EACO East African Communications Organisation

Communications for all in East Africa

FRAMEWORK FOR COMBATING THE IMPORTATION, SUPPLY AND USE OF COUNTERFEIT / SUBSTANDARD TERMINALS IN THE EACO MEMBER STATES

Prepared by EACO

July 2017

TABLE OF CONTENTS

1. INTRODUCTION

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 the OECD published a report that estimated, on the basis of customs seizures, that the total international trade in counterfeit and pirated goods (not including digital products or those produced and consumed domestically) accounted to more than US$200 billion in 2005. This estimate was updated on the basis of the growth and changing composition of international trade from just over US$100 billion in 2000 to US$250 billion for the year 2007, accounting for 1.95% of world trade. 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 $600 billion per annum.

In addition to counterfeit devices, there is also a proliferation of ICT equipment and accessories which are commonly known as “substandard”. Except for the fact that the equipment is different enough to avoid the ‘counterfeit’ label, a substandard device is essentially similar to a counterfeit device.

During the 18th EACO meeting held in Kigali, the Assembly of regulators resolved that all mobile operators should install an Equipment Identity Register (EIR) and that a Central Equipment Identity Register (CEIR) should be established to be used by all EACO Member states. Due to the high circulation of terminals without IMEIs or with multiple IMEIs in the region, the Assembly of operators also suggested that regulators should give them adequate time for migration and that they should provide policy guidelines to ban importation of mobile devices without IMEIs or with multiple IMEIs.

2. ABBREVIATIONS AND ACRONYMS

3GPP – 3rd Generation Partnership Project
CEIR - Central Equipment Identity Register
EIR - The Equipment Identity Register
ESN- Electronic Serial Numbers
GSMA- Groupe Speciale Mobile Association
IMEI - International Mobile Station Equipment Identity
IMSI- International Mobile Subscriber Identity
MSISDN – Mobile Station International Subscriber Directory Number

3. DEFINITION OF TERMS

1) 3GPP – 3rd Generation Partnership Project is collaboration between groups of telecommunications associations.

2) Central EIR - A Central Equipment Identity Register is a database of IMEI numbers of blacklisted handsets. If a device's ESN or IMEI number is listed on a CEIR, it is not supposed to work on member service providers' networks; only paying members may access the database.

3) EIR -The Equipment Identity Register. This is a database employed within mobile networks. It holds records for 3 types of mobile; namely black, grey and white. Besides, there is also a 4th category i.e. "Unknown". It is a tool to deny services or track problem equipment.

4) ESNs - Electronic Serial Numbers. Was created to uniquely identify mobile devices, ESNs are currently mainly used with CDMA phones (and were previously used by AMPS and TDMA phones), compared to International Mobile Equipment Identity

(IMEI) numbers used by all GSM phones. ESNs are often represented as either 11-digit decimal numbers or 8 digit hexadecimal numbers.

5) GSMA – Formed in 1995, the GSMA is an association of mobile operators and related companies devoted to supporting the standardizing, deployment and promotion of the GSM mobile telephone system.
6) IMEI – This is a unique 15 digit number given to every mobile phone, GSM modem or device with built-in phone / modem capabilities. Based on this number, you can check information about the device, e.g. brand or model.

7) IMSI - International Mobile Subscriber Identity. It is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the home location register (HLR) or as locally copied in the visitor location register. The IMSI is used in *any* mobile network that interconnects with other networks. For GSM, UMTS and LTE network, this number is provisioned in the SIM card and for CDMA2000 in the phone directly or in the R-UIM card (the CDMA2000 analogue to a SIM card for GSM).

8) MSISDN – Mobile Station International Subscriber Directory Number. This number includes a country code and a national destination code which identifies the subscriber’s operator. It is defined by the E.164 numbering plan

4. COUNTERFEIT / SUBSTANDARD DEVICES

4.1 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 does not however define the intention behind the use of the counterfeit trademark but 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.

