DIRBS SOP 2017

PTA/DIRBS/SOP/001

Version 1.12

9th November, 2017

First Amendment Date   : 10-Oct-2019
Second Amendment Date   : 28-Nov-2022

Table of content

DIRBS SOP

In accordance to Mobile Device identification Registration and blocking system regulation 2017, following Standard Operating procedure shall be taken into account for public facilitation, Mobile Operator, Government organization and PTA in order to handle DIRBS operational procedures as and when required

1. Introduction

Pakistan Telecommunication Authority is empowered under section 9.6.2, 9.6.3 and 9.6.4 of the Pakistan Telecommunications Policy, 2015, to develop a regulatory framework to ensure that non-compliant mobile devices (stolen phones, phones with duplicate or non-standard identifiers etc.) are blocked from use in Pakistan. To implement the policy a regulatory framework, available on PTA website in the form of DIRBS Regulations, has been developed with the consultation of the stake holders and a Mobile Device Identification, Registration and Blocking System (DIRBS) has been developed and installed by PTA.

DIRBS will function by analysing data dumps received from MNOs. It will generate a black list, exceptions list and notifications list. The first two lists will be implemented by MNOs on their EIRs. Implementation of the lists result in blocking of non-compliant devices. Their implementation also result in unblocking of recovered devices and pairing of existing non-compliant devices with SIMs of owners who are given relief by PTA.

2. Definitions

2.1. **"Authority"** means Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunication (Re-organization) Act,1996;

2.2. **"Person"** means a natural or juristic person who intends to imports PTA approved terminal equipment into Pakistan with the objective of personal use or sale of such equipment, for connection to a public switched network. (2) Words and expressions used but not defined herein shall bear the meanings given there in the Act or the Rules.

2.3. **"Black List"** means a list of IMEIs that are associated with mobile device(s) which have been denied mobile communication service(s) by Mobile Networks Operator(s) (MNO) as they have been reported lost, stolen, have an invalid IMEI number(s), have duplicate IMEI(s) or not having certification of compliance to technical standards for such mobile devices issued by the Authority;

2.4. **"Cloning"** means transfer of identity (IMEI) from one mobile device to another.

2.5. **"Compliant Mobile Device"** means a device that fulfils the following requirements:

2.5.1. Devices with valid IMEIs assigned by Global System Mobile Association (GSMA);

2.5.2. Devices with unique IMEIs; No duplication of IMEI is being observed in MNO's EIR

2.5.3. Devices not in the stolen/lost lists (reported locally to the Authority and globally to GSMA); and

2.5.4. Devices type approved/having Certification of Compliance to Technical Standards for IMEI devices issued by the Authority.

2.6. **"Device Pairing System"** means creation of IMEI - Subscription paired exceptions for permission to allow non-compliant devices to keep receiving mobile service only with the subscription they are paired with

2.7. **"Device Registration System"** means a registration for certification of compliance to technical standards' for IMEI devices in the manner as prescribed by the Authority to the Persons/ Distributers/OEMs/ODM(s)/Type approval Holder(s)/Individuals from time to time;

2.8. **"Device Verification System"** means a web interface and application for stakeholders to verify mobile device status

2.9. **"Duplicate IMEI"** means IMEIs found with two or more mobile devices and also includes same IMEI on a dual or more SIM device for each SIM slot.

2.10. **"Exception List"** means a list containing specific IMEI(s) and Subscription Pairings that are allowed to continue receiving Mobile Communication Services even if their IMEI(s) appear on the blacklist on the basis prescribed by the Authority in Type Approval Regulations, DIBRS Regulations, DIRBS SOP that are in vogue.

2.11. **"Genuine Duplicate Device"** means a device - having valid GSMA assigned IMEI – where IMEI has been duplicated on another device(s) which does not have the same IMEI assigned to it

2.12. **"IMEI"** means an international mobile equipment identity by GSMA. It comprises of unique 15 digit decimal numbers required to identify mobile devices on mobile networks.

2.13. **"IMEI-Subscription Pairing"** means pairing of a particular IMEI with subscriber's SIM.

2.14. **"IMSI**" means the 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.

2.15. **"Mobile Device Blocking"** means-denial of telecommunication service to a device by the MNOs

2.16.   **"MSISDN"** means the Mobile Station International Subscribers Directory Number is a number uniquely identifying a subscription in a GSM or a UMTS mobile network.

2.17.   **"Non-Compliant Device"** means a device which does not fulfill any condition(s) as defined for compliant devices.

2.18.   **"Notification List"** means a list of Mobile Devices with certain authentication issues such as having IMEI numbers allocated by GSMA but is not type approved by PTA, and/or does not have certification of compliance to technical standards for IMEI devices issued by Authority and /or is non-duty paid and/or is duplicate IMEI and/or any other reason notified by PTA

2.19.   **"OEM/ODM"** means an Original Equipment Manufacturer/Original Device Manufacturer, who are type approval holder(s), to market and sell mobile devices in the territory of Pakistan;

2.20.   **"Secure File System"** means the secure interface for Mobile Network Operators to upload mobile device data in the Authority pre-defined format;

2.21.   **"Type Approval Holder"** means and includes an entity holding a valid type approval certificate issued by the Authority under the Type Approval Regulations, 2021(as amended from time to time).

2.22.   "**Valid Devices**" Devices that qualify following criteria will be considered as valid

2.22.1. Devices with valid IMEIs assigned by Global System Mobile Association(GSMA); (Applicable for commercial and Individual Personal Import)

2.22.2. Devices with unique IMEIs; (Applicable for commercial and Individual Personal Import)

2.22.3. Devices not in the stolen/lost lists (reported locally to the Authority and globally to GSMA); (Applicable for commercial and Individual Personal Import)

2.22.4. Devices having Type Access Code (TAC) which belongs to model type approved by PTA (This condition is applicable for commercial import by persons)

3. Implementation Phases

3.1. Phase 1. The phase consists of mapping and identification of IMEIs, including blocking of stolen/lost devices. **Phase 1 started with effect from 10th May 2018 and end on 15th January, 2019**. Following had been done during this phase:

3.1.1. The devices (IMEIs) observed during this phase operational on MNOs networks

which do not comply with clause 2.5.1 and 2.5.2 of this SOP has been paired with SIM (IMSI) by DIRBS as per the **clauses 10.1 and 10.2 of this SOP**.

3.1.2. For phase 1 only, IMEI devices conforming to conditions 2.5.1, 2.5.2 & 2.5.3 of the given "compliant devices" definition considered valid after analysis done by PTA**.**

3.1.3. Black list containing IMEIs of stolen/lost devices are being generated by DIRBS and provided to MNOs on hourly basis for implementation on EIRs for blocking. Subsets of black list will also be provided as per clause 6.1.9 of this SOP.

3.1.4. Exception and Notification lists populated by DIRBS but it had not been implemented on EIRs by MNOs during Phase 1. However, these lists provided to MNOs for their information.

3.1.5. Updated Exception and Notification lists provided to MNOs on hourly basis via DIRBS. However PTA had authority to change the provision of these lists as and when required.

3.1.6. Black list common for all MNOs, whereas Exception and Notification lists were operator specific.

3.1.7. SMS Messages sent to users during Phase I, whose IMEI-IMSI pairings were included in the Exception List, by DIRBS core through SMSCs of relevant MNOs. Table of reasons for pairing and the relevant messages (Non-Compliant Device Possibilities, Reasons and Messages) is attached as Appendix A.

3.1.8. The contents and format of the Black, Exception and Notification lists are attached as Appendix B.

3.1.9. Before the end of Phase 1 or as decided by PTA, DIRBS provided a list of all IMEIs observed on the MNO Networks to PTA, which conform to clause 3.1.2 above. PTA validate the list and subject to fulfilment of other requirements of a compliant device, these IMEIs were not included in the Black lists generated during Phase 2.

