Device Identification, Registration and Blocking System (DIRBS)

CONSULTATION DOCUMENT

Table of Contents

1. Introduction:

The already very vibrant telecom sector of Pakistan has experienced tremendous smartphone growth with the introduction of 3G and 4G networks. There is a strong influx of mobile devices being imported into the country, however, there remains a significant issue with grey market and counterfeit devices impacting Government, Mobile Network Operators, OEMs/Distributors and Consumers.

At a government level, there is loss in revenue due to import tax evasion as well as public security is potentially endangered from non-registered devices. From an OEM/Distributor industry perspective, counterfeit and grey market devices pave the way for unfair competition, resulting in lost sales, pricing pressure, and impact to brand equity. With counterfeit devices, end users face degraded performance issues and potential health hazards.

International Mobile Equipment Identity (IMEI) is a unique identification code for each mobile device allocated by GSMA. The IMEI is a 15 digit number that is used to identify the device. The IMEI also reveals the manufacturer, make & model, type approval details and country of production. The Equipment Identity Register (EIR) is a database located within the Network Operation Control (NOC) of mobile network operators, that contains a record of all the mobile devices that are allowed in a network as well as database of all equipment that is blocked, e.g. because it is reported lost or stolen. The identity of the mobile station is given by the International Mobile Equipment Identity (IMEI). Each time a call is made, the MSC requests the IMEI of the mobile station, which is then sent to the EIR for authorization. The use of genuine IMEI along with other processes/systems such as type approval, EIR and the one proposed in this document ensures a healthy mobile eco-system.

The Government of Pakistan (GoP) has recently introduced Telecom Policy 2015 in line with modern day technological evolution and current telecom requirements of consumers. To overcome the issues of counterfeit and illegal devices and it negative repercussions, the Pakistan Telecommunications Authority (PTA) in line with the Telecom Policy 2015 objectives has proposed a system called Device Identification, Registration and Blocking System (DIRBS). The system will use IMEI of device along with other parameters and help in identifying, monitoring and regulating such devices. DIRBS will have capability to help identify counterfeit and illegally imported mobile devices that avoid collection of tax

revenues, contribute towards security issues, and negatively impact both end users and MNOs in Pakistan. As per Section 9.6 of Telecommunication Policy 2015, GoP has mandated the PTA to develop a regulatory framework for clauses 9.6.1.-9.6.4 in consultation with all relevant stakeholders and this document seeks the advice and comments of all stakeholders specially MNOs, OEMs/Distributors and Consumers.

2. Scope of Work:

The defined scope of work within the DIRBS project will be to develop a framework in consultation with all relevant stakeholders and follow the spirit of National Telecom Policy 2015 with the following objectives:

- ***Terminal equipment identification and approval***
    - Terminal equipment with SIM functionality must have a valid and unique IMEI or equivalent identifier.
    - All parties wishing to import SIM based devices commercially into the territory of Pakistan must have a valid GSMA Type Access Code (Tac) for the model being configured and use IMEI values containing that TAC.
    - Mobile Network Operators (MNOs) will disallow registration of new terminal equipment with un-authenticated DIRBS IMEI/invalid identifiers on their networks.
    - End users and retailers should verify IMEI validity.
    - Terminal equipment imported into the country must be type approved by PTA.
- ***Stolen terminal equipment handling***
    - PTA within the framework will introduce a mechanism that will allow for OEMs, Operators to report to PTA any business identified as source of stolen devices.
    - Mobile Network Operators (MNO)'s will report to PTA any devices latched on to their network and reported/identified as stolen.
    - MNOs will block stolen terminal equipment once reported.

DIRBS will enable identification and blocking of these illegal/invalid devices in the market and active on MNO networks with the help of MNOs/OEMs and Consumers. It shall facilitate importers of legitimate devices to continue import of genuine mobile devices through legal import channels.

Illegal/invalid devices include:

