October 4, 2018

Combatting Mobile Counterfeiting and Theft

Mohammad Raheel Kamal

Combatting Mobile Counterfeiting & Theft with Regulations & Technology

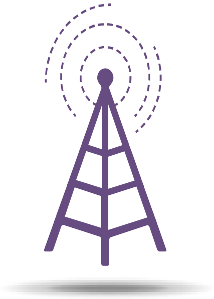
- Due to scale of the negative impacts to the ecosystem caused by fraudulent devices, governments and industry are increasingly interested in methods to address this growing problem
- Governments are motivated to implement regulations to assist in controlling a wide range of issues including:

Mobile Theft | **Security** | **Tax Loss** | **Consumer Privacy** | **Network Quality** | **IPR Infringement**

Proper regulatory and technical framework can serve as an excellent foundation to controlling the proliferation of counterfeit, illegal, non-compliant & stolen devices.

Effects of Counterfeit Devices on Mobile Networks

Qualcomm study concluded fraudulent and counterfeit devices:



Have suboptimal link performance resulting in lower network capacity

- ↓ 23% lower LTE data capacity*
- ↓ 6% lower HSPA data capacity*
- ↓ 27% lower UMTS voice capacity*

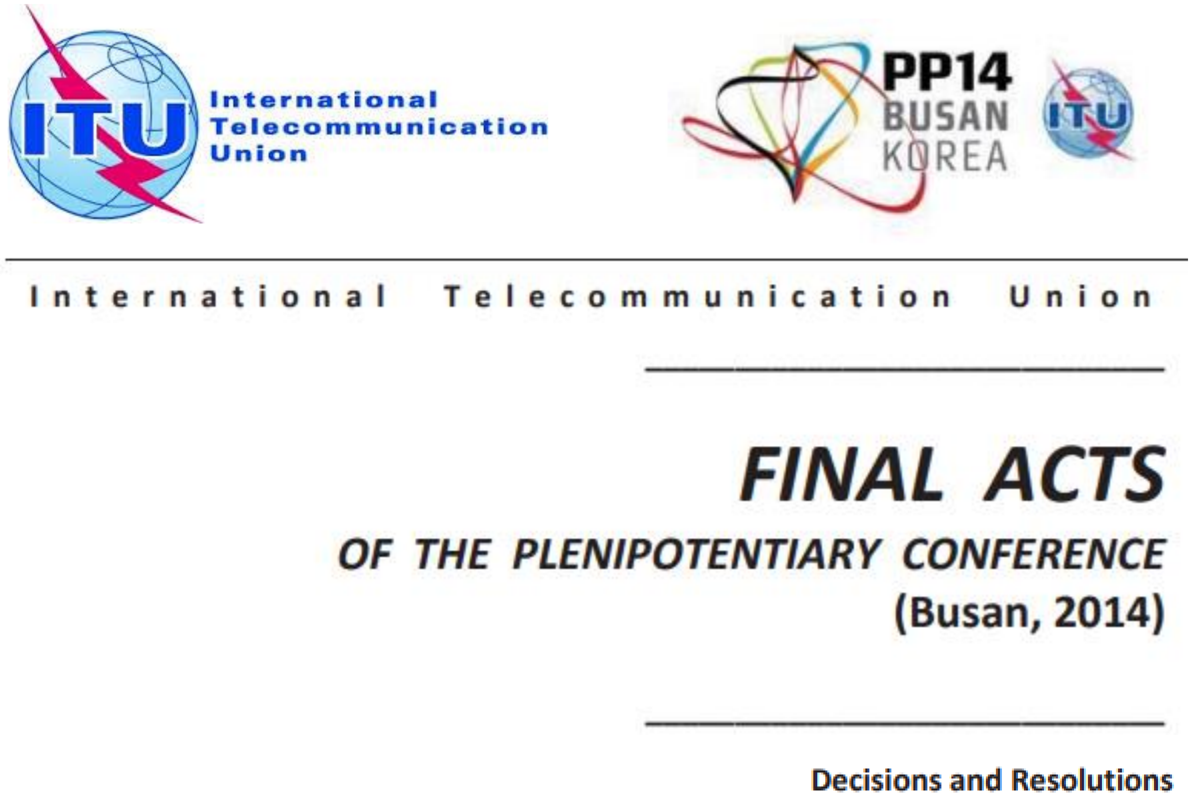
Often lack support for latest LTE features such as LTE-CA, 4x4 MIMO, & 256QAM further degrading network capacity and overall user experience