4.2 SUBSTANDARD TERMINAL

Although there is not an ITU definition of Substandard ICT terminal, substandard is a category of ICT terminal that is sold in contravention of applicable national and international technical standards, conformity processes, as well as national regulatory requirements or other applicable legal requirements. In some cases the manufacturer may intend to deceive the purchaser into believing that he/she is buying conformant products. The product may or may not resemble an original brand.

There is a tendency to focus only on counterfeit ICT terminal when in fact substandard devices present the same societal challenges and indeed may actually be a bigger problem than counterfeits and substandard device distribution model may be more difficult to control than the counterfeit distribution model. Hence, it is important to focus on new and innovative ways to control this problem.

5. SCOPE

This framework provides guidelines to be adopted to ensure effective actions are taken to combat the importation, supply and use of counterfeit / substandard terminals in the EACO member states.

6. IMPACT OF COUNTERFEIT / SUBSTANDARD TERMINALS

Counterfeit / substandard terminals impact several players in different ways. These include the industry, consumers and governments as detailed below. Each of these sectors needs to respond uniquely to address the challenges in order to successfully eliminate counterfeit / substandard terminals.

6.1 INDUSTRY

Industry includes the manufacturers, network operators, distributors and the retailers among others.

1. Manufacturers of original devices invest huge sums of money in producing quality devices, only for these devices to get to the market and compete with the counterfeit/substandard devices.
2. Manufacturers of the counterfeit / substandard devices do not pay royalties to the owners of essential patents and copy rights.
3. Counterfeit/substandard mobile devices do not operate well, they are of low quality and they cause interference with the network. Studies have shown that such mobile devices fail receiving sensitivity tests and transmit performance requirements. Due to their poor performance, coverage by the mobile network is significantly reduced and therefore directly impacts on the quality of service provided by the mobile operators. This then pushes the industry/operator to deploy more base stations in a bid to solve this problem which is a costly venture.
4. Consumers will prefer to buy the counterfeit / substandard devices because they cost less and are intensively marketed. This directly impacts the industry involved in the supply chain of genuine terminals.

6.2 CONSUMERS

1. Counterfeit/substandard terminals have high levels of hazardous substances like ***lead*** on their internal and external components.
2. Counterfeit/substandard terminals have not been subjected to extensive testing (like audio safety, electromagnetic compatibility, low-voltage device safety) like it is for the legitimate/genuine terminals. These devices are not type approved and therefore they pose a very high safety risk to consumers.
3. Counterfeit/substandard terminals do not operate well, they are of low quality and they cause interference with the network. Studies have shown that such mobile devices fail

receiving sensitivity tests and transmit performance requirements. Consumers using these terminals receive poor services and are unable to achieve their expected return on investments.

4. Counterfeit / substandard terminals are sold without warranty; this denies the consumers the opportunity to have their devices replaced in the event that this is needed.
5. Counterfeit / substandard terminals can be easily used in crime. This is because these devices cannot be easily tracked.
6. Counterfeit / substandard terminals have a short life span and therefore become expensive to the consumer in the long run.

6.3 GOVERNMENTS

1. The governments lose huge sums of money in taxes because of these devices. These products gain entry into the market through informal routes and therefore dealers of these devices do not pay duties and taxes.
2. The existence of these devices has posed major challenges to the government's effort to create and enforce laws that govern this industry. This is because dealers of these devices do not follow any of these laws and it is not easy to crack them down.
3. The regulatory cost is inflated by the existence of the Counterfeits / substandard products as elaborated in the process above. More staff, man-hours and collaboration efforts is needed to just address these in order to safeguard the industry and assure Consumers of quality and protection from the associated harmful effects.
4. The life cycle of the counterfeit / substandard terminals is very short increasing the rate at which they are disposed off. This immensely contributes to accumulation of electronic waste which is a challenge to the environment.

7. FUNCTIONAL REQUIREMENTS

Combating counterfeit/substandard terminals in the region will require stopping importation of counterfeit/substandard terminals and elimination of counterfeit/substandard terminals already on the market and in use by consumers.