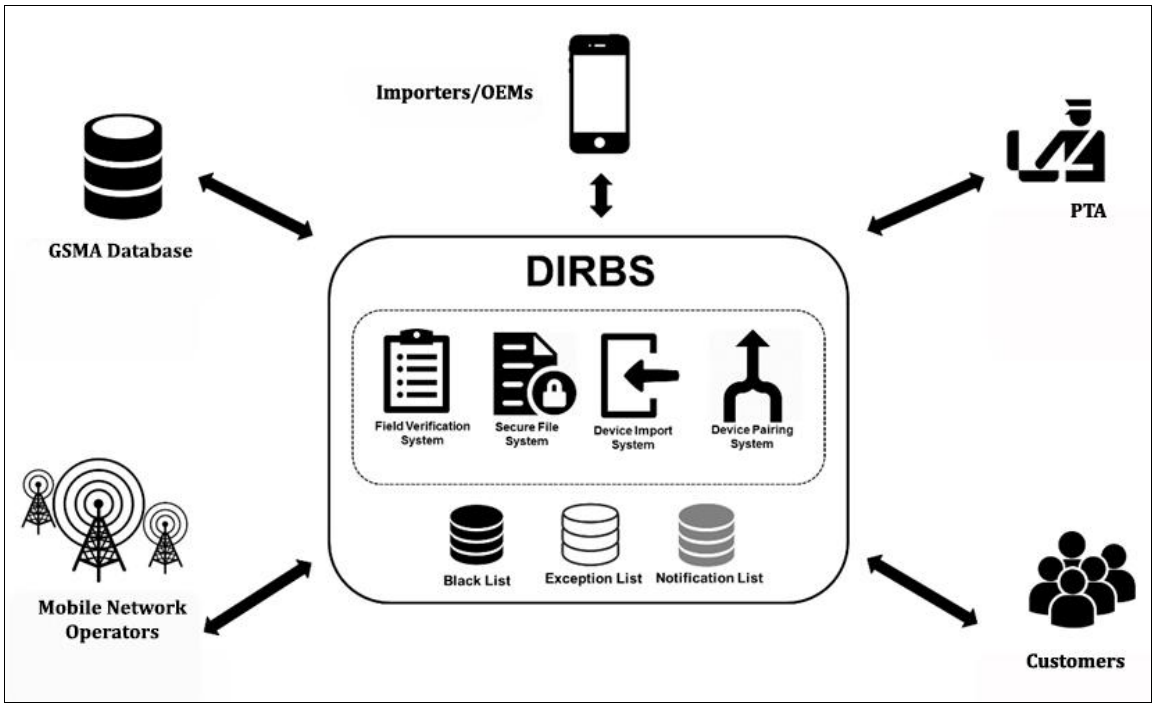
- Counterfeit devices (replicas of official OEMs' original devices).
- Illegally imported devices (import tax not paid).
- Devices with invalid IMEIs (IMEIs not assigned by GSMA).
- Devices with duplicate IMEIs (multiple devices with same IMEI).
- Devices reported as stolen/lost (reported locally in Pakistan and globally to GSMA).

DIRBS will enhance GoP revenue by allowing devices imported through proper channel. DIRBS will not only monitor devices being brought into the country in the future, but will also check the installed base of devices currently active or being sold in the channel. Devices identified as illegal/invalid will be mapped to notification or blacklist per classification rules to be defined by PTA explain in the later sections.

In short, DIRBS and its successful implementation will benefit the entire mobile ecosystem in Pakistan.

3. DIRBS Overview:

DIRBS comprises a core analysis system combined with subsystems to support verification of IMEIs by stakeholders, registration of IMEI paired exceptions, and import of various inputs including operator device data dumps, GSMA device database, importer device lists, and stolen device lists. Analysis performed by DIRBS will allow the identification and tracking of illegal/invalid devices according to rules and guidelines to be defined by PTA in consultation with the stakeholders.



DIRBS will generate three lists: black, exception and notification list. These lists will be provided to MNOs periodically so that they take appropriate actions on them.

3.1 Black list

The blacklist is a list of IMEIs to be blocked. IMEIs may be present on the blacklist for one or more reasons including the following:

- IMEI is reported stolen/lost according to PTA (local stolen list).
- IMEI is reported stolen/lost according to GSMA (global stolen list).
- IMEI is invalid and has expired from notification list.
- IMEI is a duplicate and has expired from notification list.

3.2 Notification list

Notification lists are used to indicate devices with certain problems. IMEIs may be present on a notification list for one or more reasons including the following:

- IMEI has not passed PTA type approval.
- IMEI has not been reported on any import list.
- IMEI is invalid (IMEIs not assigned by GSMA).
- IMEI is a duplicate (multiple devices with same IMEI).

IMEIs on a notification list are provided along with the subscription with which they were observed. This allows the operator to contact the user of the device in order to attempt and resolve the issue. Separate notification lists would be provided for each operator consisting of only pairings involving their respective subscribers. Upon receipt of a notification list, the MNO should contact their subscriber to resolve the device issue before it expires onto the blacklist.

3.3 Exceptions list

Exception List is a list of IMEIs to be operational on the network. This list contains specific IMEI-subscription pairings that are allowed to continue receiving service even if their IMEI appears to qualify initially to be on the notification list. Entries in this list are added via “Device Pairing Interface” by the MNOs. IMEI may be present on the exception list for one of the following reasons.

- Devices with valid IMEIs (known to GSMA)
- Paired IMEIs (user CNIC with IMSI/MSISDN)
- PTA type approved IMEIs
- Legal Import list IMEIs

Upon receipt of black and exceptions lists, MNOs must update their Equipment Identity Registers (EIRs) per these lists. After update, any device with an IMEI on the blacklist will be prevented from accessing the network unless the specific IMEI-subscription pairing for that device was on the exceptions list. Note that operator EIRs must support this ability to block blacklisted devices based on IMEI and override such blocking for specific IMEI-subscription pairs.

3.4 Guests Devices Registration

DIRBS will give an option to the guests/visitors entering the country to register their own devices in the system. Guest devices with valid IMEIs will be registered in the system for the designated period of time. The device will be registered using identity number (ID card or Passport) and other personal details and will be added to the notification list. Guests will be notified during the period about the remaining duration. After the deadline, these devices will be blocked from being operational on any mobile network operator.

4. DIRBS Support Sub-Systems/Interfaces:

DIRBS will have APIs supporting the following system interfaces to provide relevant stakeholder with pre-defined access through web and mobile application to either read/write/upload/download information to/from DIRBS.

