October, 2019

ITU Bishkek

DIRBS

Prevention of Counterfeit and illegal Devices for a Healthy Mobile Ecosystem

Challenges, Regulatory Framework & Open Solutions

Impact of Fraudulent/Counterfeit Devices

Consumer

- Poor performance and reliability
- Theft/ privacy issues
  (No blocking of stolen devices)

Government

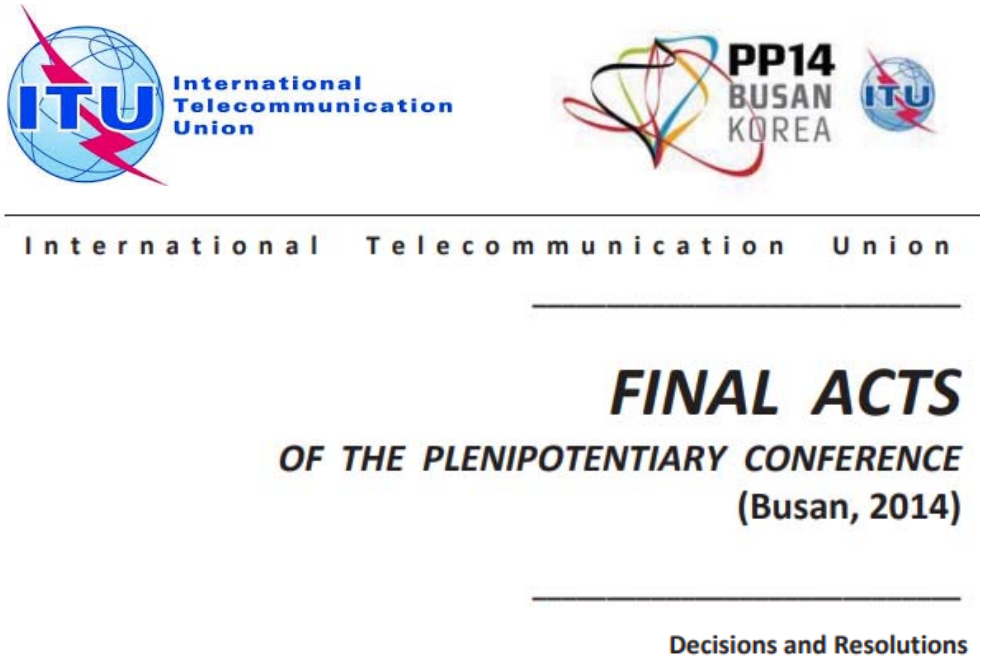
- Non-compliant device ecosystem
- Security / Consumer Protection
- Tax Revenue Lost

Operator

- QoS
- Network Capacity
- Interference

Manufacturers

- Loss of sales
- Unfair competition and pricing pressure



Resolution 188 (Dubai, 2018): Combating counterfeit telecommunication/information and communication technology devices

Resolution 189 (Dubai, 2018): Assisting Member States to combat and deter mobile device theft

- 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
- Tampering with unique device identifiers diminishes the effectiveness of solutions adopted by countries

Multiple I elated issues impacting the stakeholders

Types of Fraudulent IMEIs

Malformed IMEIs

Do not meet format requirements

MNV12KvuGS8WRTY
1122334455667788
11111

Misused IMEIs

Old TAC used on a newer device

491234567891234

Invalid IMEIs

Not allocated by the GSMA

351234567891234

Transient IMEIs

Equipment constantly changes IMEIs

Duplicate IMEIs

Same IMEI cloned on multiple devices

356938035643809
356938035643809
356938035643809

Non-Approved IMEIs

Non-homologated/Type Approved
Illegal imported

Overview of International IMEI Regulations

- Many counties at different stages in the fight against fraudulent and counterfeit devices

Type Approval

- ✓ Colombia
- ✓ Brazil
- ✓ India
- ✓ Pakistan
- ✓ Turkey
- ✓ Russia
- ✓ Azerbaijan
- ✓ Egypt
- ✓ Indonesia
- ✓ Vietnam
- ✓ Kenya
- ✓ Sri Lanka
- ✓ Denmark
- ✓ Sweden
- ✓ United Kingdom
- ✓ France
- ✓ Germany
- ✓ Austria
- ✓ Italy
- ✓ Greece
- ✓ Finland
- ✓ Norway