7.1 STOP IMPORTATION OF COUNTERFEIT/SUBSTANDARD TERMINALS

7.1.1 Proper implementation of the type approval process in all EACO member states

To ensure seamless and coordinated response, the framework proposes collaboration among all stakeholders (including the Revenue Authority, Bureau of standards, Manufacturers and Mobile network Operators) led by the ICT Regulatory authorities to not only reduce the cost of the exercise but also to ensure the consumers and importers of genuine terminals are protected.

1. The ICT regulatory authorities will define all the devices that require type approval before importation, sale and distribution into the EACO region.
2. The ICT regulatory authorities together with the bureaus of standards will define the standards on which the technical evaluation of the devices will be based.
3. Both parties will then determine whose responsibility it will be to carry out the technical evaluations of the equipment. This can be carried out at either party's laboratory or a third party can be designated to carry out the technical evaluations from the export country, before importation.
4. Certificate of type approval / Type Acceptance will be issued for the specific model of devices
5. Type approved/Accepted devices will possess an approval label provided by the regulatory authority and on importation, the bureau of standards and the revenue authority should confirm

6. Periodic inspection of the distributors and outlets on the market should be conducted to arrest and dissuade stocking and distribution of any products without an approval.

7.1.2 Acquire IMEI database from GSMA

The GSMA maintains a unique system known as the International Mobile Equipment Identity Database (IMEI), which is a global central database containing basic information on the unique serial numbers (IMEI) of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) in use across the world’s mobile networks. The IMEI number ranges are allocated by the GSMA to all manufacturers of 3GPP compliant devices to ensure that no two devices have the same IMEI.

In order to access the IMEI database, a membership to GSMA is required by regulators and mobile operators. This information should also be availed to importers and consumers so that they are able to check the IMEIs of the mobile devices before importation and purchase.

7.2 ELIMINATE COUNTERFEIT/SUBSTANDARD TERMINALS ALREADY ON THE MARKET

7.2.1 Acquire an SMS platform that will be used to interrogate the IMEI database

The regulatory authorities will need (they may identify a third party) to run anSMS based platform that will be used by the consumers to determine whether their terminals are genuine.

7.2.2 Awareness campaigns to the consumers.

These campaigns will educate the consumers on the dangers of using counterfeit / substandard terminals. They will also educate them on how to identify counterfeit / substandard terminals on the market.

7.2.3 The operators should have an Equipment Identity Register (EIR)

This will keep records of the IMEI of a mobile device and their matching IMSI used on that device. This system will pave way for monitoring counterfeit / substandard terminals.

The Turn Key Technical Solution is however preferred, where the operators do not need to purchase EIR but rather collaborate to make their networks available for integration.

7.2.4 Deny substandard/counterfeit terminals access to operators networks

The Regulatory authority together with the operators will determine the terminals that should not access the operator's networks and how to eliminate them in long run.

8. PROPOSED PRACTICAL MEASURES

This section highlights the processes that can be used to technically identify and eliminate counterfeit / substandard terminals in the EACO member states. This list is however not conclusive and further developments need to be exploited.

This is to ensure a standardized approach in the EACO member states using International standards, to provide practical methodology and best practices for use by the EACO member states and to avoid duplication and implementation challenges.

8.1 TYPE APPROVAL IMPLEMENTATION

8.1.1 Implementation Concept

To ensure seamless and coordinated response, the framework proposes collaboration among all stakeholders (including the Revenue Authority, Bureau of standards, Manufacturers and Mobile network Operators) led by the ICT Regulatory authorities. This will ensure synergy that will ultimately reduce the cost of the exercise and also ensure that the consumers and dealers of genuine terminals are protected.

1. The ICT regulatory authorities will define all the devices that require type approval before importation, sale and distribution into the region.
2. The ICT regulatory authorities together with the bureaus of standards will define the standards on which the technical evaluation of the devices will be based.