4.1 Device Import Interface

The Device Import Interface support sub-system provides a web interface to OEMs/Importers to add IMEIs and information of devices to be imported. Importer will need to get single-use approval code from PTA to add new list. Once approved by PTA as per its Type Approval process and cleared by Pakistan Customs as custom cleared, these devices are added to the import list.

4.2 Field Verification Interface

The Field Verification Interface support sub-system that provides a web interface and application for stakeholders (PTA, Federal Bureau of Revenue & its Allied departments such as Pakistan Customs, Retailors/Distributors, OEMs and Consumers) to verify the status of a device. Such tools could enable the verification at time of import, in the distribution channel, or at point of sale/purchase. This system will check IMEI queries against DIRBS lists to provide accurate information to users. Different access levels will be provided to stakeholders such as PTA, FBR, Importers/Retailers, OEMs and Consumers.

- PTA will be able to view complete record of IMEI.
- Retailors/Distributors, OEMs and Consumers will only be able to check device authenticity.

4.3 Secure File Interface

The Secure File Support Sub-System provides a secure interface for mobile network operators to upload device dumps in predefined format. The recommended format and guidelines for the device dumps are provided in the annexure-A. These dumps are kept secure and go into DIRBS as input for analysis.

4.4 Device Pairing Interface

The Device Pairing support Sub-system provides a web interface to assist operators with IMEI-subscription pairing for device regularization. Once a customer's MSISDNs has been verified as registered against their CNIC and deemed allowable by PTA, pairings are added to the exceptions list.

5. Development Strategy:

DIRBS system is planned to be implemented in multiple phases with core functionality being introduced in phase 1 and incremental functionality being introduced in later phases. Initial phases are defined in the following subsections in the context of inputs and outputs.

5.1 Phase-1

Phase 1 will include mapping and identification of devices, including blocking of stolen devices and awareness campaign. Devices with invalid IMEIs (IMEIs not assigned by GSMA) will be treated as per PTA directive.

In this phase, the system will begin generating lists discussed above; however it is planned that only stolen devices would be immediately blacklisted during the initial phase with blocking of other illegal device to begin in Phase-2.

Awareness campaign is of key importance to the success of DIRBS and ensures that all the stakeholders i.e. MNOs, OEMs their distributors/retailers and consumers understands the goals and benefits of the solution and the system. The campaign to be run in collaboration with all business stakeholders such as MNOs & OEMs will inform all concerns about both the presence of illegal/invalid devices and the problems associated with such devices. Consumers will be informed by the PTA. FBR, MNOs, and

OEMs/Importers via regular advertisements and SMS. The awareness campaign should include workshops, seminars, and both Above- and Below-The-Line (ATL & BTL) promotions.

5.2 Phase-2

Phase 2 introduces more visibility into legally imported and type approved devices as well as service-based duplicate detection thus curbing device smuggling. It is during this phase that standard blocking is planned to occur and additions to the exceptions list (allowed to operate on network) are expected to be substantially reduced. More advanced functionality will also be added, such as service based clone detection and multiple SIM device identification. It is during this phase that full blocking is planned to be supported.

6. Stakeholder Roles and Responsibilities:

6.1 OEMs and Importers

OEMs and Importers will provide the list of devices they are importing into the country with all the details regarding device specifications, including the number of SIM slots support and range of device IMEIs being imported etc. An online system will be made available to them for providing the following information in order to streamline and facilitate this process. The information required will generally include the following:

Field	Format Information
Brand	Contains brand/OEM name of a device
Model	Particular model name of the brand mentioned above
IMEI Range	Range of Device IMEIs being imported e.g. “872256488913450” – “872256488913800”
Total IMEIs	Total number of IMEIs being imported e.g. “350”
Device SIM(s) Capacity	SIM capacity of a device i.e. whether “Single SIM” or “Dual SIM”
Number of Devices	Total number of devices being imported e.g. “175”

6.2 Pakistan Telecommunications Authority (PTA)

As a regulator, PTA has a core responsibility to regulate and manage the entire DIRBS and the activities around project. It shall coordinate with all stakeholders and ensure that each provide the following inputs for DIRBS accurately and on time:

- Import lists
- GSMA TAC database
- GSMA global stolen list
- Exceptions list
- Local stolen list
- Administration/configuration
- Audit/enforcement of blacklist
- Awareness campaigns

In addition, it is of vital importance that PTA ensure MNOs provide timely predefined device dumps (Guidelines for MNOs provided as Annexure-A) as input required for DIRBS using the “Secure File Interface”.

PTA shall make available the following reports as an output of DIRBS for the benefit of all stakeholders:

- Country report to be displayed on its website for public/consumer interest.
- Operator reports to be sent to respective operators only.

PTA will manage and install the required hardware, software and infrastructure through its own resources. Additionally, it shall manage the operation and maintenance of the Hardware, Software and Infrastructure for the entire project excluding any upgradation of MNOs EIR or any facility/system if required at MNO or OEM/Distributors side.

6.3 Mobile Network Operators (MNOs)

As key members of the ecosystem, MNOs will have to do the following:

- Upload pre-defined device dumps (Detailed Guidlines provided in Annexure-A) through secure system at the requested interval.
- Update their EIR provisioning with provided exception and blacklists to ensure blocking of illegal devices.
- Notify customers who are on notification list to resolve device issues.
- Provide facility and support to customers for pairing devices via the "*Device Pairing Interface".*
- Prepare and Launch awareness campaign for consumers.