Drive higher network site count requirements with associated capital and operating expenses, negatively impacting the mobile operator's business case

*Based on fraudulent/counterfeit devices having 10dB worse Total Isotropic Sensitivity relative to legitimate devices per extensive multi-party device testing

Required Elements to address Counterfeiting & Theft

1. Government Regulations & Enforcement
2. Technical Platform



International Telecommunication Union

PP14 BUSAN KOREA

ITU

International Telecommunication Union

FINAL ACTS

OF THE PLENIPOTENTIARY CONFERENCE

(Busan, 2014)

Decisions and Resolutions

Telecommunication/ICT devices that do not comply with a country's applicable national conformity processes and regulatory requirements or other applicable legal requirements should be considered unauthorized for sale and/or activation on telecommunication networks of that country.

Regulatory Framework for Combatting Counterfeiting & Device Theft

Mandatory Elements in Country’s Telecom Regulations

Type Approval

- Ensures device authenticity and Standards conformance

Device Registration

- Ensures IMEI uniqueness; Curbs counterfeiting; Eliminates illegal import

IMEI Tampering Laws

- Laws to criminalize changing or improperly using IMEIs deters counterfeiting and theft

Device Related NW Data

- Regulatory mandate for the operators to provide device related data from the networks

EIR Deployment

- Mandatory requirement for networks to have EIRs for device blocking and granting amnesty

Device Blocking

- Mandate to block non-conforming, illegal and stolen devices using operator EIRs

Stakeholders Roles & Responsibilities

Government

- Develop Regulatory Framework
- Implement Standard Operating Procedure
- Deploy and Administer a technology platform to enforce regulations
- Run an Awareness Campaign

Manufacturers / Importers

- Obtain Device Type Approval from the Government / Regulator
- Register all devices to be imported
- Register all locally manufactured devices

Operators

- Provide Device related Network Data to the government
- Ensure EIRs support Blacklisting of valid/ invalid IMEIs & allow for exceptions
- Notify subscribers of their device status via SMS as required

Consumers

- Verify Device Status via SMS, App, Web Interface
- Register individually imported device(s)
- Report Device Theft to authorities
- Submit proof (invoice) for Genuine Devices, if required

Qualcomm

Technical Framework for Combatting Counterfeiting & Mobile Theft

1. Classify Existing Devices

- Analyze device data from network information
- Classify devices by their IMEIs (valid / invalid, unique / duplicate)

2. Allow All Existing Devices

- Pair existing fraudulent IMEIs with IMSIs and MSISDNs

3. Register New Devices

- Require Type Approval with unique device identifiers
- Register imported & locally produced devices with valid and unique identifiers only

4. Detect IMEI Falsification

- Analyze network data
- Identify devices with fraudulent IMEIs

5. Enable Network Blocking

- Control device access of non-compliant devices / non registered devices - through network control