IMEI Requirement & Validation

- ✓ Colombia
- ✓ Brazil
- ✓ India
- ✓ Pakistan
- ✓ Turkey
- ✓ Azerbaijan
- ✓ Egypt
- ✓ Kenya
- ✓ Sri Lanka
- ✓ Ethiopia
- ✓ Kazakhstan
- ✓ Nigeria
- ✓ Uganda
- ✓ Ukraine
- ✓ Vietnam*
- ✓ Argentina*
- ✓ Indonesia*

**in process*

IMEI Tampering Laws

- ✓ Turkey
- ✓ Kenya
- ✓ Sweden
- ✓ Czech Republic
- ✓ United Kingdom
- ✓ France
- ✓ Lithuania
- ✓ Estonia
- ✓ Germany
- ✓ Austria

List above is not intended to be comprehensive, for discussion purposes only
Type approval - country regulator has an established device type approval process before a device can be activated on network
IMEI Requirement & Validation - country has some form of IMEI validation, could be basic IMEI check or full device registration and blocking
IMEI Tampering Laws - country has laws criminalizing the tampering and/or modification of a device's IMEI with some including jail time

Problem Continues Despite Industry's Actions

Operators actions are generally limited to blocking stolen IMEIs

Mobile Operators

Specifications / Standardization

3GPP has identified device authentication as an issue: SMARTER Study Item (sec 5.63.3) and SA3 Key Issue #2.4 in TR 33.899

Multiple proposals submitted; MMF Requested to take the SI forward as a WI for Rel 15

Market Surveillance / Law Enforcement

Solution?

Network Access Control under the Government Mandate

Control at Source / Export Points

GSMA, MWF, Qualcomm presented and discussed the issues for China Customs

GSMA

Blacklisting; IMEI Training; DSG Initiatives for IMEI security and strengthening

Device Security / IMEI Strengthening

Control at Import Points / Customs

IPM INTERFACE PUBLIC-MEMBERS THE WCO TOOL IN THE FIGHT AGAINST COUNTERFEITING

• Regulatory Framework for Combatting Counterfeiting & Device Theft

Key Elements of the Framework

Requiring Type Approval

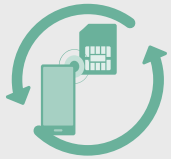
- Ensures device authenticity and standards conformance

Mandating Device Registration

- Ensures IMEI uniqueness
- Curbs counterfeiting
- Eliminates illegal import
- Allows for blocking of stolen devices

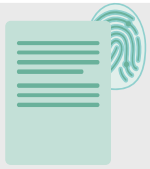
Providing Verification Systems

- Mechanism for users to verify device status and its authenticity



Granting Amnesty

- Allowing existing fraudulent devices to operate on the networks before phasing them out



Reporting Lost/Stolen Devices

- Mechanism to report lost and stolen devices to allow for network blocking

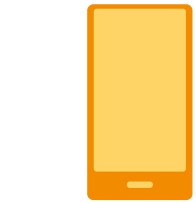
Mandating Device Blocking

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

Stakeholders Roles & Responsibilities

Government

- Develop Regulatory Framework for device registration and blocking of Non-approved, Illegal and Stolen devices
- Implement Standard Operating Procedure
- Deploy and Administer a technology platform to enforce regulations



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 and Device Pairing
- Notify subscribers of their device status via SMS as required

Consumers

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

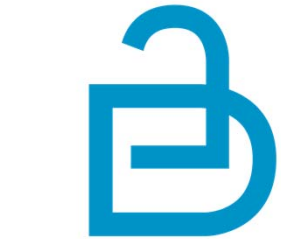
Technical Framework for Combatting Counterfeiting and Mobile Theft

1. Classify Existing Devices	2. Allow All Existing Devices	3. Register New Devices	4. Detect IMEI Falsification	5. Enable Network Blocking
• Analyze device data from network information • Classify devices by their IMEIs (valid / invalid, unique / duplicate)	• Pair existing fraudulent IMEIs with IMSIs	• Require Type Approval with unique device identifiers • Register imported & locally produced devices with valid and unique identifiers only	• Analyze network data • Identify devices with fraudulent IMEIs	• Control access of devices - that do not have certification or are not registered - through network control

This Frameworks 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
- 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
- Standalone system alleviating the need for mobile network integration and interoperability that cause unnecessary cost, capacity constraint and resource burden on the operators
- Provides tools for users to check device validity before purchase



DIRBS

Device **I**dentification, **R**egistration, and **B**locking **S**ystem (**DIRBS**) is a server-based software platform that is intended to identify counterfeit, illegal, and stolen mobile devices in a country.