3. Both parties will then determine whose responsibility it will be to carry out the technical evaluations of the equipment. This can be carried out at either party’s laboratory or a third party can be designated to carry out the technical evaluations from the export country, before importation.
4. Certificate of type approval / Type Acceptance will be issued for the specific model of devices
5. Type approved/Accepted devices will possess an approval label provided by the regulatory authority and on importation, the bureau of standards and the revenue authority should confirm
6. Periodic inspection of the distributors and outlets on the market should be contacted to arrest and dissuade stocking and distribution of any products without an approval.

8.1.2 Challenges

1. Some of the expected country standards do not have international benchmarks.
2. The cost of the type approval process is high giving room for alternative ways of skipping the process
3. The type approval process takes long yet the demand for these certificates is normally urgent.
4. The countries do not have test centers to carry technical assessment of the equipment and those that are available are ill equipped.
5. Improper implementation of the proposed procedures by some countries. Processes are not fully followed and the time of implementation is different making it possible for counterfeit / substandard terminal dealers to relocate their activities.

8.2 Equipment Identity Register (EIR) Implementation

8.2.1 Implementation concept

EIR is a database employed within mobile networks, which is able to match every IMSI to the IMEI of every device on which it is used and keep records.

The information from this database may then be provided to the authorities as required. Mandating all operators to have this EIR database will pave way for the implementation of the system for monitoring counterfeit / substandard terminals and related records.

The EIR implementation should be done through memorandum of understanding between ICT regulators and network operators. This may be supported by Acts and Regulations.

Individual operator EIRs will however not prevent Cloning of Devices, hence it is inefficient in addressing the main challenge given that most counterfeit and substandard devices have their IMEI Cloned, and constitute a very high percentage of the existing local market.

8.2.2 Challenges

1. The implementation of EIR requires the network operators a considerable investment
2. The process of developing the EIR database may take a long time to achieve required accuracy and completeness.
3. Membership to GSMA must be maintained.
4. Handsets with duplicate / cloned IMEIs are cannot be stopped with this solution.

The Turn-Key Technical solution would work well as an alternative to the EIR database. This solution allows a particular MSISDN/IMSI to be locked to a specific IMEI or vice versa. A given IMEI can also be authorized but not locked to any MSISDN; notification SMS is sent to the subscriber.

The turn-key solution allows for implementation of various device locking rules as listed below:

1. **Lock type 1**: A particular MSISDN/IMSI and a particular IMEI are locked to each other, therefore, that MSSISDN can only use the device of the specified IMEI
2. **Lock type 2:** A given IMEI can be locked to a specific MSISDN/IMSI, but the MSISDN/IMSI can be used with any other IMEI.
3. **Lock type 3:** A given IMSI/MSISDN can be locked to a specific IMEI, but the IMEI can be used by any subscriber (IMSI/MSISDN).

8.3 IMEI Interrogation on the GSMA Database

8.3.1 Implementation concept

The IMEI is a unique 15 digit number in-built in every mobile device. Based on this number, you can check information about the device, e.g. brand or model.

The GSMA maintains the IMEI Database, which is a global central database containing basic information on the unique serial numbers (IMEI) of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) in use across the world's mobile networks. The IMEI number ranges are allocated by the GSMA to all manufacturers of 3GPP compliant devices to ensure that no two devices have the same IMEI.

In order to access the IMEI database, a membership to GSMA is required by regulators and mobile operators. This information should also be availed to importers and consumers so that they are able to check the IMEIs of the mobile devices before importation and purchase.

The interrogation of the database is done via an SMS platform e.g. 1555 short code (for Kenya) which the customer IMEI will be sent to and an automatic feedback is given confirming the type and make of the handset. If this is different, then the handset is most likely counterfeited.

8.3.2 Challenges

1. The GSMA database is only accessed via subscription, therefore, access is limited to only those with paid up membership.
2. The SMS platform for interrogating the GSMA database is an added cost to the user.
3. There is continuous need to educate consumers on use of the SMS platform and IMEI identification for their handsets (*#06# for IMEI).
4. Handsets with duplicate / cloned IMEIs are difficult to verify authenticity.