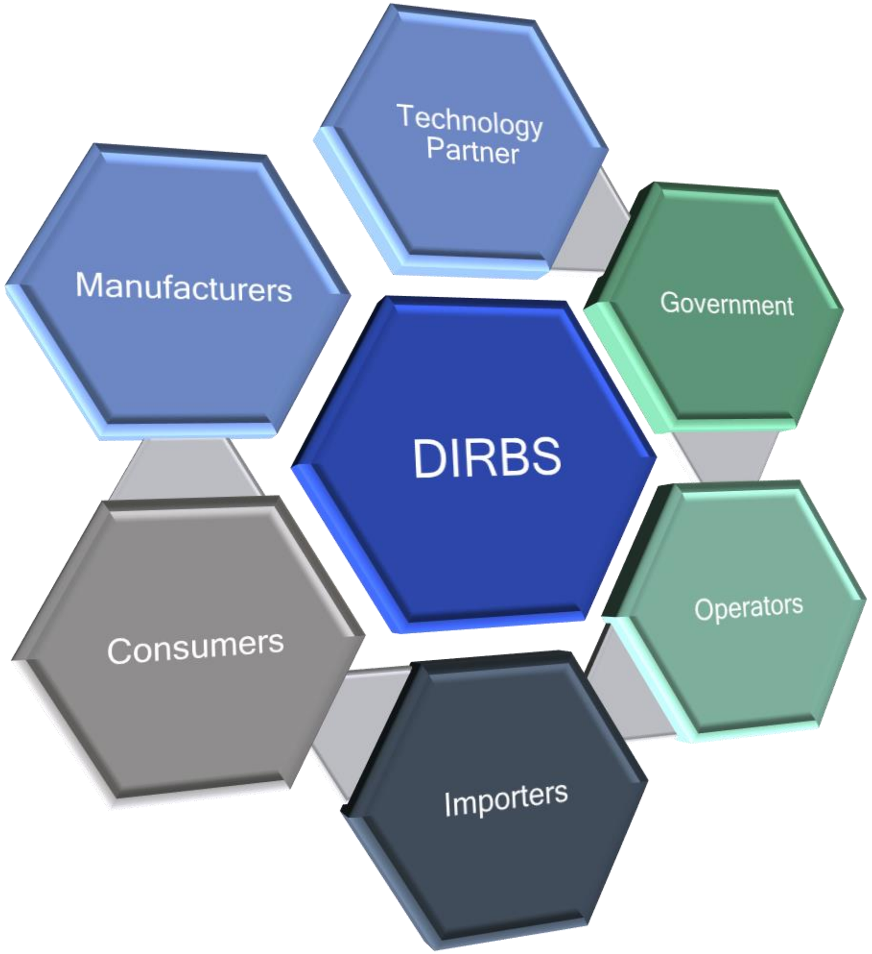
This Framework Curbs Counterfeits, Mobile Theft and Illegal Imports (Smuggling) and Benefits the Entire Ecosystem

Considerations for Technical System Implementation

- Convenient for all stakeholders, especially the consumers
- Standalone system alleviating the need for mobile network integration and interoperability that cause unnecessary cost, capacity constraint and resource burden on the operators
- Not requiring strict binding of every single device to a given customer
- Flexible/Configurable to adapt to local country regulations without the need for any customization
- Provides tools for users to check device validity before purchase

Qualcomm Technologies Inc., has Developed and Shared its Technology Platform via Open Source to Address the Issues

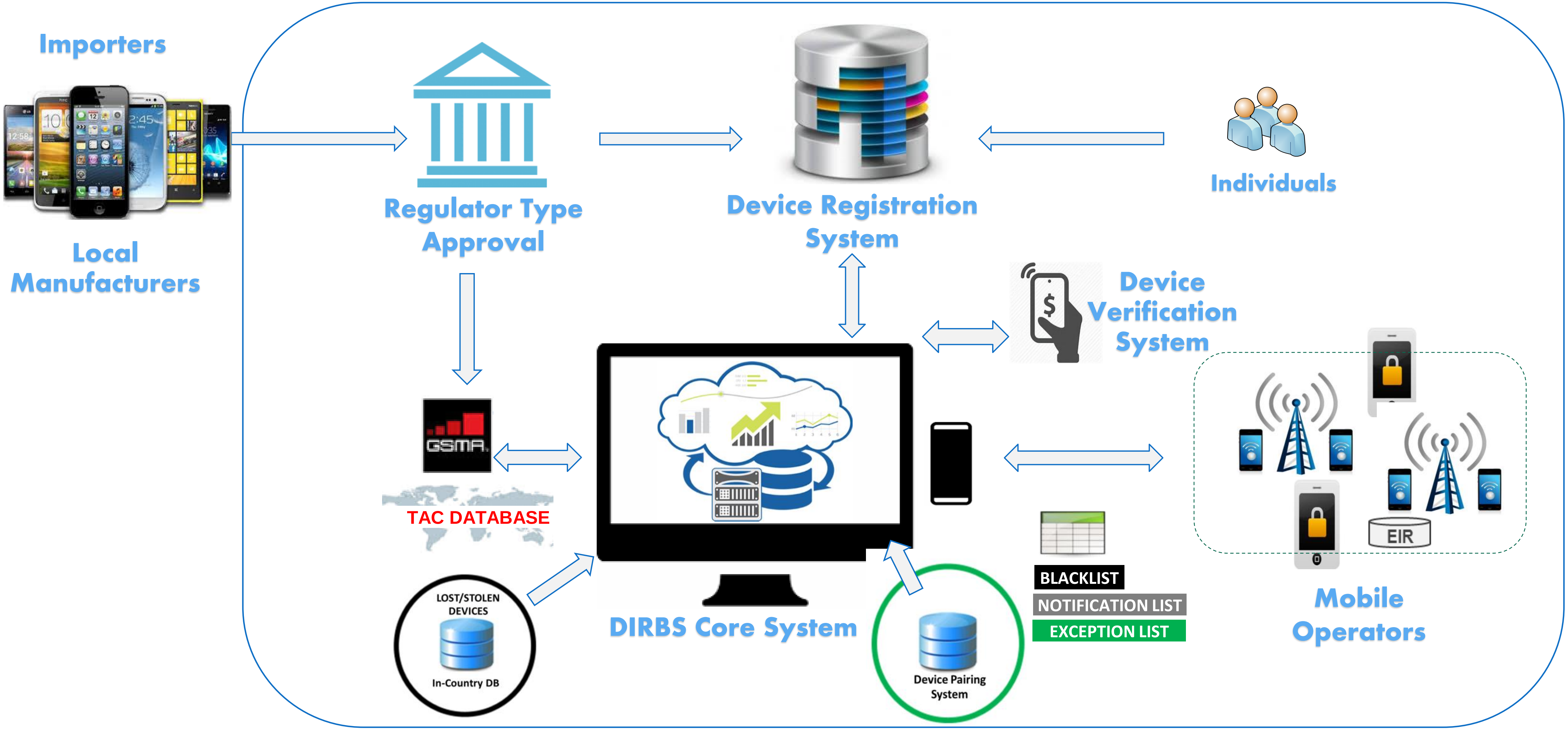
DIRBS: Device Identification, Registration, and Blocking System