3.1.10. All paired devices during phase 1 allowed to continue receiving cellular services till the expiry of their useful life

3.1.11. All Mobile Devices already active on Cellular Mobile networks within Pakistan till 15th January, 2019 remained operational without service disruption. Even non-compliant devices in operation by this date tied to those numbers and remain operational till the useful life of the device.

3.2. Phase 2. Full blocking to be supported including blocking of non-compliant devices except

those paired in accordance with clause 3.1.1.

3.3. All the valid IMEIs which were not observed during Phase 1 and start appearing on mobile networks during Phase 2 will be processed in line FBR issued CGO or in vogue C.No.2 (16) L&P/2018(Pt) issued 28th January, 2019 or in vogue as well as conditions described within PTA issued Type Approval Technical Standards Regulations 2021 as well as DIRBS Regulation 2017 and this SOP for each category of applicants i.e. **Commercial and Individual** import.

   3.3.1. Phase 2 started on 16th January, 2019

   3.3.2. MNOs system must be ready in terms of hardware and software in order to support DIRBS system by 10th October 2018 so that their testing can be carried out between DIRBS and MNOs EIRs before launch of phase 2.

   3.3.3. MNOs have to make sure that they have implemented the final Exception list of Phase 1 before starting the Phase 2.

   3.3.4. During this Phase black list consist of IMEIs of all the non-compliant devices and the IMEIs of devices on the exception list and excluded the IMEIs of devices specified in clause 3.1.9 above.

   3.3.5. Devices showing up "Valid Device" status have an option to register their device by applying via and subject to fulfillment of codal formalities of PTA and FBR, all such devices are made compliant. Devices that are not registered within 60 days date of activation on Cellular Networks in Pakistan shall be subject to blocking.

   3.3.6. Devices showing up "Non-compliant" status subject to blocking after 1 day from date of activation on Cellular Networks in Pakistan. Each non-compliant device (operational on the Networks) will be sent message by DIRBS through relevant MNO SMSC intimating them that the device is non-compliant along with the reason of non-compliance status.

   3.3.7. MNOs will ensure that they implement blacklist and exception list on their EIRs as and when provided by the PTA.

   3.3.8. Updated Black list will be provided on hourly basis. However, the frequency of provision of Exception and Notification lists may increase or decrease if required by PTA. Subsets of black list and exception list will also be provided as per **clause 6.1.9 and 6.2.6 of this SOP.**

   3.3.9. Each MNO instructed to ensure that the latest updated lists have been implemented

on the EIRs at all times.

3.3.10. As a result of implementation of lists on EIRs, IMEIs in the Black list will be blocked except those which are in the Exception list.

3.3.11. The devices who's IMEIs are in the Exception list will work only with the SIMs who's IMSIs have been paired with the IMEI still expiry of useful life of the device(s).

3.3.12. Call flow required for DIRBS exception list support in MNO network will be as given in Appendix C.

3.3.13. Service based Radio Access Technology (RAT) field clone detection shall be used to curb IMEI cloning by PTA (DIRBS).

3.3.14. All the duplicated devices having valid GSMA IMEI will be notified to provide proof of authenticity of their device. IMSI(s) of Genuine Duplicate Device will be paired as per clause 10 of this SOP after providing proof to PTA and the IMEI will be added to the black list.

3.3.15. PTA will differentiate between a genuine duplicate device and a non-genuine duplicate device in accordance with clause 15 of this SOP.

3.3.16. The paired devices will continue to receive service till expiry of the useful life of the device(s).

4. International Roamers

4.1. Roamers will be allowed service while roaming in Pakistan in accordance with Regulation 8 of DIRBS Regulations.

4.2. Roamers will be allowed service for unlimited period; however, the Authority retains the right to revise the time limit to a finite time period.

4.3. In case of finite time limit, change in IMSI or IMEI will not reset the Roaming Period to initial value.

4.4. If a roamer starts using local SIM, in case on non-compliance they will be treated as per clause 3.3.5 or 3.3.6 whichever applicable and upon existence in duplicate/clone field it will be treated as per clause 15 of this SOP respectively.

5. Data Dumps Uploading by MNOs

5.1. All MNOs shall upload Data dumps to DIRBS servers, through secure connectivity between DIRBS and each MNO, as per the requirements/format attached as Appendix D.

5.2. Data dumps will consists of DATE, IMEI, IMSI, MSISDN and RAT columns in the format

attached at Appendix D.

5.3. Before uploading the data dumps, MNOs shall validate the dumps through the latest version of validator provided by PTA.

5.4. MNOs shall upload the validated data dumps and provide the same on hourly basis. The timelines for provision of data dumps will be revised as and when required by the Authority.

5.5. Secure IT connectivity for uploading of data dumps of their respective networks is being established/maintained by each MNO with DIRBS.

5.6. MNO will make sure that the IMEI information being shared precluded all alphanumeric or non-standard format IMEIs. On receipt of data dumps by the system the data will again be validated and processed. In case any discrepancy found in data dumps, the system will generate and transmit a notification to the relevant MNO. Data dumps will be provided again by the MNO with updated version number with in next 24 hours.

5.7. Each MNO shall ensure that data dumps shall be uploaded (pushed) to the DIRBS server in accordance with the schedule at clause 5.5 and above. MNOs shall nominate the focal person in case of any problem arise for collection of data dumps through IT connectivity between DIRBS and MNOs in order to resolve the issue.

6. Handling of DIRBS Lists

6.1. <u>Black List</u>

 6.1.1. It will be prepared as per the format prescribed in Appendix B.

 6.1.2. It will be generated by DIRBS on hourly basis.

 6.1.3. During Phase 1 it consist of IMEIs of stolen/lost mobile devices

 6.1.4. During Phase 2 it consist of IMEIs of all the non-compliant devices seen on networks on 24 hour basis, valid devices not registered within 60days from date of activation and the IMEIs of devices on the exception list.

 6.1.5. It will also contain IMEIs of exception lists

 6.1.6. MNOs will implement the list on their EIRs on hourly basis upon receipt from PTA.

 6.1.7. It will be transmitted to MNOs over IT links by using secure file system for uploading data for implementation within their EIRs.

 6.1.8. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading list.

 6.1.9. For practical implementation reasons Sub-sets of blacklist in the form of daily add and remove lists will also be provided to each MNO.

6.1.10. To ensure all implemented Black lists are synchronized with DIRBS Black list PTA may require MNOs to provide copy of the Black lists implemented in their EIRs from time to time.

6.2. Exceptions List

6.2.1. It will be prepared as per the format prescribed in Appendix B.

6.2.2. Exception list will consist of all the IMEI-IMSI pairings/re-pairings done in accordance with clause 10 of this SOP

6.2.3. It will be generated by the system on hourly basis and MNOs shall submit the compliance report on daily basis to PTA. The Authority may revise it from time to time.

6.2.4. It will be transmitted to MNOs over IT links by using secure file system for uploading data and its implementation on their EIRs.

6.2.5. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading the list.

6.2.6. For practical implementation reasons sub-sets of relevant Exception list in the form add and remove lists will also be provided to each MNO.

6.2.7. To ensure all implemented Exception lists are synchronized with DIRBS Exception lists PTA may require MNOs to provide copy of the Exception lists (through IT link) implemented in their EIRs from time to time.

6.3. Notifications List

6.3.1. Notification list will consist of IMEIs, IMSIs, MSISDNs, Block dates and reasons of IMEIs being on notification list.

6.3.2. DIRBS will intimate the consumers through SMS about their device(s) status as specified in clause 3.1.5 of this SOP

6.3.3. Notification List will be prepared as per the format prescribed in Appendix B.

6.3.4. It will be generated by DIRBS on daily basis and implemented by MNO within 24 hours. The Authority may revise the frequency from time to time.