Each operator will upload a data dump periodically (e.g. weekly) to DIRBS using the "Secure File Interface". This format generally consists of the following fields (Detailed Guidelines provided in Annexure-A). These fields are available from output CDRs and must be aggregated using "GROUP BY" such that every unique combination of these fields is reported. Blank and missing fields are to be considered as distinct values and included as such.

Field	CDR source field and format information
Date	• Format: YYYYMMDD (e.g. 20150423). Converted from date portion of: ○ Seizure Time / Answer Time (Record Types 0, 1, 87) ○ Event Timestamp (Record Types 6-7, 21-23, 25, 28, 93-94, and IMEI Observation Ticket) ○ Record Opening Time (Record Types 18, 20, 84-85, 96)
IMEI	• "Served IMEI"
IMSI	• "Originator IMSI" (Record Type 93) or "Recipient IMSI" (Record Type 94)

	• "Served IMSI" (otherwise)
MSISDN	• "Originator MSISDN" (Record Type 93) or "Recipient MSISDN" (Record Type 94) • "Served MSISDN" (otherwise)

6.4 FBR/Pakistan Customs

FBR/Pakistan Customs can verify devices being imported and update the number of actual devices imported by each importer. FBR/Pakistan Customs can confirm these devices legality through the "Field Verification Interface".

7. Overview of InternationalBest Practices:

Different countries have introduced or launched similar systems in order to prevent their countries from the negative impact of illegal and counterfeit devices. In order for their systems to function properly these systems were accompanied by appropriate regulatory frameworks for their licensees (Operators, Importers, and OEMs) and consumers to follow that ensured it cleans up their networks from fake devices. The following sections provide information/overview of similar systems being implemented and operational by various countries around the world.

7.1 Malaysia

Malaysian Regulatory Authority has implemented a system called MCEIR. Purpose of the implemented system was to handle the lost/stolen devices by maintaining a central repository for the reported devices. MCEIR is connected to EIR for transmission of blocking/unblocking requests.

Devices that are reported stolen/lost are updated to MCEIR and gradually updated to EIR. The system is responsible to block and unblock the reported devices.

The relevant Licensees will carry out necessary end user verification to ensure the authenticity of generated request. User who request the device blocking has been given the authority to unblock it (in case of device recovery). This is to avoid fraudulent blocking and unblocking.

7.2 Azerbaijan

In 2011, The Mobile Devices Registration System also referred as MDRS was established in the Information Computer Center (ICC) of the Ministry of Communications and Information Technologies in accordance with the "Rules of Mobile Devices Registration".

Main purpose of this system was to not only prevent the import of low-quality devices with unknown origin that do not meet the required technical standards (limiting the emission of harmful electromagnetic radiation) but also to increase the recognition and competitiveness of manufacturing companies. MDRS makes sure lost/stolen mobile devices along with those illegally imported into the country are prevented from use on the networks.

Since 1st March 2013, a registry of IMEIs (active in Azerbaijan) is maintained by MNOs on daily basis. Prior to the launch of MDRS, IMEIs used in the network were considered as registered and therefore operate freely on the networks. After the implementation of MDRS, IMEIs of imported devices (used by private users on local networks) should be registered within 30 days of the date of its connection to the network. This rule is not applicable to roaming mobile devices (used by private user with foreign network connection). Subscribers can check their device's legitimacy either through a webpage i.e. imei.az or by sending SMS to the particular operator.

7.3 Sri Lanka

In March 2013, the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) expressed their interest to "Design, Develop, and Install Central Equipment Identity Register (CEIR) for Mobile Networks in Sri Lanka.

Main aim of TRCSL was to restrict the usage of counterfeit devices, discourage mobile phone theft and protect consumer interests. TRCSL implemented a Central Equipment Identify Register (CEIR) that

connects to the EIRs of all the mobile operators. This enabled blacklisted devices to remain blocked on all the mobile networks.

7.4 Columbia

To control the marketing and sales of both new and used terminal devices, the Ministry of Information and Communication Technologies issued Decree 1630 in 2011. For this purpose two types of centralized databases were created.

- A registry of the IMEI numbers of stolen/lost terminal devices (preventing their use or activation).
- A registry of IMEI numbers of legally imported or manufactured terminal devices in the country. These IMEIswere paired with an identification number of the owner or subscriber.