DIRBS Open Source

DIRBS Open Source Resources

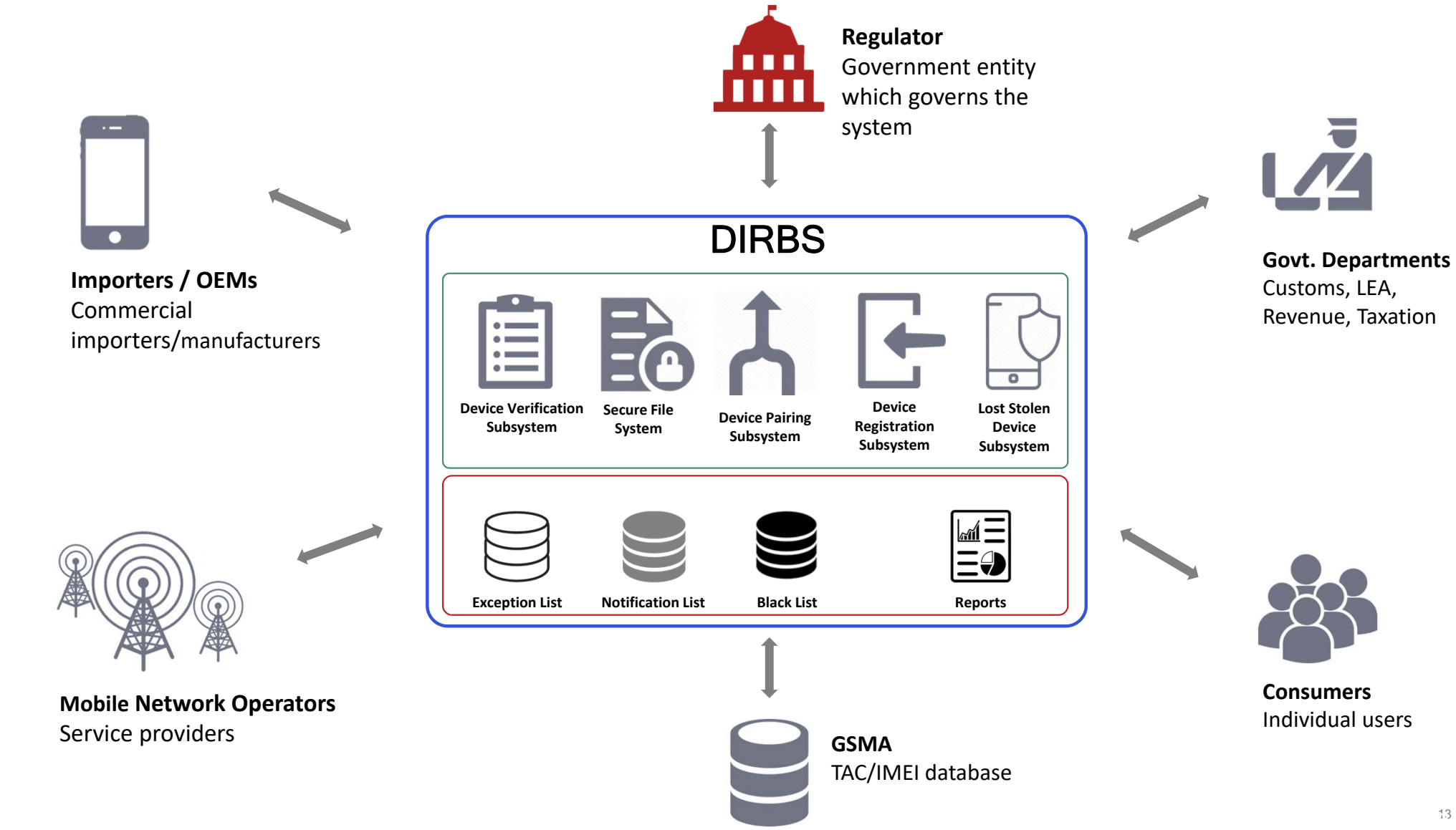
- DIRBS Open Source provides free DIRBS software including the source code
- DIRBS Open Source Software and documentation is available in Public Domain