6.3.5. It will be sent to MNOs for information regarding their consumer being notified.

6.3.6. Each MNO will be given a separate login to Secure File System using ssh-keys for downloading the list.

6.4. Unblocking List

    6.4.1. Unblocking list will be shared on hourly basis, 7 days a week. This list will be implemented by MNO's within hour of receipt.

7. Other Inputs to DIRBs

7.1. Multiple Lists are inputs to DIRBS in CSV format which are Stolen/lost, GSMA TAC and devices having certificate of compliance to technical standards issued by the Authority.

7.2. Lists will be transmitted to MNOs through SFTP.

7.3. Stolen Reported Phone List

    7.3.1. Reported stolen/lost/recovered devices' IMEIs will be included/removed in/from black list on hourly basis.

    7.3.2. Stolen phone blocking/un-blocking shall be handled as per clause 21 of this SOP.

7.4. GSMA TAC Numbers List. Latest GSMA TAC number lists will be uploaded in the system on occurrence

7.5. Certification of Compliance to Technical Standards for IMEI Based Devices Updates. Device Registration System (DRS) will be populated with the details of devices which have been issued the certification (commercial/personal) by PTA till date and kept updated from there on.

8. DIRBS Subsystems

8.1. Device Registration System (DRS).

    8.1.1. DRS is a web based system, provided by PTA, designed to facilitate Type Approval Holders/Distributers/OEM/MNOs/Individuals to apply for issuance of Certification of Compliance to Technical Standards for IMEI devices to PTA.

    8.1.2. After the issuance of Certificate of compliance to technical standards to the applicant by PTA, DRS will upload the data to the DIRBS system.

    8.1.3. Procedure for obtaining Certificate of Compliance to Technical Standards for IMEI Based Devices by commercial entities and individuals is attached as Appendix E.

8.2. Device Verification System (DVS).

    8.2.1. DVS is a web/mobile app/SMS based informatory service, provided by PTA, for general public through which they will be able to check the status of their of IMEI/Device by sending their IMEI number via SMS through short code 8484, PTA

website and DIRBS Android App.

8.2.2. The SMS facility will be provided via the SMSC of MNOs at their own cost for public facilitation through Large Account and it will not be charged for outgoing SMS, However the mobile operators may charge their customers a maximum sum of Paisa 10 + tax per SMS query.

8.3. <u>Secure File System (SFS)</u>**.**

8.3.1. Secure File System will be used to upload data dumps by MNOs to DIRBS and to transfer the three lists which include blacklist, exception list and notification list to MNOs by DIRBS.

8.3.2. The Files will be transferred using SFTP.

8.4. <u>SMS/Notifications Generation System</u>**.**

8.4.1. Each MNO will establish connectivity between DIRBS core and its SMSC for generation of SMS messages to subscribers as per notifications list and to respond to users' SMS messages for verification of IMEIs. It will send SMS to consumers using MNO SMSC.

8.4.2. DIRBS SMSC servers will be connected to all MNOs through SMPP (short message peer to peer) protocol.

8.4.3. SMSC connectivity will be arranged by each MNO and provide relevant SMSC documentation to integrate with DIRBS SMS gateway.

8.4.4. SMS throughput will be ensured by MNO to avoid SMS congestion.

9. DIRBS – MNOs Connectivity

9.1. Redundant Point to Point secure connectivity will be arranged by MNOs to DIRBS.

9.2. 99.9% connectivity uptime will be ensured by MNO/Service providers.

9.3. Each MNO shall designate responsible representative to ensure connectivity to the System.

9.4. Connectivity requirement throughput is 20 Mbps. Requirement may be revised as and when required by PTA.

9.5. IT connectivity as per clause 9.2 and above of this SOP will be used to send/receive SMS notification to consumers, Uploading of Data Dumps by MNOs to DIRBS and downloading of DIRBS Lists by MNOs.

10. Pairing/Re-pairing

10.1. During Phase 1, all non-compliant device IMEIs which do not have valid IMEIs as per clause 2.22 or are not unique will be paired with all the SIM(s) (IMSI(s)) in use with these devices subject to clause 10.5 of this SOP

10.2. Pairings mentioned in clause 10.1 will be done automatically by DIRBS and will remain paired for the period given in clause 3.1.10 above.

10.3. Only genuine duplicated/cloned IMEIs will be paired (in accordance with clause 15 of this sop) after providing proof to PTA and the IMEI will be added into the black list. Provision of cellular services are being allowed on the IMEI-IMSI pair to curb the counterfeit devices.

10.4. Paired devices will be eligible for re-pairing of SIM(IMSI) under the following conditions;

10.4.1. SIM damaged or lost provided there is no MSISDN change

10.4.2. SIM changed due to conversion from a previous generation technology to a next generation technology e.g. from 3G to 4G etc. provided there is no MSISDN change.

10.4.3. A genuine duplicated device user wants to sell/gift the device will be allowed to re-pair the IMSI of new owner with the IMEI of the device.

10.4.4. If the user want to use mobile network portability facility as per Mobile Network Portability Guidelines clause 5.6.

10.4.5. Any other conditioned notified by PTA

10.5. Each genuine IMEI as per clause 15 of this SOP can be paired with maximum of 5 IMSIs (Mobile numbers) that can be replaced upon user request for the conditions mentioned in clause 10.4 of this SOP.

10.6. Authority has the right to amend the IMSI numbers (Sim numbers) being paired with duplicate/clone IMEI as and when require.

11. Continuity of Service to Paired Devices on SIM Change

11.1. To ensure minimum disruption of service MNOs may replace the IMSI of the relevant IMEI-IMSI pair in their EIRs for the situations mentioned in Clause 10.4.

11.2. MNOs will report to PTA for each occurrence through DIRBS portal.

11.3. For the situation mentioned in clause 10.4.3 request will be sent to DIRBS through Complaint management System (CMS) app or web-portal by the selling owner to change his/her pairing by providing seller's and buyer's MSISDNs and their service providers. DIRBS will identify the IMSI of the seller and replace with maximum of 5 IMSIs of buyer

from his service provider.

11.4. DIRBS will amend the exception lists of both MNOs un-pair/re-pair the old/new IMSIs with the device IMEI and send the add/remove sub-sets of the exception list(s) to MNO(s) concerned for implementation. MNOs will implement the required modifications on the same day after being received from DIRBS.

11.5. MNOs will not include any additional IMEI-IMSI combination into the exception list of their system not covered under clause 10 of this SOP.

12. EIR Upgradation.

Cellular Mobile operators shall upgrade their systems in terms of hardware and software to support Exception and Black lists of DIRBS system in the following manners.

12.1. MNOs will upgrade their EIR to accommodate both Valid & Invalid IMEIs in Black List.

12.2. Mobile Operators will upgrade their EIR to accommodate Exception List.

12.3. In Exception List, there must be a pairing of IMEI with IMSI. The overall customization of EIR shall be completed as per PTA decision

12.4. The capacity of Black list & Exception list maintained by operators must be sufficient to accommodate existing subscriber as well future forecast.

12.5. Any future Software & Hardware expansion requirements of EIR, must be catered by MNOs.

12.6. All MNOs will customize their EIRs to convert NULL IMEIs to 14-digit ZEROs, 1s, 2s up to 9s or any other sequence or as required by PTA.

12.7. All MNOs will validate their EIRs to confirm that there is no alphanumeric or any other invalid IMEI entry exist in their data dumps before sharing with PTA.

13. Removal of an IMEI from the Black List

13.1. A blacklisted device will not be activated except for lost/stolen devices which have been found/recovered and type approved devices/Issued certification of compliance to technical standards for IMEI devices or as required by PTA.