8.4 IMPLEMENTATION OF IMSI

8.4.1 Implementation concept

The IMSI is a unique identification of the cellular network and is associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the Home Location Register (HLR) or as locally copied in the visitor location register. The IMSI is used in any mobile network that interconnects with other networks. For GSM, UMTS and LTE networks, this number is provisioned in the SIM card and for CDMA2000, it is in the phone directly or in the R-UIM card (the CDMA2000 analogue to a SIM card for GSM).

The IMSI is vital in combating counterfeit / substandard terminals usage as it will provide information on the network operator involved and the SIM card / R-UIM card holder including location. This may work hand in hand with the SIM / R-UIM card registration that captures details of the subscribers.

8.4.2 Challenges

1. Mandatory SIM / R-UIM card registration is not yet fully implemented in all EACO member states.
2. It is still possible for fraudsters to access SIM / R-UIM cards with invalid information which makes it difficult to trace them.
3. IMSI is considered private and confidential by operators and may lead to legal challenges in terms of access.

8.5 TRIPLE-PLAY APPROACH

This is the latest approach to combating counterfeit / substandard terminals. It combines the use of the IMEI, IMSI and MSISDN. If the characteristics of the terminal do not match, the IMSI is marked as using a cloned IMEI. The Mobile Network Operator in collaboration with the government can block the IMSI or send a notification to the mobile user

Even though the Triple-play approach is an intensive and lengthy process that should be used as a second phase in combating counterfeit / substandard terminals, it is the most successful approach in stopping duplicate and cloned IMEIs.(This system is being implemented in Ethiopia, a first of its kind in Africa.)

Given that the Triple-Play approach requires IMEI Registration, it also combines many other benefits, including but not limited to:

- Full exhaustive database of all IMEIs in the country/region that can be integrated to SIM-Card registration system, for full tracking and security (e.g. in Sri-Lanka)
- Stimulating genuine device distributors to invest in the country where this is implemented since the Governments can guarantee exclusive distribution rights.
- Since random IMEIs will not be able to function, (unless registered), SIM-Boxes, which use random IMEIs will hence not function, contributing greatly to the quality of international calls, and increasing related revenues to the state.
- Such a system is centralised and will also make device theft an issue of the past as any device can be tracked / blocked on all mobile networks.
- Such a system can be integrated to the Customs networks and enable enforcement of Tax collection. This can be a tool for the Governments to increase their tax collection base and move towards modernization of the existing taxation structure for example lowering the tax percentage but enforcing its collection.
- With Triple-Play, taxation can also be made more specific to certain device types (e.g. luxury smart phones can have different and higher tax rates, also e-learning IMEI devices could be exempt from taxation)
- With the Triple-Play, Governments can subsidize the cost of genuine terminals to make them more affordable by the consumers.
- Device smuggling could also be combated with this system.

Triple-Play National systems can then be integrated into a Regional EACO IMEI Database to fight against cross border dealings in illegal devices, and hence stopping the actual crime network of outlaws behind these illegal activities.

8.5.1 Challenges

1. Until recently, Triple-play was an expensive venture and needs close collaboration among stake holders. A new market survey of suppliers is needed to compare costs.
2. Detailed technical expertise is required to implement Triple-play

8.6 DISCONNECTION PROCESS

The disconnection process will require a joint decision from the mobile network operators and the ICT regulators. This process will be enabled by the use of the Equipment Identity Register. All data from Mobile Network Operators' EIR will be checked against the IMEI database from GSMA. IMEIs that do not match those listed in the GSMA database will be blacklisted as counterfeit / substandard. A third party can be appointed by the ICT regulator to be in charge of checking the IMEIs received from the Mobile Network Operators against the IMEI database from GSMA.

The ICT regulator will then authorize the Mobile network operators to deny network access to these devices.

8.7 RISK ANALYSIS AND RESPONSIBILITY MATRIX

8.7.1 Risk Analysis

1. Competing political, commercial and technical interests make the process complicated.
2. Consumers are not keen on acquiring and using genuine terminals. Their main consideration is cost.