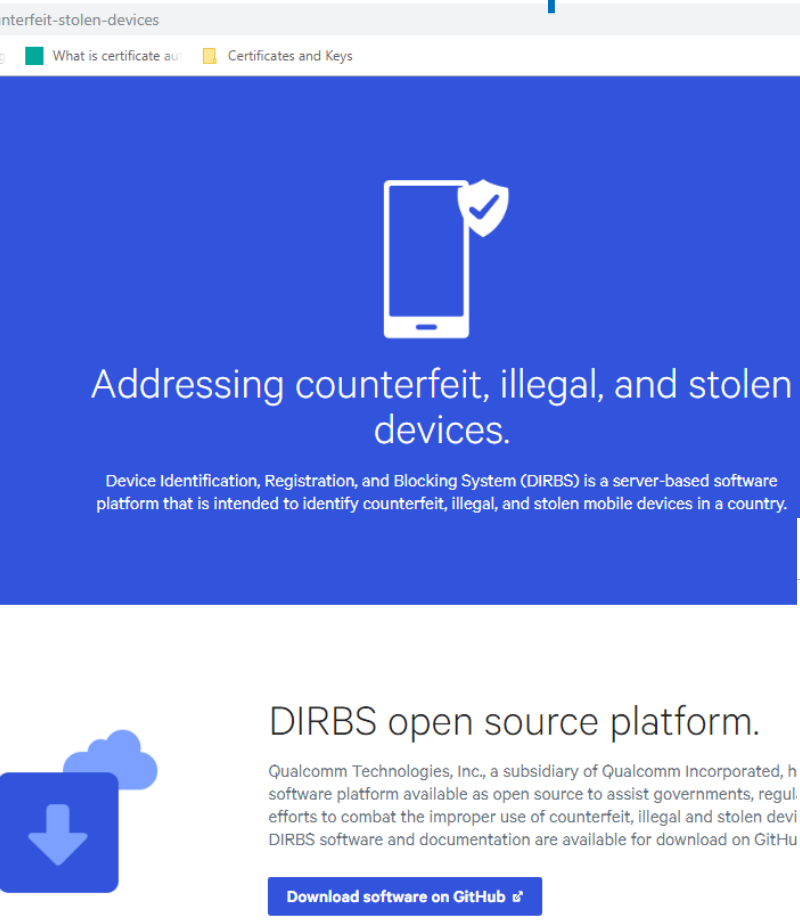
DIRBS addresses fraudulent IMEIs, illegal and stolen devices

- Allows for identification of all devices
- Captures installed base of devices
- Monitors all new device activations
- Addresses illegal and counterfeit devices
- Addresses mobile theft
- Allows for exceptions/amnesty