13.2. Unblock lists of Type Approved devices will be provided to DIRBS, in accordance with clause 8.1.2 above.

13.3. Provision of removal of back list for duplicate/clone IMEI will be allowed only in below mentioned circumstances

13.3.1. If the IMEI being mark in duplicate/clone, PTA reserve the right to review internally and in case of false positive scenario same can be removed from black list

13.3.2. If the IMEI marked in complete blacklist due to un-availability of information in

GSMA TAC database during first connectivity with local cellular service provider shall be consider for un-blocking after the TAC addition has been conducted in GSMA database

13.4. The provision of unblocking lists vide clause 13.3 above to DIRBS will result into automatic removal of the relevant IMEIs from the blacklist, which on implementation by MNOs on their EIRs will result in unblocking of the IMEIs provided vide clause 13.2.

14. Customer Services

14.1. PTA will provide relevant information to the public through awareness campaign before the launch of DIRBS and through DIRBS portal accessible through PTA web site. There will be no direct contact by the customers with PTA except where specifically indicated in this SOP.

14.2. Complaints by customers will be handled in accordance with DIRBS Regulation 18

14.3. All MNOs/Type Approval Holders/Distributors/Persons will train their Customer Service Center/Help line agents to handle DIRBS related queries/complaints by the customers.

14.4. Apart from any other relevant information the agents will be trained so that they are familiar with the contents of Appendix A, Device Verification System (Clause 8.2 above) and Device Registration System for individuals (Clause 8.1 above) so that they can guide the complainants appropriately

14.5. To train the agents, train the trainer programs will be arranged by DIRBS team at 2-3 locations in consultation with MNOs.

14.6. DIRBS will provide Device Verification System for the public to verify the compliance status of IMEIs. The facility for checking will be provided on DIRBS portal, DVS App and SMS short code.

14.7. For SMS query sent by customer to the system, CMO may charge customer as per clause 8.2.2 above

14.8. Existing stolen/lost mobile phone procedure will be as given in clause 7.3 above and will be handled as per clause 21 of this SOP.

14.9. Genuine device whose IMEI has been duplicated will be handled in accordance to clause 15 of this SOP).

15. Handling of Genuine Duplicate/Clone Devices

The following criteria shall be used to evaluate if a duplicate IMEI device is genuine or otherwise.

15.1. On detection of duplicated or cloned IMEIs the device owner/user for duplicated IMEI devices(s) will be notified through SMS sent via DIRBS short code on their last used MSISDN against the identified IMEI or any other mechanism prescribed by the Authority that their device is non-compliant along with necessary actions required for continuity of their mobile service(s). Non-provision of require data will result in blocking of device IMEI after the lapsed of maximum notification period of 7 days. To avoid blocking device owner/user shall be directed to provide following documents through email ID

dirbscare@pta.gov.pk, PTA Complaint management system (CMS) or in person etc.

    15.1.1. Total number of IMEI(s) programmed within mobile device along with screenshot

    15.1.2. Serial number

    15.1.3. Brand and Model

    15.1.4. Any other document available to prove ownership

    15.1.5. MSISDN(s) (Mobile number) details along with operator name e.g. ZONG, JAZZ, TELENOR, UFONE

    15.1.6. Images of the mobile device and its original box under investigation

15.2.   Notification message disseminate to all MSISDN latched within duplicate/clone mark IMEI will be , "Your IMEI is detected as cloned, send your IMEI(s) by dialing *#06# along with screenshot, serial number, brand & model and mobile numbers to dirbscare@pta.gov.pk for validation within 7 days from receipt of SMS. Non-Provision of details will result in blocking of IMEI"

15.3.   Upon reception of user provided documentation through email dirbscare@pta.gov.pk will be co-related with the extracted data from DIRBS. The below mentioned information will be evaluated for authentication of mobile device IMEI.

    15.3.1. All MSISDNs and IMSIs used with the IMEI along with dates of usage

    15.3.2. Which service(s) (2G, 3G , 4G or future supported technologies) accessed by the IMEI along with the each MSISDN and co-related with the provision of technology by the GSMA

    15.3.3. IMEI shall conforms the clause 2.5 of this SOP

    15.3.4. PTA will verify the provided data /information related to mobile device from the concern OEM if required

15.4.   With the information available vide clauses 15.3 and above, it will be possible to distinguish between the genuine and non-genuine duplicate devices.

15.5.   If required the PTA may ask the owners to bring the devices/boxes/documents for physical inspection.

15.6.   After evaluation, if it is observed that the mobile device having genuine IMEI number and its duplicate IMEI is being used, genuine IMEI will be paired with the provided IMSIs in accordance with the clause 10 of this SOP and the IMEI will be added into the black list. Provision of cellular services are only allowed on the IMEI-IMSIs pair.

15.7.   DVS status of paired deice will be "Your mobile device (***************) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services. Type "pair" and send it to 8484 to find out IMEI(s) pairings with your mobile number".

15.8.   Upon validation of non-genuine device, IMEI will continue into the black list. Cellular service (s) will continue to prohibit upon validation of non-genuine IMEI.

16. Handling of Registration of IMEI(s) for International Warranty claim

16.1.   Warranty claim IMEI replacement application shall be accepted via online portal https://dirbs.pta.gov.pk/drs . Following documents will be required to process and validate the case

16.1.1. Warranty replacement job order by the manufacturer/distributor which shall include all IMEIs of the old and new device.

16.1.2. Warranty card of the device

16.1.3. Old IMEI of Device along with brand and model

16.1.4. New IMEI of the replaced device along with brand and model

16.1.5. Copy of CNIC/ Passport

16.1.6. Mobile Number

16.1.7. Email ID

16.1.8. Postal Address of applicant

16.2.   If only serial number has been furnished in Warranty replacement Authorization document by manufacturer then old and new IMEI, serial number picture shall be entailed in an application

16.3.   Old and replaced IMEI shall conform clause 2.5 of this SOP

16.4.   If the replaced IMEI observed in duplicate/clone field then it shall be handled as per clause 10 & 15 respectively of this SOP.

16.5.   Any application without authentic OEM/Distributor job order/Work Authorization shall not be processed further

16.6.   IMEI replacement under international warranty shall only be processed if the damaged IMEI and replaced IMEI belongs to same model.

16.7.   Upon validation of provided detail in DIRBS as mentioned in clause 16.1, provided replaced IMEIs details will be replaced with the damaged IMEI and DVS status will be updated within 24 hours after application processed.

16.8.   After processing of replaced IMEIs for registration, damaged IMEI(s) shall be placed in black list

17. Handling of non-Register devices

17.1.   The following are the available mechanism for registration of mobile device(s) subject to payment of applicable custom duties/ taxes in following categories: -

17.1.1. International Traveler: The travelers may register the mobile devices brought-in accompanied baggage within sixty (60) days of their arrival in Pakistan by entering their travel credentials i.e. Passport Number, CNIC/NICOP (if applicable) along with IMEI(s) of device through DIRBS system mechanism.

17.1.2. Local Applicant: Local applicants may register the mobile device by entering

their CNIC along with IMEI(s) of device through DIRBS system mechanism.

17.2.   PTA has implemented DIRBS Portal system which can be accessed via following mechanism for ease of applicants:

17.2.1. Online Portal Link: - https://dirbs.pta.gov.pk/drs

17.2.2. USSD by dialing *8484# from any mobile phone having a local SIM

17.2.3. By visiting any mobile service provider Service Centre or Franchisee

17.3.   The above-mentioned information submitted by applicant will be auto processed/validated through WeBoc. The mobile devices will accordingly be cleared by the system in accordance with applicable rates of duty and taxes.

17.4.   The system shall electronically generate Payment Slip ID (PSID) having validity of 7 days from date of PSID generation by WEBOC, for payment of duty/taxes. The applicant will then have options to pay the leviable duty/taxes through online banking, ATM, mobile banking and bank branches of all leading banks. Once the system confirms the payment of duty/taxes, the mobile device IMEI(s) will be white-listed in DIRBS.