8.7.2 Responsibility Matrix

1. The Governments need to subsidize the cost of genuine terminals to make them affordable by the consumers.
2. The Governments need to ensure collaboration among the stakeholders is sustained and legalized.

3. The Governments must ensure that there is public awareness
4. The Governments must invest into training technical personnel to provide the necessary skills

9. PUBLIC AWARENESS CAMPAIGN PLAN

The public awareness campaign should be implemented in line with the EACO guidelines on Consumer Education.

10. LEGAL FRAMEWORK

The proposed framework should be implemented in due consideration to the unique existing national laws, sectoral laws, acts, regulations and policies. The framework shall be implemented by the ICT Regulatory authorities in each EACO member state.

ANNEX I: CURRENT SITUATION IN THE EACO MEMBER STATES

In regards to the resolution of the EACO Assemblies, Regulators from EACO member states have embarked on the ban/elimination/ prevention of the use of counterfeit / substandard terminals. In Kenya, The Communications Commission (CCK), in collaboration with other stakeholders and operators, has to some extent managed to disconnect and ban counterfeit/substandard mobile devices. Tanzania has implemented the type approval process and has also embarked on awareness campaigns in this regard while Uganda procured equipment for type approval though it is not yet operational. Rwanda has implemented a type approval procedure and is also engaged in addressing counterfeit / substandard terminals using the GSMA database. Burundi is evaluating a technical supplier to implement a nationwide IMEI Database, without requiring operators to purchase EIRs.

Clearly there are different approaches and levels attained in each country and therefore there is a need for a common approach and framework to ensure success in the whole region.

UGANDA

A working committee composed of representatives from all licensed telecommunications operators and the Uganda Communications Commission (UCC) was formed to come up with a solution for the counterfeit/substandard terminals in Uganda.

This working committee proposed that equipment capable of identifying and monitoring fake and/or cloned IMEI's on the networks of all operators in Uganda be purchased.

The equipment has already been purchased and it has the added functionality of being able to deny devices with fake and/or cloned IMEI's access to operator networks.

The equipment is being housed at the Uganda Communications Commission and once the law to this effect is approved, the equipment will be operational.

TANZANIA

Tanzania has put in place the Tanzania Communications TYPE APPROVAL OF ELECTRONIC COMMUNICATIONS EQUIPMENT Regulations, 2005. This regulation requires all electronic communications equipment used to connect or access the public operating electronic communication networks and all wireless communications equipment to be type approved by the Tanzania Communications Regulatory Authority (TCRA) before they are imported into Tanzania. In addition Tanzania also uses the Electronic and Postal Communications Act number 3 of 2010, provision 82 of the act,1- 2 (b). The type approval test is used to check the compatibility of the all electronic communications equipment with any operating electronic communication network.

The Tanzania Regulatory Communications Authority (TCRA) also conducts inspections (enforcement) in the Tanzania Market to make sure that all the electronic and communication equipment being sold meet the standards set out by the Authority.

The Authority is still open to more ideas on how to effectively curb the importation and use of counterfeit/substandard electronic communications equipment.

KENYA

In Kenya, laws related to counterfeit goods are already in place, that is, Section 32 of Anti-Counterfeit Act, 2008 which states that, it is an offence to possess or trade in counterfeit goods e.g. mobile handset and Section 3 of The Kenya Information and Communications Type Approval Regulations, 2010 which states that all mobile handsets must be type approved by the Communications Commission of Kenya (CCK). These laws have therefore given the Commission the powers it requires to deal with the counterfeit / substandard terminals.

Collaboration was established between the Communications Commission of Kenya (CCK) and the Anti-Counterfeit Agency, Kenya Revenue Authority (KRA), Kenya Bureau of Standards (KEBS), Security Agencies, GSMA, Handset manufacturers, Mobile operators and the Consumer organisations.