DIRBS: Device Identification, Registration & Blocking System



Qualcomm Technologies Inc., has Developed and Shared its Technology Platform via Open Source to Address the Issues



nterfeit-stolen-devices

What is certificate au Certificates and Keys

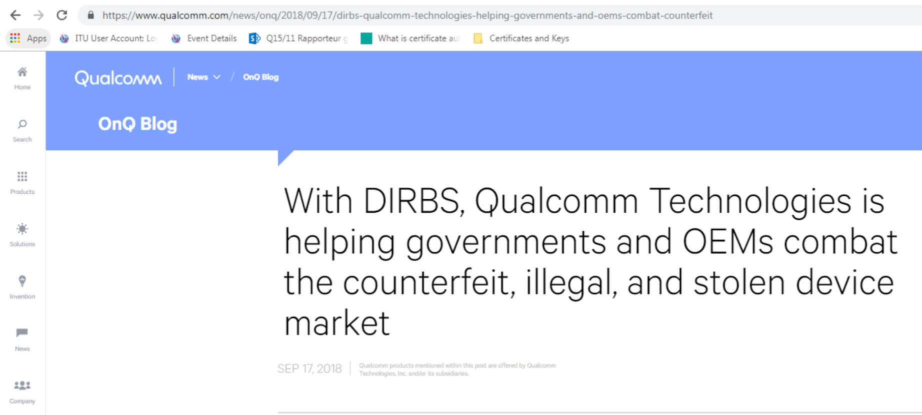
Addressing counterfeit, illegal, and stolen devices.

Device Identification, Registration, and Blocking System (DIRBS) is a server-based software platform that is intended to identify counterfeit, illegal, and stolen mobile devices in a country.

DIRBS open source platform.

Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, h
software platform available as open source to assist governments, regul
efforts to combat the improper use of counterfeit, illegal and stolen devi
DIRBS software and documentation are available for download on GitHu

Download software on GitHub



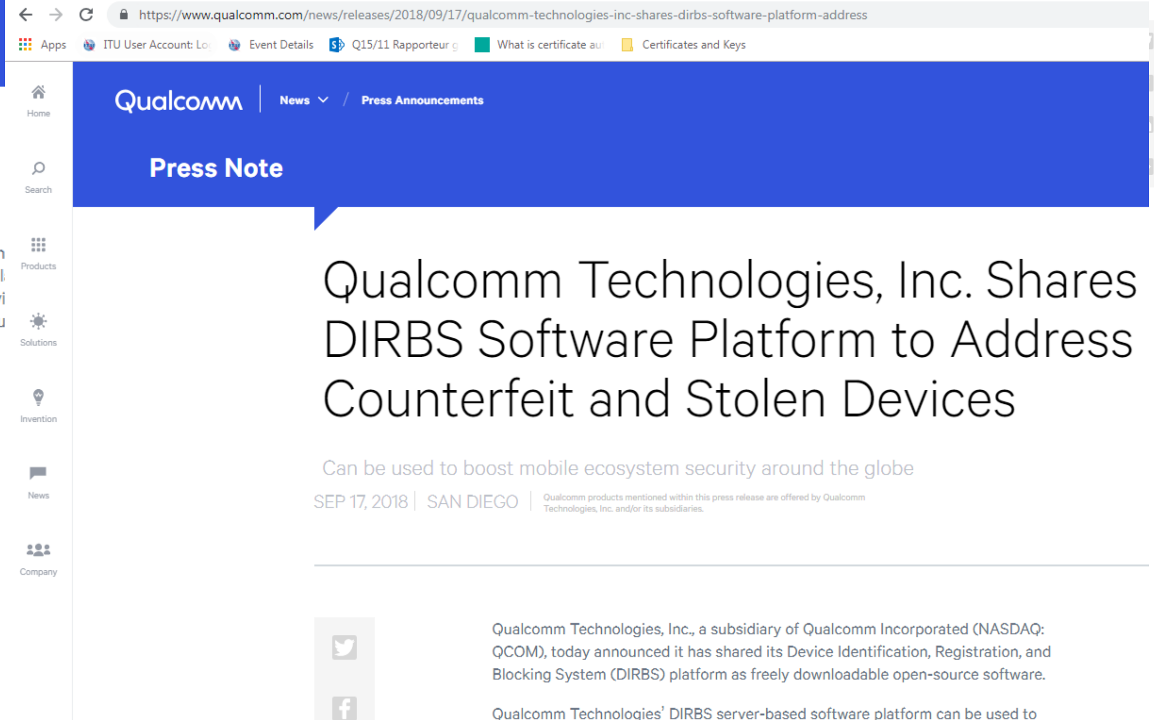
https://www.qualcomm.com/news/onq/2018/09/17/dirbs-qualcomm-technologies-helping-governments-and-oems-combat-counterfeit