17.5.   After the expiry of aforesaid time-limit such mobile devices shall be registered on payment of leviable duty/taxes along with prescribed fine notified for the purpose

17.6.   IMEIs shall comply clause 2.5 of this SOP

17.7.   IMEI shall not be duplicated or clone. If the IMEI already exist in the duplicate or clone field before registration then it will be evaluated upon receiving of data as per clause 15.3 and above. If the data provided by the applicant co-relate with the DIRBS extracted information then it will be removed from duplicate/clone field for registration process

17.8.   IMEI shall be registered if conform above mentioned steps within 24 hours

17.9.   Maximum of 5 devices shall be allowed to register in personal category on individual's cnic /passport in a calendar year.

17.10.   If the IMEI already exists in system before registration then user has to register a complaint on CMS web portal or app for its removal before filing application for registration.

17.11.   Model and manufacturer information shall be shared along with payment slip Identity (PSID), FBR duty in notification sms to applicant. Applicant need to make sure that the model and manufacturer shall conforms to the model & manufacturer received in notification sms before paying tax.

17.12.   If the device model and manufacturer founds inconsistent with the received information in notification sms then your device shall not be consider authentic and authority has the right to block such type of devices even after FBR duty paid.

17.13.   PTA in its mandate of technical institution shall not reserve any rights in tax domain. FBR duty payment carried out on inconsistent model and manufacturer from the user received notification message shall not be refunded by PTA.

17.14.   Non-register user shall use cellular service within 60 days of their first connectivity over local network in Pakistan.

18.   Handling of Device registration received from Ministry of Foreign Affairs (MOFA)

DIRBS shall process the IMEI(s) being received from ministry of foreign affairs (MOFA) for whitelisting if it conforms below mention conditions.

18.1.   Application shall be received from Ministry of foreign affair along with following requirement

    18.1.1. Embassy letter duly signed by authorized person

    18.1.2. IMEI information shall be attached in USB or CD (removable media) or any other mechanism defined by the Authority from time to time.

18.2.   After receiving the information the IMEI information shall be co-related with the DIRBS extracted information.

18.3.   IMEI shall conforms the clause 2.5 of this SOP.

18.4.   IMEI information produced in the application shall comply in accordance with the number of sim slots of the device for further processing. Application shall be processed for validation only upon receiving complete IMEIs detail.

18.5.   Upon validation of the IMEI information, whitelisting shall be conducted by DIRBS within 24 hours of application processed and DVS status shall be modified accordingly.

18.6.   Certificate of Compliance (COC) up to technical standard shall be shared with the concern after whitelisting of IMEI(s).

19. Registration of Mobile Devices Imported By Individuals through Postal Service or Courier

All mobile devices imported by the Individuals through Postal Service, courier, custom detention shall be released as per following procedure: -

19.1.   Officials from Postal Service, Courier, Custom office etc. shall issue detention notice/memo to applicant as well as list down all IMEI(s) programmed within the detained mobile device on the issued detention memo.

19.2.   The applicant shall generate PSID by applying through DIRBS system as per mechanism specified in clause 17 of this SOP

19.3.   The applicant shall provide copy of proof of payment along with PSID details to concerned office.

19.4.   Concerned office shall validate the payment status as well as check IMEI(s) status in DIRBS and if found to be registered, the detained mobile devices shall be released accordingly to the applicant.

19.5.   In case of non-compliant IMEI (i.e. Replica, Fake, Non-Standard GSMA, Reported Stolen etc.) as identified via DIRBS system shall be confiscated and disposed of in accordance with the law in respect of the detained device.

20. Handling of Lost and Stolen Mobile Devices

A field of lost/stolen device shall be provided in web interface of Complaint Management System (CMS) https://complaint.pta.gov.pk/registercomplaint.aspx to an application of blocking or unblocking of IMEI under category Stolen Mobile Handset / IMEI Related Complaint in CMS. Such kind of cases shall be handled as per Consumer protection Regulation issued by the Authority by time to time.

20.1.   Following information shall be entails during filing application for lost & stolen device.

    20.1.1. IMEI information shall be required in accordance to sim slot of device

    20.1.2. Last MSISDNs (SIM numbers) used in both IMEIs

20.1.3. Brand , Model , Color of the device

20.1.4. Reason for Blocking (Stolen/ Snatched/ Missing)

20.1.5. Complainant Credential i.e. Name, CNIC , Address , Father's name, Email Address

20.1.6. Incident location/Area and Incident City and incident date

20.1.7. FIR number if the incident reported to authorities or Application copy in word format launch in police department (15)

20.2. Information provided in clause 21.1 of this SOP shall be co-related with DIRBS extracted information from PMD, NADRA , MNO and upon validation of produced data an one time password (OTP) will be generated on the provided sim number

20.3. Provided sim number should be register on the produced CNIC in the application and shall be operational on incident date for further processing. If the sim had been lost during such type of incident then concern person shall require operational sim (get a duplicate sim from cellular operator) to register a complaint. One of the produced MSISDNs shall co-relate with the MSISDN being reported by mobile network operators.

20.4. If there is no operational sim in the second slot of device till incident date then you have to provide only one IMEI along with the MSISDN being used

20.5. Provision of un-blocking shall be bound to only person's credential which had been produced during blocking. Following information shall be entail during filing an application of unblocking of stolen device

20.5.1. Previous Application number

20.5.2. CNIC information

20.5.3. One time password (OTP)

20.6. Blocking and unblocking shall be carried out within 24 hours of application submission

20.7. Lost and stolen device blocking shall not be carried out if it conforms below mentioned scenarios

20.7.1. MSISDN detail produced in the application does not match with MNO's EIR

20.7.2. Provided sim number CNIC is indifferent from the produced in the application

20.7.3. No MSISDNs (Sim numbers) are being used in the device

20.7.4. If the produced IMEIs are not register in DIRBS

20.7.5. If the concern person failed to provide any information in clause 20.1 of this SOP.

20.8. For any issue observed in filing an application for lost and stolen device , a complaint can be launched on CMS as general query

20.9. Above complaint shall be handled for lost and stolen device (LSDS) as per standard operating procedures and regulation issued by the Authority from time to time

21. Coordination.

For smooth functioning of DIRBS, all MNOs, DIRBS, Type approval holders / distributors/persons and PTA will nominate Points of Contact PoCs.

22. SOP Revision.

The said SOP shall be revised in consultation with all stake holders by the authority.

Non-Compliant Devices Possibilities, Reasons and Messages

In line with the definition of a compliant device, following conditions may occur for compliant/noncompliant devices. Any other combinations are invalid combinations

ISSUES				TREATMENT & MESSAGES				
GSMA Invalid	Stolen	Duplicate	No COC		Phase 1	Phase 2		
							Observed First Time	Observed in Phase 1
				C	Your mobile device IMEI is compliant (PTA Approved)	C	Your mobile device IMEI is compliant (PTA Approved)	Your mobile device IMEI is compliant (PTA Approved)
			*	V	Your device IMEI is Valid. If you haven't used this device then insert SIM and make a call/SMS to anyone for auto registration	N	Your device IMEI is not registered (GSMA Valid). Please register your IMEI(s) at https://dirbs.pta.gov.pk/drs and in case of non-registration IMEI will be blocked after expiry of 60 days from the date of activation on mobile network	Your mobile device IMEI is compliant (PTA Approved)
		*		P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	P (Genuine only)	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.
		*	*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	N, P (Genuine only)	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.
	*			B	Device IMEI is blocked. Reported stolen	B	Your mobile device IMEI is blocked. Reported Stolen/Lost/Misused to PTA	Your mobile device IMEI is blocked. Reported Stolen/Lost to PTA
	*		*	B	Device IMEI is blocked. Reported stolen	B	Your mobile device IMEI is blocked. Reported Stolen/Lost/Misused to PTA	Your mobile device IMEI is blocked. Reported Stolen/Lost to PTA
*				P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	B	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.
*			*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	B	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.
*		*		P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	B	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.

