aca.go.ke .

[11] http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/ .

[12] http://www.iccwbo.org/bascap/id7608/index.html .

[13] http://www.pasdirectory.com .

[14] http://www.iccwbo.org/bascap/id42204/index.html .

[15] http://www.iccwbo.org/policy/ip/id2950/index.html .

[16] http://www.iacc.org/ .

[17] http://www.ascdi.com/ .

[18] http://www.anticounterfeitingforum.org.uk .

[19] http://archive.basel.int/convention/basics.html .

[20] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf .

[21] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm .

[22] http://www.bbc.co.uk/news/world-europe-10846395 .

[23] http://www.numberingplans.com/?page=analysis&sub=imeinr .

[24] http://www.gsma.com/imei-database .

[25] http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/VAT-Report_TKO.pdf .

[26] http://www.uidcenter.org/learning-about-ucode .

[27] http://www.gs1.org/gsmp/kc/epcglobal .

[28] http://www.wcoomd.org .

[29] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html .

[30] http://www.anticounterfeitingforum.org.uk/best_practice.aspx .

[31] http://www.ipo.gov.uk/ipctoolkit.pdf .

[32] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf .

[33] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818.

[34] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID)*.

[35] ANSI INCITS 371.1-2003, *Information technology - Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol*.

[36] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard*.

[37] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier*.

[38] Adapted from Market Surveillance Regulation EC no 765/2008, art 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf.

[39] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012. http://www.nkrzi.gov.ua/images/upload/142/3963/4b2c475b68c147860c36a6e1fc2a3e47.pdf.

[40] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE and WEEE). Process Management Specification (March 2011) http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346.

[41] DIN 66401 (2010), *Unique Identification Mark (UIM)*.

[42] *Defence Industrial Base Assessment: Counterfeit Electronics*, January 2010 http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-count.

[43] Directive 2002/96/EC.

[44] Establishing Conformity and Interoperability Regimes – Basic Guidelines (ITU, 2014).

[45] *Estimating the global economic and social impacts of counterfeiting and piracy.* http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf.

[46] GS1 EPC Tag Data Standard 1.6, 9 September 2011. http://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf

[47] *Guidelines for developing countries on establishing conformity assessment test labs in different regions*, ITU, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Gu

[48] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412.

[49] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

[50] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.

[51] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 October 2013.

[52] In *WIPO Intellectual Property Handbook* http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf.

[53] Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf.

[54] 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.

[55] *Recycling – From E-Waste to Resources*, UNEP, 2009.

[56] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.

[57] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.

[58] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors*.

[59] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.

[60] *The Economic Impact of Counterfeiting and Piracy*, OECD, June 2008.

[61] UK IP Toolkit 2009.

[62] http://www.cti-us.com/CCAP.htm].

[63] www.wcoipm.org and http://ipmpromo.wcoomdpublications.org/.