DIRBS Deployment

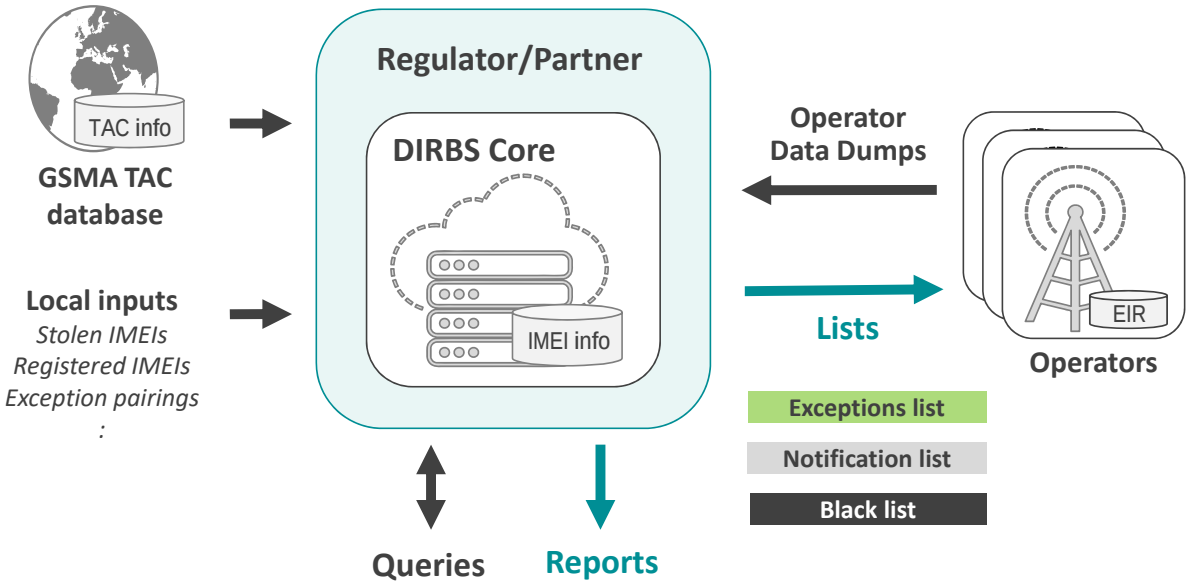
- Governments deploy DIRBS platform through in-house experts or through outsourcing the implementation to third parties

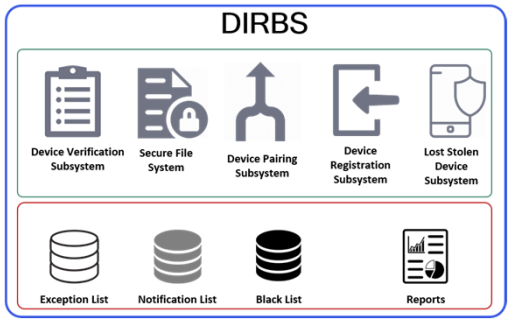
DIRBS Operation

- Governments in charge of the Software, System Operation and Maintenance of the DIRBS Platform
- Operators maintain their EIR Operations


Regulator
Government entity which governs the system
DIRBS
Device Verification Subsystem
Secure File System
Device Pairing Subsystem
Device Registration Subsystem
Lost Stolen Device Subsystem
Exception List
Notification List
Black List
Reports
Importers / OEMs
Commercial importers/manufacturers
Govt. Departments
Customs, LEA, Revenue, Taxation
Mobile Network Operators
Service providers
Consumers
Individual users
GSMA
TAC/IMEI database

- All operators provide data to country's centralized DIRBS
- IMEIs are classified using configurable conditions
- Lists are generated for operators
- Reports are generated at operator and country levels
- Subsystems interface with core analysis engine