*		*	*	P	Device IMEI is non-compliant. Your IMEI will be paired with your mobile number. Your device will continue receiving services.	B	Your device IMEI is non-compliant and will be blocked at expiry of 1 day from the date of activation on local mobile network.	Your mobile device (IMEI) is non-compliant. Your IMEI has been paired with your mobile number and your device will continue receiving services if you have been using it on mobile network before 16th Jan 2019.

Treatment Legends	
Block	B
Pair	P
PTA Certification of Compliance Required	N
GSMA Valid but NOT PTA TYPE APPROVED MODEL	V
Compliant	C

Contents and Format of Black, Exception and Notification Lists

1.   Lists will be shared using secure FTP and authorized credentials. Lists will be in .CSV format. Size of each list is dependent on project implementation phases.

2.   Date and time will be appended in name of list after consultation with stakeholders e.g. black_list_20172509.csv

3.   Frequency of lists will be as follows:

List Name	Distribution Frequency
Black List	Daily
Notification List	Daily
Exception List	Daily

4.   Black List Sample:

a.   Black list will be same for all operators

b.   Headers are (IMEI, BLOCK_DATE, REASONS)

c.   List will not be delta list

d.   Sample entries are given below:

Imei	block_date	Reasons
35335407509863	20170701	Stolen
35551405663500	20170701	Stolen
35396801210014	20170701	Stolen

5.   Notification List Sample:

a.   For each operator, separate list will be provided

b.   Headers are (IMEI, IMSI, MSISDN, BLOCK_DATE, REASONS)

c.   Name of operator will be suffix. e.g., Notification_mobilink.csv

d.   Sample entries are given below:

Imei	Imsi	Msisdn	block_date	Reasons
35738006070489	410018937826633	923084248572	20180701	Stolen, gsma_not_found, Duplicate, etc
35645606474058	410018308077873	923014772876	20180701	Stolen, gsma_not_found, Duplicate, etc
35422706411153	410018558561776	923012842203	20180701	Stolen, gsma_not_found, Duplicate, etc
35635105791242	410018138639138	923004018004	20180701	Stolen, gsma_not_found, Duplicate, etc

6. <u>Exception List Sample</u>:

   a. For each operator, separate list will be provided

   b. Headers are (IMEI, IMSI). Name of operator will be suffix. e.g., mobilink_exception.csv

   c. Sample entries are given below:

Imei	Imsi
35738006070489	410018937826633
35645606474058	410018308077873
35422706411153	410018558561776
35635105791242	410018138639138

Call Flow Required DIRBS Exception List Support

The diagram below shows the EIR call flow required for DIRBS exception list support. The check IMEI request must support both IMEI and IMSI in the check IMEI message.
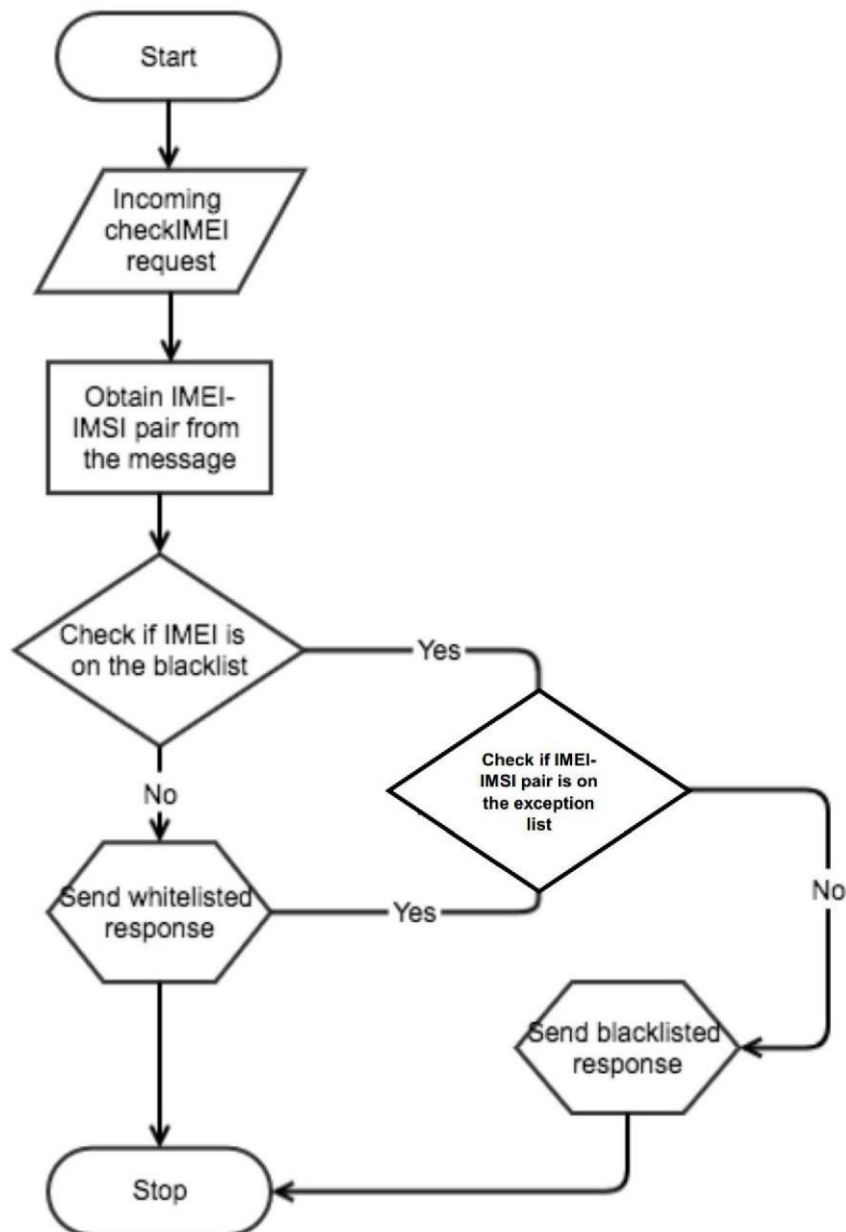
Requirements & Format for Data Dumps

Definition of data fields

All necessary fields are available from output CDRs. Field details and formatting are shown below.

Field	CDR source fields that contain the information	Format
Date	Converted from date portion of the following, aggregated by local time: • Seizure Time / Answer Time (Record Types 0, 1, 87) *(note: Seizure Time is used for unsuccessful calls, Answer Time is used for successful calls. Use Answer Time if available, otherwise Seizure Time.)* • 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)	YYYYMMDD* (e.g. 20160423) *aggregated by local time
IMEI	"Served IMEI"	14-16 digits* (e.g. 013845000153547) *includes any leading zeros *(i.e. if an IMEI starts with one or more zero digits, these leading zeroes must not be stripped off, as doing so would completely change the IMEI value)*
IMSI	"Originator IMSI" (Record Type 93) or "Recipient IMSI" (Record Type94) "Served IMSI"(otherwise)	14-15 digits
MSISDN	"Originator MSISDN" (Record Type 93) or "Recipient MSISDN" (Record Type94) "Served MSISDN"(otherwise)	Up to 15 digits* (e.g. 18583551234) *in E.164 format *(i.e. international telephone number, including country code but excluding any international call prefixes, spaces, or separators)*
RAT	"System Type" (Record Types 0-1, 6-7, 23,25) "RAT Type" Record Types 18, 20-22, 28, 84-85, 93-94, 96) *At the time of writing, defined RAT values include:* *001 – UTRAN (3G) 007 – Virtual* *002 – GERAN (2G) 101 – IEEE 802.16 (WiMAX)* *03 – WLAN 102 – 3GPP2 eHRPD (3.5G)* *04 – GAN 103 – 3GPP2 HRPD (3G)* *05 – HSPA Evolution (3.5G) 104 – 3GPP2 1xRTT (2G)* *06 – E-UTRAN (4G) 105 – 3GPP2 UMB (4G)*	Pipe-separated list of 3 digit codes, with leading zeroes intact

Data 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.…). The description in the second column in 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 obtain a complete view, capturing as many IMEIs as possible, regardless of the kind of chargeable activity in which they engaged. Once data is aggregated, the different source record types and fields that were used will not be apparent.