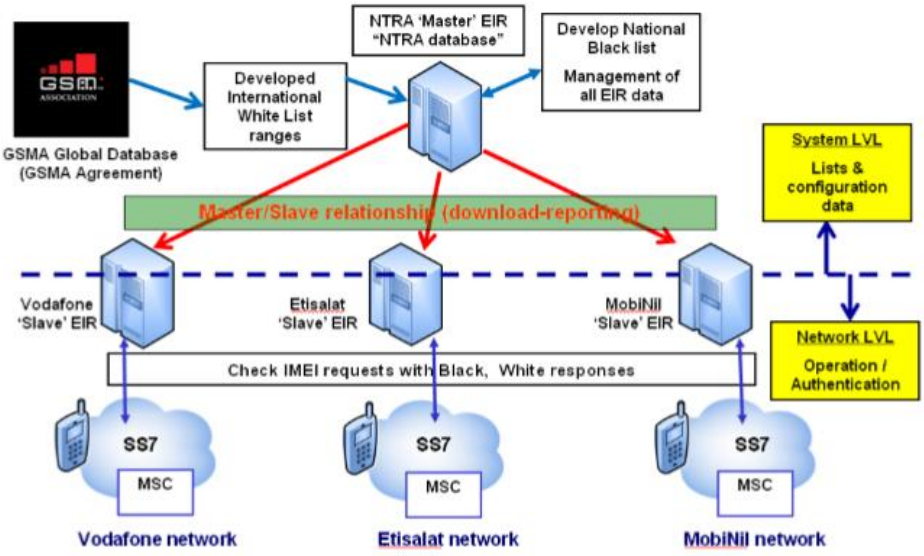
Furthermore, those who tamper with, reprogram, re-label, modify the IMEI or reactivate stolen mobile device are to be sentenced for 6 to 8 years imprisonment under Law 1453 on Citizen Security. In addition, altered equipment is confiscated.

These initiatives not only controlled the sale and use of stolen mobile devices but have also helped in reducing the use of counterfeit products.

7.5 Egypt

To support the Type Approval activities, a market surveillance department was established in 2008 by National Telecommunication Regulatory Authority (NTRA). In 2010, Egypt adopted the system to combat the use of counterfeit devices. GSMA IMEI database and the TAC White list was used to maintain a CEIR-IMEI database.

The system was implemented to restrict the use of Illegal, Fake, Null and Duplicate IMEIs as well as stolen devices.



IMEI database solution in Egypt

7.6 United Arabs Emirates

In UAE, the use, sale, purchase, distribution and promotion of fake devices is prohibited as per the UAE's Telecom Laws. Telecom Regulatory Authority is responsible for taking necessary steps to ensure the implementation of Laws against usage of such devices. Laws are made to tackle with persons involved in usage of such devices.

In 2011, TRA launched a campaign to create awareness and to discourage usage of fake mobile phones in UAE. It was announced that devices having fraudulent IMEIs would be ceased on the network within UAE. Advertisement were given for awareness of the people about the ban on counterfeit devices.

An SMS service was launched through which the customers were able to check the status of their device. During the awareness program consumer were informed about the side effects of using such devices. MNOs were also made responsible to inform their customers about devices status and in case of fake IMEIs, the customers were disconnected from the network.

Customers were also informed about the side effects of usage of such devices: the health hazards related to low quality fake devices, battery leakages/explosions and highly corrosive and poisonous chemicals in batteries. An ultimate goal of the 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. The TRA recognized that the issues of counterfeiting and piracy had a tremendous impact on the economy and intellectual property rights. Additionally, fake mobile phones were also of low quality devices that had been manufactured without proper tests and checks impacting health of both subscribers and networks.

7.7 Uganda

In 2012, a project for elimination of counterfeit mobile phones was undertaken. The project was implemented by The Uganda Communications Commission (UCC) aimed at gradually and orderly eliminating the usage of counterfeit devices from the Ugandan market. The project consisted of four implementation phases which are stated as follow.

PHASE 1: Verification of mobile phones: Consumer has two ways to verify the device status i.e. through SMS or UCC website (http://ucc.co.ug/data/imei/2/IMEI-Verification.html).Consumers are advised to immediately verify the legitimacy of their devices using either of the two methods.

PHASE 2: Denial of service to new counterfeit phones: This phase denies any access to those counterfeit devices that haven't previously subscribed on any of the Ugandan mobile network.

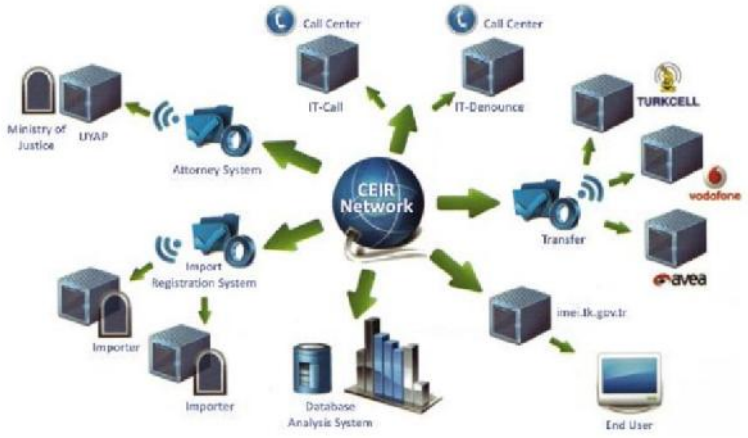
PHASE 3: Disconnection of all counterfeit mobile phones: All counterfeit devices, including the ones that have already subscribed to a particular network to be disconnected.

PHASE 4: Consolidating the project: During this phase, outcomes of the project relating to the implementation of the project and issues to do with e-Waste management and cloning of IMEIs are reviewed by the commission.

7.8 Turkey

In 2006, the Information and Communication Technologies Authority (ICTA) of Turkey established a Central Equipment Identity Register (CEIR). The purpose of this CEIR was 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 system was implemented to restrict illegally imported devices and disconnect the smuggled, lost/stolen and duplicate IMEI devices from wireless networks.