The Anti-Counterfeit Agency inspects the traders of handsets, KRA and KEBS check entry of counterfeit mobile devices at border points, Security agencies enforce laws on counterfeits, GSMA provides the IMEI database, the handset manufacturers pay for the SMS service (1555 short code), the mobile operators switch off counterfeit handsets as advised by the

Communications Commission of Kenya and the Consumer organisations ensure that the consumer rights are protected in the process

Post Implementation Challenges

1. Discovery of numerous devices operating on the GSM networks with duplicate/cloned IMEIs. This makes it difficult to identify the counterfeited terminal.
2. Genuine IMEIs have also been embedded on counterfeit handsets resulting in counterfeit handsets being sold to the public as genuine handsets
3. Slow contributions by handset manufacturers to finance the sms service (1555 short code)

With the above mentioned challenges, the Communications Commission has planned to benchmark with Administrations that have successfully implemented the triple-play **(**combines IMEI, IMSI and MSISDN: If the capabilities don't match, the IMSI is marked as using a cloned IMEI. Mobile Network Operators can block the IMSI or send a notification to the mobile user**)** approach to counterfeit elimination successfully. There was also a second phase of counterfeit handsets switch-off to eliminate counterfeit handsets with cloned IMEIs after further interrogation. The Commission is also sharing the data resident in Equipment Identity Registers (EIR) between Mobile Network Operators within the region and beyond.

Kenya, like Tanzania has also established the Communications TYPE APPROVAL OF ELECTRONIC COMMUNICATIONS EQUIPMENT Regulations, 2010 which requires all electronic communications equipment used to connect or access the public operating electronic communication networks and all wireless communications equipment to be type approved by the Communications Commission of Kenya (CCK) before they are imported into the country.

The link to Type Approval Regulations is given below;
http://www.cck.go.ke/regulations/downloads/xImportationx_Type_Approval_and_Distribution_of_Communications_Equipmentx_Regulationsx_2010.pdf

The Communications Commission of Kenya (CCK) also conducts inspections (enforcement) on the Kenyan Market to make sure that all the ICT electronic and communication equipment being sold and installed meet the standards set out.

RWANDA

In Rwanda, the Law governing telecommunication especially in its article 42, forbids any natural person or entity to import, supply, (whether for sale or rent, loan or gift), connect, or allow to remain connected to a telecommunications network, or put into service any item of terminal equipment which does not comply with RURA type approval requirements, however these devices are being connected to operators' network through unofficial means.

RURA has implemented type approval as a measure of minimizing importation of counterfeit / substandard terminals. To specifically eliminate counterfeit the authority is currently in the process of acquiring an SMS platform to interrogate the GSMA database to confirm if the terminals are genuine or counterfeited.

BURUNDI

In Burundi, laws related to approve equipment are already in place, that is, DecreeNo.1/011 of 1997 September 4 on organic provisions on telecommunications Article 27: The purchase of approved terminal equipment is free.

However, they cannot be connected to a public network without the prior approval by the ARCT. This approval is required in all cases for radio facilities, whether or not intended to be connected to a public network. The accreditation is to ensure compliance with the essential requirements and interoperability defined in paragraphs 20 and 21 of Chapter. Article 29:Terminal equipment or facilities subject to the approval referred to in Article27can not be manufactured for the domestic market, imported for release for consumption, held for sale, sold, distributed free or not connected to the public network or be advertised if they were the subject of approval

Any subsequent changes must be approved DecreeNo.100/97 of 2014 April,18 laying down the operating conditions of the electronic communications sector Article 17:The manufacture, import, editing and export of electronic communications equipment are subject to prior authorization from the ARCT.

Such equipment must first be approved by the 1'ARCT services. ′Article 18: The purchase of approved terminal equipment is free. However, they cannot be connected to a public network without the prior approval of 1'ARCT. As of 2014, May 30, a national workshop was organized on the management of terminals connectable to the network. The workshop was attended by the regulator, operators, and vendors of mobile devices, the media and civil society.

The ARCT has identified a technical partner in charge of setting up a solution to fight against the use of counterfeit and substandard devices and users who do not pay taxes. The Triple-play approach has been suggested as a probable solution.

A study of technical and financial feasibility has been given to the ARCT for consideration before signing a contract with the solutions provider.