Excluded CDRs

In general, multiple CDR Record Types are intended to contribute to the final MNO data dump, as indicated in the table above. However, some CDRs may be generated for IMEIs that are in fact blocked by the EIR. If these are included by the MNO, they may appear incorrectly as "blacklist violations" (activity by devices which should have been blocked) in subsequent reporting. Instead, the following cases should be excluded from the file submitted to DIRBS:

Emergency calls: Emergency calls are allowed regardless of blacklist status. They may be identified by the "Emergency Calls" teleservice in the "Basic service "field of a Mobile Originated Call or MSC-SRVCC Record (see 3GPP TS 32.250), or "IMSI Unauthenticated Flag" in PS CDR (see 3GPP TS32.251)

CDRs for attempts blocked by the EIR: In case a CDR is generated for an attempt by a UE that is actually unsuccessful due to EIR blacklisting. Such records may be identified by "Illegal Equipment" in the Diagnostics field,   or by correlate on with the associated blacklisted "IMEI Observation "ticket using the Call Reference field (see 3GPP TS32.250)

Aggregation of data from CDRs

Each row in an operator data dump represents an aggregation of CDR Fields comprising a distinct Date- IMEI-IMSI-MSISDN combination along with a list of distinct RAT values used by that combination. This list of distinct RAT values will be pipe delimited (i.e. a concatenated list of values with each value separated by a pipe ('|') character). Blank/missing fields shall be considered as distinct values and included as such.

Below is a set of example fields <u>before</u> aggregation:

Date	IMEI	IMSI	MSISDN	RAT
20160130	35780502398494	310150123456789	18585551234	001
20160130	35780502398494	310150123456789	18585551234	002
20160130	35780502398494	310150123456789	18585551234	006
20160130		310150123456789	18585551234	001
20160131	35780502398494	310150123456789	18585551234	001

Based on these example fields, the following would be the data dump rows created <u>after</u> aggregation:

Date	IMEI	IMSI	MSISDN	RAT
20160130	35780502398494	310150123456789	18585551234	001|002|006
20160130		310150123456789	18585551234	001
20160131	35780502398494	310150123456789	18585551234	001|002
20160131	35780502398494	310150123456790		001

Export of aggregated data to CSV

Data shall be exported to a CSV text file using UTF-8 character encoding. To ensure correct import, a header line shall be included in the CSV that identifies the fields being provided. Each record (including the header line) shall be located on a separate line with a CR/L fending (/r/n).Data fields in each line shall be separated by a comma character.
Below is example CSV formatted data.

Date,IMEI,IMSI,MSISDN,RAT 20160130,35780502398494,310150123456789,18585551234,001|002|006
20160130,,310150123456789,18585551234,001
20160131,35780502398494,310150123456789,18585551234,001|002
20160131,35780502398494,310150123456790,,001

Transfer of data to DIRBS

Each operator shall securely upload data to DIRBS during their assigned time window using their provided credentials. Time windows and credentials shall be provided to each operator by the DIRBS operational entity for that country.

Prior to upload, operators shall validate their data format using the provided schema and open source tool (identified in the schema). Performing this validation step can help ensure successful processing of the data and cut down on roundtrips.

Files transferred by each operator shall be zipped to provide efficient transfer and enable detection of corruption due to network connection failures. ZIP file details are shown below.

ZIP file name	The ZIP filename shall comprise the operator name followed by start and end dates in YYYYMMDD format as shown below. The dates shall be in local time and shall define the date range for the data inclusively (i.e. data in the file shall include both start and end dates): **OperatorName_*OptionalRegion*_StartDate_EndDate.zip** *(e.g. Foo Wireless_Zone4_20160101_20160131.zip)*
ZIP file contents	Each ZIP file shall contain only one CSV file. With the exception of the file extension, the CSV filename shall be the same as the ZIP filename as shown below: **OperatorName_*OptionalRegion*_StartDate_EndDate.csv** *(e.g. Foo Wireless_Zone4_20160101_20160131.csv)*
File security	Files shall not contain passwords. File security is accomplished via secure file transfer. No encryption is applied to files during storage on DIRBS.

Once received, each file is moved to the incoming folder in that operator's home directory on DIRBS for import and processing.

Validation of data by DIRBS

DIRBS regularly monitors for newly uploaded data from operators. When a new file is detected, it will be validated by DIRBS. If validation fails, an alert will be generated and the DIRBS operational entity for that country will contact the operator to initiate re- upload of a valid data file.

Note that while schema validation can be checked by an operator prior to upload, such validation is only a subset of the validation performed by DIRBS, which may include comparison against historical metadata, identification of invalid rows, flagging of discrepancies, and application of import failure thresholds. Validation issues may be included in operator and/or audit reporting and may result in a validation failure alert, depending on the type and/or severity of such issues.

Device Registration System (DRS) procedure for Obtaining Certificate of Compliance to Technical standard for IMEI based device

SOP for Issuance of Certification of Compliance to Technical Standards for individual and commercial user has been enlisted below

Appendix E-1

Standard Operating Procedure for Issuance of Certification of Compliance to Technical Standards for Mobile Devices with SIM Functionality for Personal Use/Gift etc.

1.   **Background**: Individual(s) can bring up to 5 mobile devices in a calendar year for personal use, however they will be required to obtain certificate of compliance (CoC) to technical standards and IMEI which meet the codal requirements will be allowed for connectivity with mobile networks within Pakistan.

2.   In order to effectively and efficiently process the cases of Certification of Compliance to Technical Standards and facilitate the general public in acquiring Certification of Compliance to Technical Standards following procedures are listed for all concerned:

(a) **For SIM/IMEI based Terminal device(s) imported by individual(s) for personal use following conditions are applicable:**

Parameter	Details
GSMA Type Allocation Code (TAC)	IMEI for device(s) will contain only GSMA TAC excluding blacklisted TAC by the Authority
Duplicated/Cloned/Stolen/Counterfeit IMEI	Mobile devices that contain duplicated/cloned/stolen/counterfeit shall not be allowed for issuance of CoC by PTA
Quantity	Only 5 mobile devices in a calendar year will be allowed
Apply via PTA online Portal	Applicant shall apply via PTA online portal link available at dirbs.pta.gov.pk/drs and upload all listed requirement into the portal system

  a. Obtain IMEI of your device using following methods prior to traveling and note it down for registration with the Customs Authority:

   i. Dial *#06# from the dial pad of your device and note down each 15-digit IMEI (for dual SIM devices) supported by the device.

   ii. IMEI is printed on the device box.

   iii. IMEI printed on the device by removing the back cover/ battery.

  b. Import in personal capacity must be in accordance with in vogue FBR issued CGO.

  c. Pakistan Telecommunication Authority (PTA) in consultation with Federal Board of Revenue (FBR) has developed an online Device Registration

System.

Follow These Steps to Register the IMEI(s) of Your Device(s):

Go to https://dirbs.pta.gov.pk/drs/& click on Sign Up for creation of user account.

Select applicable "User Type" listed below:

1. If you are an International Traveler having dual nationality and you travelled on either Pakistani passport or Foreigner passport and you are a **Pakistani citizen**, select user type as "**Pakistani (Local/International Travelers/Dual Nationality Holder)**".

2. If you are an International Traveler and you are a foreign national and travelled on visa, select user type as "**Foreigner (Travelled on visa)**".