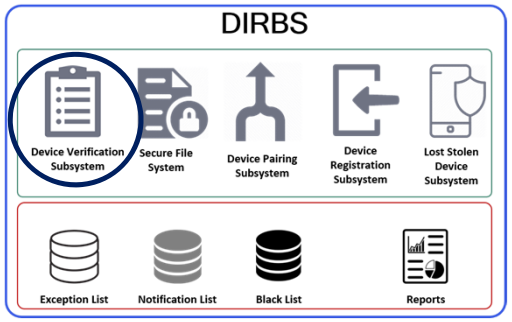


Core Analysis Engine

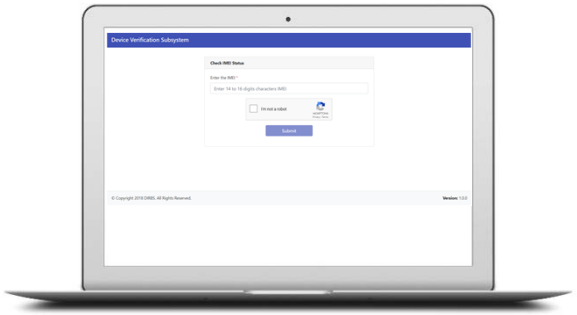
DIRBS Core is an analysis engine that ingests data from multiple sources and classify IMEIs based on a wide array of dimensions. A dimension defines an analysis algorithm along with any configuration (e.g. thresholds, duration, etc.) used by that algorithm to determine whether condition is met or not met.

Device Verification Subsystem

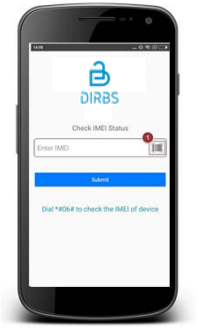
The Device Verification Subsystem (DVS) provides platform for public to check basic status of an IMEI and Authorized entity(s) to verify detail of an IMEI



DVS provides three methods for IMEI verification

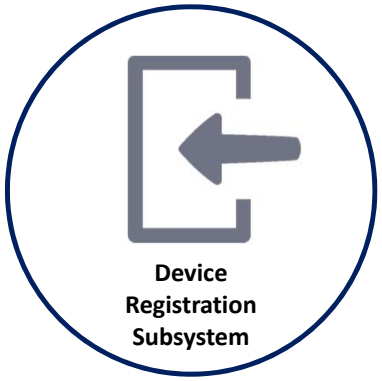


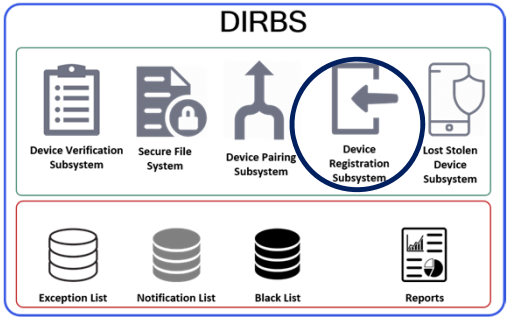
Web Portal



Mobile App

SMS





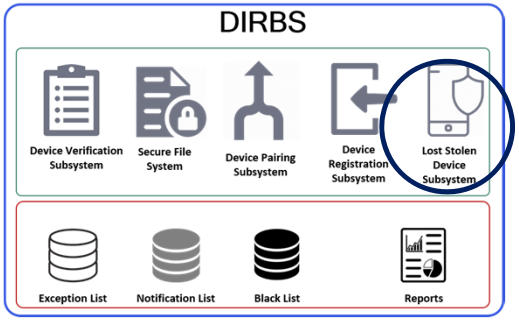
Device Registration Subsystem

Device Registration Subsystem (DRS) provides a platform for individuals and commercial importers/manufacturers to register device(s)

It provides interface for authority to review registration request and take appropriate action

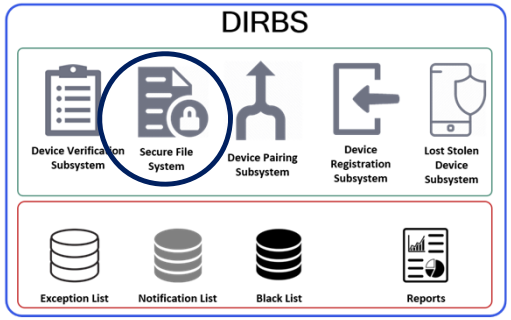
Lost Stolen Device Subsystem

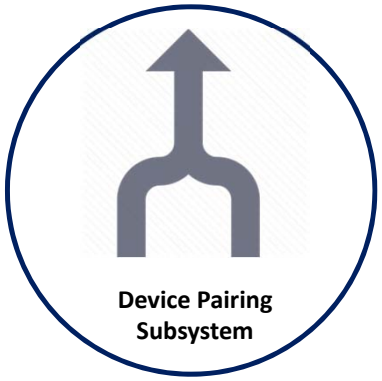
Lost & Stolen Device Subsystem (LSDS) provides a platform for authorized entity to register a report for lost/stolen device(s) of an affected consumer