CEIR Structure

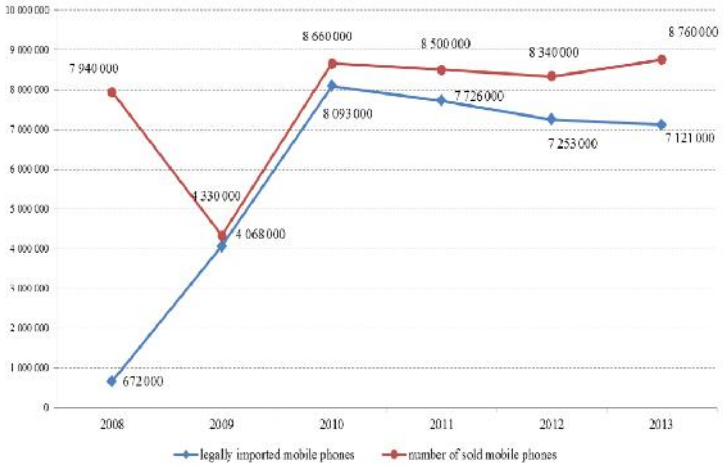
According to the ICTA 2010 Annual Report, almost 131.8 million IMEIs were legally registered and by the end of 2010, 14.3 million IMEIs were included in black list due to being lost, smuggled, stolen and duplicated.

7.9 Ukraine

In 2008, 93-95% of the local mobile phones market was filled with illegal imported devices which was a very big concern for the Government. A considerable amount of these devices did not meet the Ukrainian standards either in their technical characteristics or in their safety. To counter the problem, The National Commission for the State Regulation of Communications and Informatization (NCCIR) was authorized by the Law of Ukraine (On the Radio Frequency Resource of Ukraine) to enforce measures that will protect the Ukrainian market against low quality, unauthorized or illegally imported devices.

The NCCIR implemented a regulatory procedure for import of mobile devices. For this purpose, a system called Automated Information System for Mobile Terminals Registration in Ukraine (AISMTRU) was planned and put into operation by the Ukrainian State Centre of Radio Frequencies (UCRF) in 2009. In 2010, the number of import of illegal devices fell down to only 5-7%which shows the

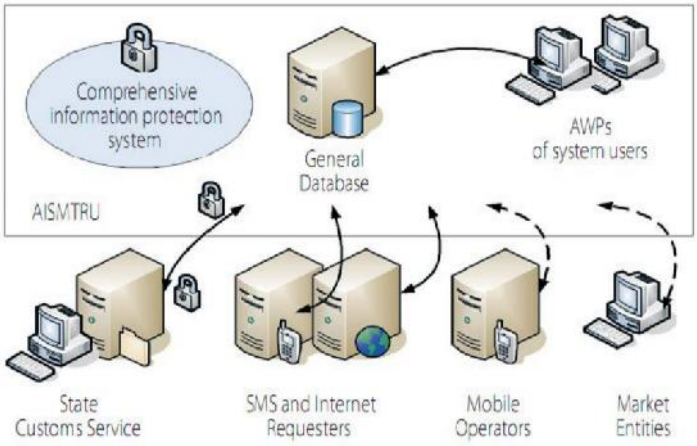
successful implementation of AISMTRU. White, grey and black lists of IMEIs are maintained to allow or deny the device's access on a particular network.



Effects of AISMTRU implementation in Ukraine

The implementation of AISMTRU enabled Ukraine to:

- Computerize the importers application process.
- Restrict the illegal imports of mobile devices into Ukraine.
- Encounter and restrict device theft.
- Identifying and blocking of duplicate IMEIs.



AISMTRU Functions

8. Conclusion and Way Forward:

Once DIRBS is implemented and made operational with assistance of all stakeholders, it will:

- Discourage unlawful business and distribution of illegal/invalid devices.
- Clean and streamline the device eco-system with device lists and interface systems to support regularization and blocking of prohibited devices.
- Reports for various stakeholders will be generated and distributed by PTA, including some to be made public through the PTA website for public and consumer interest.
- Provide level playing field for legitimate OEMs/importers, protecting operator networks from negative performance impacts of illegal/invalid devices.
- Help the government with public safety and tax issues related to such devices.
- DIRBS will benefit Pakistan's mobile ecosystem and have a positive impact on the country's economy.

This consultation paper seeks the input of all stakeholders especially Mobile Network Operators, OEM, Distributors and above all the consumers on how to improve and make DIRBS and its process simpler, easier, smoother and in line with aspiration of the consumers in Pakistan.Going forward, the following activities are proposed to make the initiative successful:

- An exhaustive awareness campaings will be carried out to inform all concerned persons about both the presence of illegal/invalid devices and the problems associated with such devices.
- The system shall be implemented in various phases so that the positive impact for all stakeholders will be ensured
- MNO's are required to upload their data dumps through "Secure File Interface" periodically. This will enable DIRBS to analyze the data and take appropriate action.
- Each operator will have secure web access to the "Device Pairing Interface" to enable them to add and remove IMEI-subscription pairings.
- Through "Field Verification Interface" different access levels will be provided to Pakistan Customs, PTA, Retailors/Distributors and Consumers. This interfacewill check IMEI queries

against DIRBS lists to provide accurate information to users i.e whether the device is legal/valid or not.