Login to your account. Click on "Apply for CoC" under "Individual CoC" category.
Pay the applicable Customs duties received through PSID code by:
Online banking, ATM OR **Bank branches**
Your device is now registered in Device Identification Registration & Blocking System (DIRBS). A sms/email of confirmation will be sent to concern.

*Please enter the number of the same passport on which you have travelled, otherwise the System will not recognize the entered passport data.

Note: In case of dual or triple SIM devices, users need to register all IMEIs of that device.

Standard Operating Procedure For Issuance Of Certification Of Compliance To Technical Standards For Commercial User To Release Mobile Devices Detained By Customs

Commercial user shall allow 5 devices for same model and memory for submission for type approval. Devices with the quantity more than 5 shall require Type approval certificate up to technical standard as per process in vogue. Following information shall require for issuance of certificate of compliance up to technical standard for maximum of 5 devices with same model and memory

Subject: NOC Request for IMEI Based Sample Device for Test and Trial Only

Consignee/Applicant Name/ Company Name:
Postal Address:
Phone No:
Email Address:

Following documents are to be included along with request form and emailed at commercialnoc@pta.gov.pk with Subject of email indicating NOC for Airway Bill Number, Qty, Make & Model
a) Commercial Invoice Copy
b) Airway Bill Copy
c) Technical Literature Copy
d) PTA Request form in Word File Format
e) End to End Network Connectivity Diagram
f) Request for issuance of NOC written and signed on company letterhead
g) In case of SIM based devices provide IMEI numbers for each device

Note
• NOC will be issued to consignee mentioned in AWB letter provided to this office.
• Issued NOC will be dispatched at given postal address in the request
• Applications received on other than above format will not be entertained.

Miscellaneous Issues and their redressal

Following exceptional cases will be handled as per procedure below for resolution.

Scenario	Issue	Resolution
CoC for Individuals: Pakistani Citizen (Local, International Traveler, Dual National) & Foreigner who applied directly via online portal or used custom airport KIOSK etc.	**IMEI entered incorrectly:** An applicant has entered wrong IMEI	**Delete applicant's request:** Application is deleted or replaced on applicant's request as he/she has entered wrong IMEI and be replaced with correct IMEI
	Invalid/Blank Passport or CNIC Error, Data Mismatch Issue, Link Down, User Identity Theft etc. : In case where the international travelers applies for registration of his/her mobile device through PTA web portal or identifies issue via email/postal mail etc. within the period of sixty days as envisaged in CGO 1 of 2019 and the registration of the mobile devices cannot be made within the aforesaid period against the admissible allowance due to issues like data mismatch with FIA, FIA link down or cases of identity theft etc.	a) PTA may process for whitelisting of such cases subject to condition that the complete particulars of the individual are verified including passport numbers, CNIC number and date of arrival of admissibly of duty free allowance. b) PTA will register such devices IMEI via DRS portal c) In case of misuse of passport data, IMEI registered under misuse will be unregistered/blocked and all misuse credentials, logs etc. will be sent to FBR for legal action under the law
	All IMEIs of device are not entered: Applicant has entered only one IMEI number of his/her device and forgot to enter all IMEIs of his/her device.	PTA will verify in such cases IMEI status where if one IMEI slot shows as Compliant and other as non-compliant. Person need to register a complaint on CMS portal for registration of non-compliant device after taking verification from OEM.

PSID generated in system is deleted by applicant, where custom duties have been paid against deleted PSID	User has option to delete an application during "pending" stage within the DRS portal. In some cases user ends up deleting the request but has paid custom duties against the deleted PSID to Custom	PTA will verify the status of payment submitted against the PSID by sending documents e.g. bank payment receipt, transaction statement etc. to FBR. Upon confirmation, PTA will ask applicant to apply for a new application in DRS where a new PSID is generated. The verified payment status from old deleted PSID will be replaced accordingly against new application and registration will be completed accordingly.
CoC for Personal Courier	COC for Personal Courier rejected/edited if any wrong entry made by user e.g. IMEI, Airway bill etc.	In such case to case scenario PTA will amend data to reflect correct details for processing of request
Reprogrammed IMEI	IMEI are identified to be reprogrammed for purpose of misuse and affect a genuine device connectivity/usage etc.	PTA DIRBS system will identify reprogrammed IMEI and upon detection all such IMEI will be blocked and denied services to network.
Whitelisting of Type Approval IMEI sample received with applications	Samples received for type approval applications containing IMEI require whitelisting	PTA officials will consolidate IMEI list for received sample for whitelisting of same in DIRBS
Commercial CoC	Queried	Applicant will reply to queried within the system for further Action
	Rejected	Reasons for rejection will be included within the system response for applicant to see
	Rejected after approval	In case where an approved request in PTA is not visible within the FBR Weboc system due to several technical reasons e.g. Waybill mismatch, GD mismatch etc. applicant will apply via email for rejection of their approved request to re-apply again. Upon rejection all entered data including IMEI will be removed from DIRBS.

Commercial COC issued prior to online portal via email based or postal based mechanism	Mobile Devices import was done prior to introduction of online portal system and such devices are showing up as non-compliant or blocked as IMEI of same is not recorded in DIRBS	PTA will ask applicant to provide following document as and where applicable and white list such exceptional cases accordingly subject to fulfilment of following conditions:_ a) Copy of issued COC and list of IMEI applied against the COC prior to online portal system b) In case of no COC, PTA will ask applicant to provide proof of import being as per legal process by providing documentation e.g. Custom import documents, evidence of custom duties were paid, IMEI imported were in accordance with type approval certificate and verified GSMA TAC

STANDING OPERATING PROCEDURE (SOP) for Registration of Devices through Mobile Operators Channels e.g. Service Centre and Franchisees etc

Background: Individual(s) can bring up to 5 mobile devices in a calendar year for personal use subject to fulfilment of legal and codal formalities. However they will be required to obtain certificate of compliance (CoC) to technical standards.

In order to effectively and efficiently process the cases of certification of compliance to technical standards and facilitate the general public in acquiring certification of compliance to Technical Standards following procedures are listed for availing the registration facility at all cellular Mobile Operator Service Centre and Franchisee etc.

CMO Service Centre and Franchisee will follow These Steps to Register the IMEI(s) of Your Device(s):

1. International traveler/locals wanting to register IMEI in individual capacity are required to register their device with PTA DIRBS system for issuance of COC through available online portal (https://dirbs.pta.gov.pk/drs) or USSD string and get "PSID" code.

2. After having PSID code, he/she can pay duties in FBR designated banks/CMOs affiliated bank's touch points.

3. CMOs designated Franchises/Sale point will ensure facilitation to all international Travelers/customers for registration of their devices using PTA's Online Portal or USSD string for generation of "PSID" code through their personal computers/Cellular devices. CSC & Franchisee may charge Rs100 from applicant for this facilitation to the customer.

4. Franchisee shall not retain any information or copies of CNIC/Passport/Travel document with them. However CMOs shall not be held accountable in case of any violation or Misuse of information by franchisee.

5. Standees will be placed at designated franchisees of CMOs to educate customers for registration through online portal/ USSD string as well as reflect the service charges of PKR 100 per registration activity. The standee will also include helpline details for CMO and PTA for reporting of any service charges taken beyond the officials approved rate to carry out necessary action by CMO and PTA

6. Applicant shall utilize the CMO offered touch points and apply via PTA online portal link available at www.dirbs.pta.gov.pk/drs or www.pta.gov.pk and upload all listed requirement into the portal system. The customer shall be encouraged to apply on their own accord.

7. The charges would apply to facilitation extended to all registering customers.
   Disclaimer
   *Please enter the number of the same passport on which you have travelled, otherwise the System will not recognize the entered passport data.

   Note: In case of dual or triple SIM devices, users need to register all IMEIs of that device.

   After verification of IMEIs, *Certification of Compliance to Technical Standards for a maximum of 5 devices** **will be issued.**