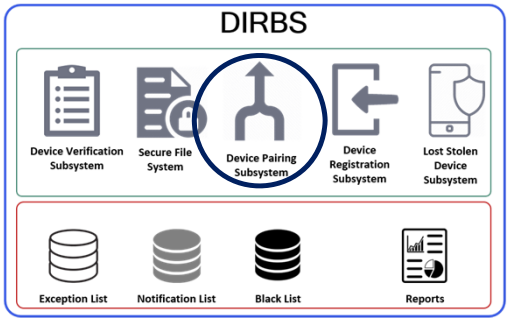


Secure File System

Secure File System provides a secure interface for MNOs to upload device dumps for analysis and download lists to be implemented on their EIR



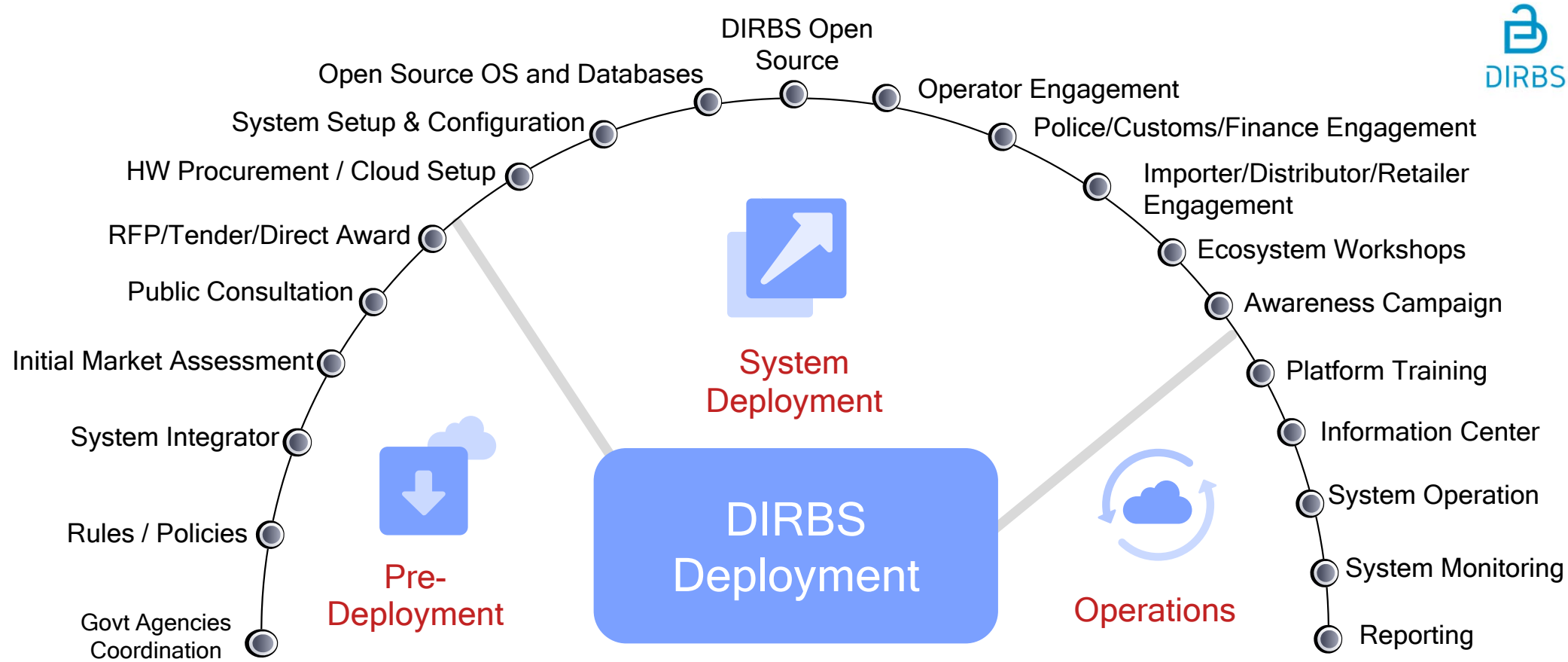




Device Pairing Subsystem

The Device Pairing Subsystem (DPS) provides a SMS platform for subscribers to manage their pairings.