- MNOs will be required to take appropriate actions as and when the lists are shared with them by the PTA.

A number of reports for various stakeholders will be generated and distributed by PTA, including some to be made public through PTA website for public, researchers, media and consumer interest. The reports being made public on its website will provide aggregated results of the device market without giving any specific MNO numbers to accomplish the strengthening of national strategy against theft and use of illegal/invalid mobile devices.

9. Annexure-A: Guidelines for Data Field Requirment from MNOs:

9.1 Purpose of the Document

This document provides a quick reference to identify the minimum data fields necessary to support operator device analysis and provide examples of how such data fields are obtained, aggregated, formatted, and transferred.

9.2 Definition of minimum Data Fields

All necessary fields are available from output CDRs and should be aggregated using "GROUP BY". Details regarding these fields and their formats are shown below.

Field	CDR source field and format information
IMEI	• "Served IMEI"
IMSI	• "Originator IMSI" (Record Type 93) or "Recipient IMSI" (Record Type 94) • "Served IMSI" (otherwise)

Date	• Format: YYYYMMDD (e.g. 20150423). Converted from date portion of:
	  • Seizure Time / Answer Time (Record Types 0, 1, 87)[i]
	  • Event Timestamp (Record Types 6-7, 21-23, 25, 28, 93-94, and IMEI Observation Ticket)
	  • Record Opening Time (Record Types 18, 20, 84-85, 96)

MSISDN	• "Originator MSISDN" (Record Type 93) or "Recipient MSISDN" (Record Type 94) • "Served MSISDN" (otherwise)

The operator data dump "Date" field can be sourced from different fields in different types of CDRs produced in the operator's network (e.g. SMS, packet data, voice call etc.). Description in second column of the above table is intended to identify which field in each of the possible CDR types (identified by 3GPP Record Type value) contains the relevant information.

The intention with listing many different record types is to spread the net as wide as possible (to capture as many IMEIs as possible) regardless of the kind of chargeable activity in which they are engaged. Once data is aggregated into the requested format (distinct Date-IMEI-IMSI-MSISDN combinations), the different source record types and fields that were used will not be apparent.

9.3 Example aggregated Data from CDRs

When reporting minimum data set, all fields are "GROUP BY"; so, every unique combination of {IMEI, IMSI, Date, and MSISDN} should be reported. Blank/missing fields should be considered as distinct values and included as such. Below is an example minimum data set per CDRs (colored text indicates duplicate records which will be combined):

Record	IMEI	IMSI	Date	MSISDN
CDR1	35780502398494	310150123456789	20150423	18585551234
CDR2	35780502398494	310150123456789	20150423	18585551234
CDR3		310150123456789	20150423	18585551234
CDR4	35780502398494	310150123456789	20150424	18585551234
CDR5	35780502398494	310150123456789	20150424	
CDR6	35780502398494	310150123456790	20150424	
CDR7	35780502398494	310150123456790	20150424	

Once aggregated, the resulting aggregated reporting data records would look like the following:

Record	IMEI	IMSI	Date	MSISDN
RDR1	35780502398494	310150123456789	20150423	18585551234
RDR2		310150123456789	20150423	18585551234
RDR3	35780502398494	310150123456789	20150424	18585551234
RDR4	35780502398494	310150123456789	20150424	
RDR5	35780502398494	310150123456790	20150424	

9.4 Export of aggregated reporting data to CSV data exchange format

Data should be exported to a CSV text file using UTF-8 character encoding. To ensure correct import, please include a header line in the CSV that identifies the fields being provided. Each record (including the header line) should be located on a separate line delimited by a line break (CRLF). Data fields in each line should be separated by a comma character. Double quotes may be used to enclose fields and to represent blank/missing fields. Below is example CSV formatted data.

```
IMEI,IMSI,Date,MSISDN
35780502398494,310150123456789,20150423,18585551234
"",310150123456789,20150423,18585551234
35780502398494,310150123456789,20150424,18585551234
35780502398494,310150123456789,20150424,""
35780502398494,310150123456790,20150424,""
```

9.5 Transfer of Data

DIRBS supports an easy-to-use, secure file transfer system known as "Secure File Interface". If a particular MNO is transferring data (device data dumps) for the first time, they will be provided the account credentials by PTA data PoC (point of contact) to transfer file(s) securely. Once account credentials are provided, MNOs will be able to securely transfer files.

[1] Seizure Time is used for unsuccessful calls, Answer Time is used for successful calls. Use Answer Time if available, otherwise Seizure Time.

10. Feedback Required on Consultation Document:

In order to obtain focused feedbacks from all the stakeholders, it is requested to respond to following questions:

a. Has the consultation document been able to address the objectives of the DIRBS and identified the stakeholders correctly? What should be included in the terms and conditions for Regulations for DIRBS? Please furnish your comments with justification.

b. Do you have any suggestion to improve further the Proposed DIRBS framework as discussed in the consultation paper? Do you see any issues that could impact the implementation of DIRBS and what should be the possible technical or regulatory solution?

c. The requirement guidelines for the MNOs and OEMs are provided in the document. Does any of the stakeholder require more information or clarification? Any suggestions in this regard?

d. How should invalid/illegal IMEI (duplicate, null, all zeros etc.) be treated? Should they be shut down immediately, overtime or regularized?

d. The issue and procedure related to suspension of service in case of invalid/illegal IMEI (duplicate, null, all zeros etc.) is provided in this document. Do you have any suggestion/comments on the procedure?

e. How do you suggest that we should undertake consumer awareness regarding Invalid/Illegal IMEIs? Importantly, do you think that we should run special awareness programs for business stakeholders i.e. MNO, OEM, Distributors and Retailers? If so, what kind of programs do you suggest?