Apps ITU User Account: Lo Event Details Q15/11 Rapporteur g What is certificate au Certificates and Keys

OnQ Blog

With DIRBS, Qualcomm Technologies is helping governments and OEMs combat the counterfeit, illegal, and stolen device market

SEP 17, 2018 | Qualcomm products mentioned within this post are offered by Qualcomm Technologies, Inc. and/or its subsidiaries.



https://www.qualcomm.com/news/releases/2018/09/17/qualcomm-technologies-inc-shares-dirbs-software-platform-address

Apps ITU User Account: Lo Event Details Q15/11 Rapporteur g What is certificate au Certificates and Keys

Press Note

Qualcomm Technologies, Inc. Shares DIRBS Software Platform to Address Counterfeit and Stolen Devices

Can be used to boost mobile ecosystem security around the globe

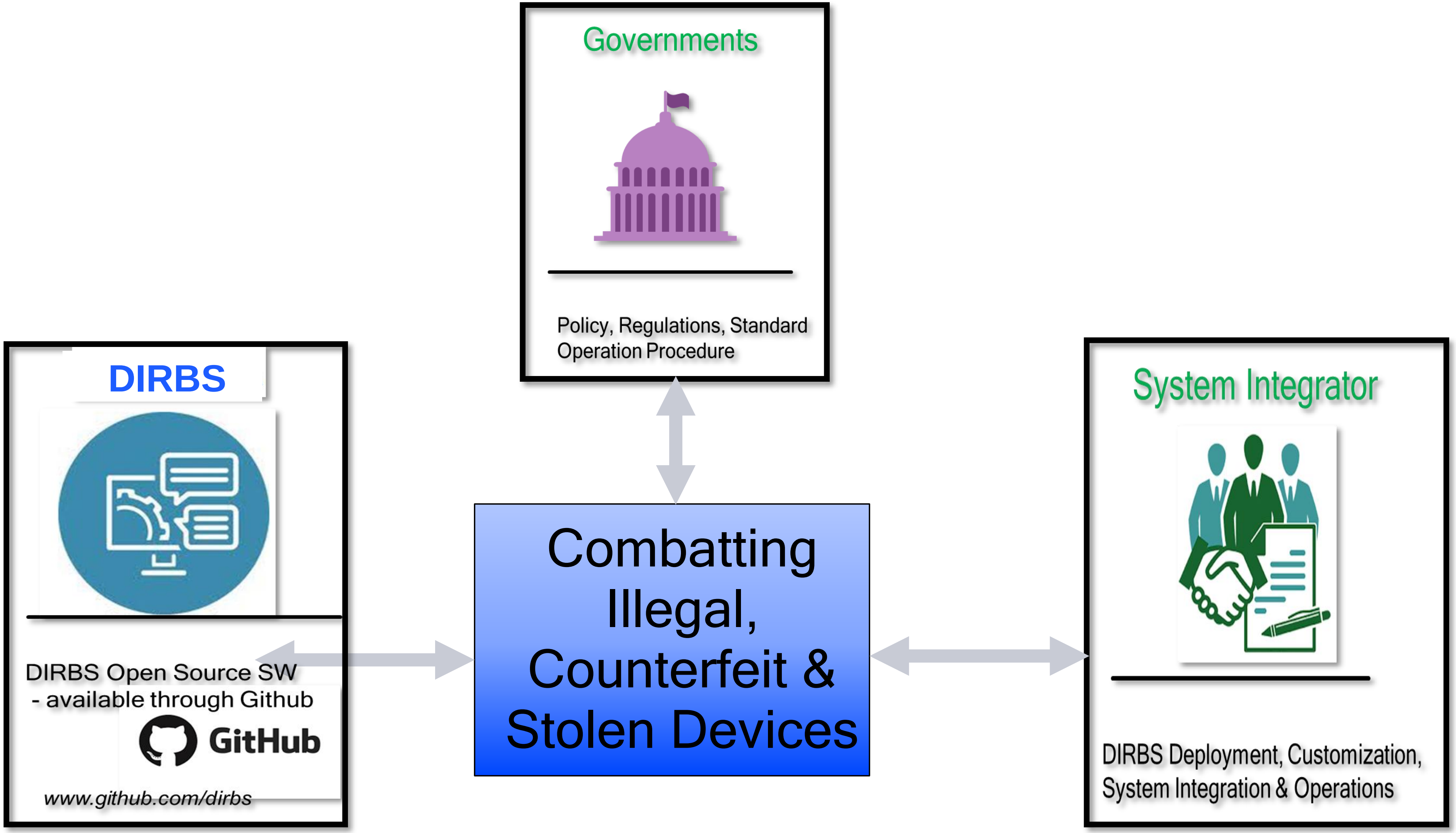
SEP 17, 2018 | SAN DIEGO | Qualcomm products mentioned within this press release are offered by Qualcomm Technologies, Inc. and/or its subsidiaries.

Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated (NASDAQ: QCOM), today announced it has shared its Device Identification, Registration, and Blocking System (DIRBS) platform as freely downloadable open-source software.

Qualcomm Technologies' DIRBS server-based software platform can be used to

- Webpage
- OnQ blog
- QC News article
- Press note

DIRBS Open Source Platform Deployment



Governments

Policy, Regulations, Standard
Operation Procedure

DIRBS

DIRBS Open Source SW
- available through Github

www.github.com/dirbs

Combatting Illegal, Counterfeit & Stolen Devices

System Integrator

DIRBS Deployment, Customization,
System Integration & Operations

Summary of Device Legislation and Regulation in Pakistan

Since 2006

IMEI Network Blocking of lost or stolen mobile devices has been in place in Pakistan

June 2016

Consultation Document issued by the Pakistan Telecommunication Authority (PTA) on a proposed Device Identification, Registration and Blocking System (DIRBS)

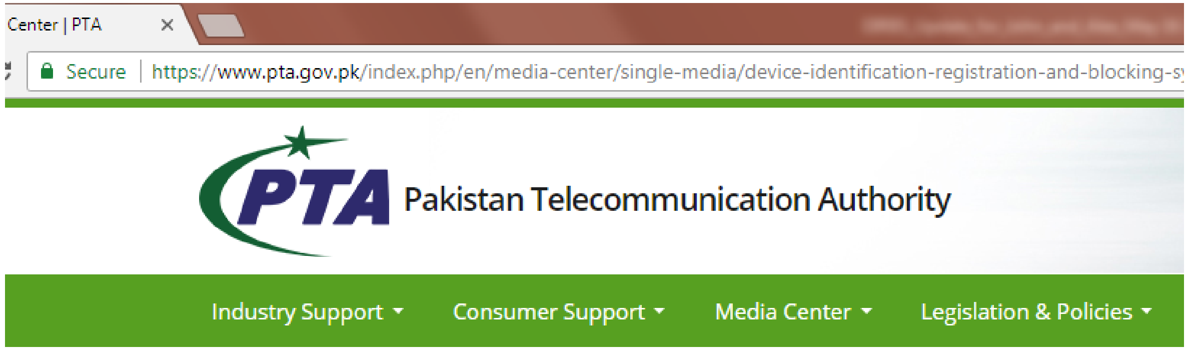
Mobile Device Identification, Registration and Blocking Regulation has been in place

Since 24th August 2017

Scope and Applicability of the Regulations:

- Apply to all MNO(s), Type Approval Holders; Authorized Distributors and OEM/ODM for registration and maintenance of accurate data of mobile device(s) and IMEI(s),to ensure the sale, purchase and provision of mobile communication service(s) to Compliant Mobile Device(s) only, through DIRBS System
- All Type approval holders/authorized distributors/OEM/ODM and Mobile Network Operators(MNOs) shall co-operate with the Authority to ensure that non-compliant mobile devices are not imported, sold, marketed or connected with the mobile operators' networks.
- Mobile devices reported as stolen, blocked or bearing a duplicate or non-standard IMEI shall be blocked by MNO(s)

DIRBS OFFICIALLY LAUNCHED IN PAKISTAN!