11. How to Respond:

All stakeholders are requested to respond back to this consultation document by 18 07 2016. All responses should be sent electronically to Director (TA) PTA HQs at naumankhalid@pta.gov.pk with a copy to Deputy Director (TA) PTA HQs at nasir@pta.gov.pk. The comments received after 18 07 2016 would not be considered. PTA assures the stakeholder that all the comments received would be duly analyzed and would be taken into account while preparing the framework for regulatory measures and solutions.

12. Definiation and Glossary of Terms:

The following terms and abbrivations are used in this documet.

Terms	Explanation
Counterfeit Devices	These are the fake and low cost replicas of original and branded devices. These devices are mostly manufactured using cheap and substandard material and are introduced into the market at lower prices as compared to original devices. Such devices are not manufactured under proper quality assured techniques and do not fulfill the requirements of the regulators. Counterfeit devices also have fake IMEIs. All the fake, cloned, duplicated, having zero or Null IMEI devices are known as counterfeit devices.
CDR	Call Detail Record is a data record produced by the telecom equipment that documents the details of calls and other telecom transactions. CDR attributes could include subscriber's phone number, call type, starting and finish time of call etc.
Devices	All communicating devices that uses SIM (subscriber identity module) such as mobile phones, tablets, SIM Based Routers, SIM based laptops etc.
DIRBS Exception	A list of devices IMEIs allowed to be operational on a

List	particular network. Exception list contains specific IMEI-subscription pairings that are allowed to continue receiving service even if their IMEI appears on the blacklist. Entries in this list are added via the "Device Pairing System".
DIRBS Notification List	Devices with certain authentication issues i.e. IMEI has not passed PTA type approval, IMEI has not been reported on any import list, IMEI is invalid (IMEIs not assigned by GSMA) and IMEI is a duplicate (multiple devices with same IMEI).
DIRBS Black List	The blacklist is a list of IMEIs to be blocked. IMEIs may be present on the blacklist for one or more reasons including: IMEI is stolen/lost according to PTA or GSMA, IMEI is invalid/duplicate and has expired from notification list.
EIR	Equipment Identity Register is a database of IMEIs maintained by concerned Operators. EIR keeps a list of mobile phones (identified by their IMEIs) that are to be blocked from being operational on a network.
Fake IMEIs	Duplicate IMEIs that are replicas of original IMEIs.
Invalid devices	Device with replicated IMEIs come in the category of invalid. These are called invalid because the IMEIs are not assigned by GSMA.
Illegal devices	Devices that are either illegally imported into the country or stolen (locally or Internationally).
Importers	Individual/bulk entities who bring in devices from foreign for use, sale etc. purpose.
IMSI	International Mobile Subscriber Identity is used to identify the

	user of a particular mobile network operator and is unique with all the cellular networks. IMSI consists of mobile country code, mobile network code etc.
MNOs (Mobile Network Operators)	Telecom service provider organization licnesed by PTA that provides wireless voice and data communication for its subscribed mobile users.
Mobile Station (MS)	Comprises of user equipment (mobile phone or mobile computer) and software needed for mobile network communication.
MSISDN	Mobile Station International Subscribers Directory Number is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. In simple words, it's a telephone number to a SIM card in a mobile phone.
Null IMEIs	A counterfeit device with zero or no IMEI.
Network Operations Center (NOC)	Network Management Center for monitoring and controlling the telecom network. Few of its functions include: analyze problems, perform troubleshooting and communicating with site technicians or other NOCs etc.
OEMs	Original Equipment Manufacturer (OEM) are manufacturing companies that design, manufacture, and sell market products (mobile phones) under their own brand name. Some OEM's only design their products while the manufacturing is outsourced to contract manufacturers.
Stolen Devices	These devices are reported by the owners as being snatched or stolen locally/globally. The device that a person takes secretly or by force without any permission of its owner.

Stakeholders (DIRBS)	Anyone with an interest in the mobile business and use of the device. DIRBS Stakeholders are individuals, groups or organizations that are affected by the activity of the mobile business such as PTA, FBR/Customs, MNOs, OEM, Importers, Distributors, Retailers and Consumers.
Smuggled Devices	Devices that are brought into the country without paying custom duty. These devices have IMEIs and are valid but the channel through which they are brought into the country is not legal. These devices are available at a lower price as compared to the legal devices because of not paying the custom duty.
TAC	The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEI codes used to uniquely identify wireless devices. The Type Allocation Code identifies a particular model (and often revision) of wireless telephone for use on a GSM, UMTS or other IMEI-employing wireless network. The first two digits of the TAC are the Reporting Body Identifier. This indicates the GSMA-approved group that allocated the TAC.