Center | PTA

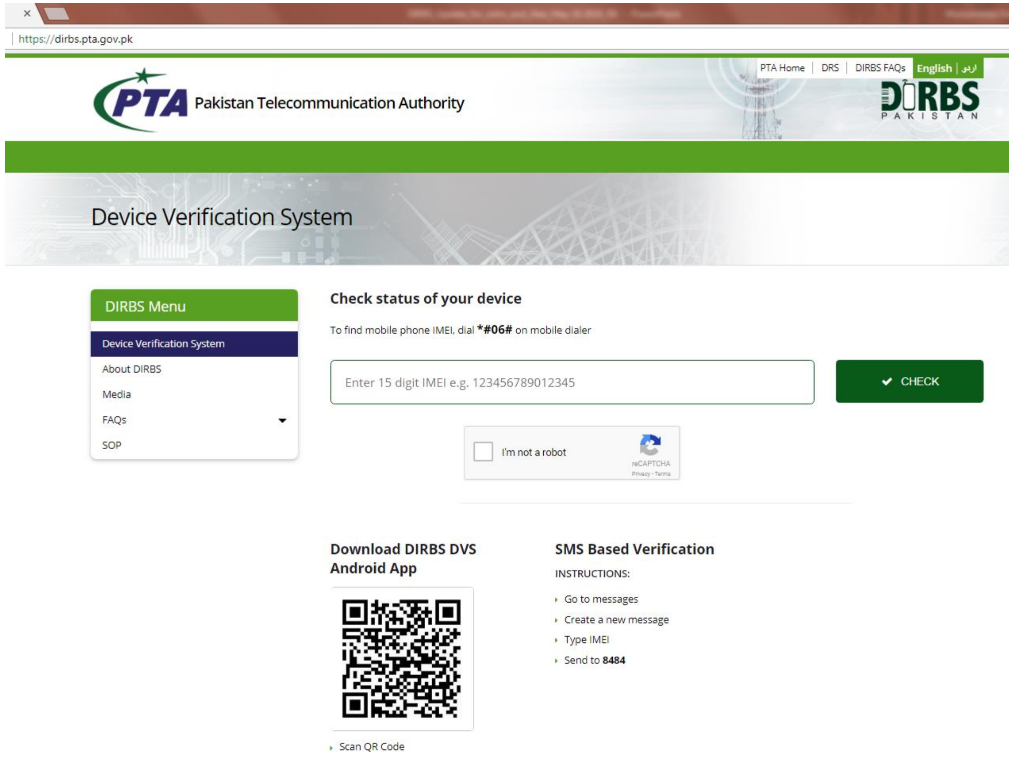
Secure | https://www.pta.gov.pk/index.php/en/media-center/single-media/device-identification-registration-and-blocking-sy

Press Release

May 10, 2018

DEVICE IDENTIFICATION REGISTRATION AND BLOCKING SYSTEM (DIRBS) LAUNCHED AT PTA

Islamabad: In line with the Telecom Policy 2015, Pakistan Telecommunication Authority (PTA) launched Device Identification, Registration and Blocking System (DIRBS) in collaboration with 3G Technologies today here at PTA Headquarters Islamabad. Chairman PTA Mr. Mohammad Naveed was the chief guest while Mr. Abdul Samad, Member Compliance and Enforcement PTA, Executive Director, 3G Technologies, IT and telecom industry experts, CEOs of telecom companies, representatives from FBR and media community attended the event. Member Compliance & Enforcement gave presentation on DIRBS during the event.



https://dirbs.pta.gov.pk

PTA Home | DRS | DIRBS FAQs | English | اردو
PTA
Pakistan Telecommunication Authority
DIRBS
PAKISTAN
DIRBS Menu
Device Verification System
About DIRBS
Media
FAQs
SOP
CHECK
I'm not a robot
reCAPTCHA
Privacy - Terms

Device Verification System

Check status of your device

To find mobile phone IMEI, dial ***#06#** on mobile dialer

Enter 15 digit IMEI e.g. 123456789012345

Download DIRBS DVS Android App

- Scan QR Code

SMS Based Verification

INSTRUCTIONS:

- Go to messages
- Create a new message
- Type IMEI
- Send to **8484**

October 4, 2018

Qualcomm

Contact:

Mohammad Raheel Kamal

Senior Director
Qualcomm Technology Licensing
mkamal@qualcomm.com

Chair: Counterfeit & Security Working Group (MWF)
Chair: Joint Device Identification Taskforce (GSMA / MWF)

Qualcomm

Thank you!

Follow us on: f 🐦 in

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes Qualcomm’s licensing business, QTL, and the vast majority of its patent portfolio. Qualcomm Technologies, Inc., a wholly-owned subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of Qualcomm’s engineering, research and development functions, and substantially all of its product and services businesses, including its semiconductor business, QCT.