It provides a web interface for authority to generate new pairing codes and for MNOs to add IMSI information for pairs.

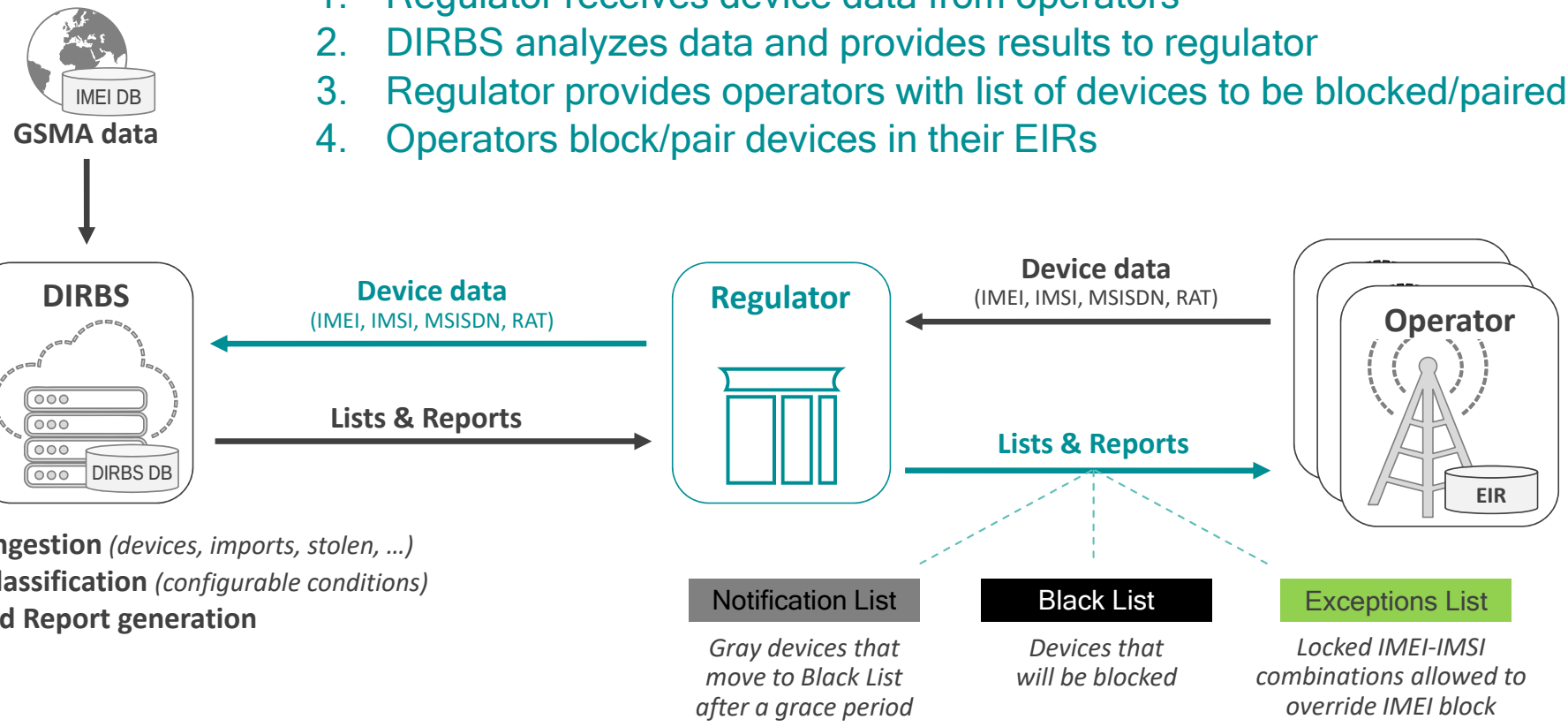


DIRBS Implementation Framework

DIRBS Concept

Analysis of observed device data

1. Regulator receives device data from operators
2. DIRBS analyzes data and provides results to regulator
3. Regulator provides operators with list of devices to be blocked/paired
4. Operators block/pair devices in their EIRs



Data ingestion *(devices, imports, stolen, …)*
IMEI classification *(configurable conditions)*
List and Report generation

DIRBS

Dashboard | Core | DRS | LSDS | DVS | DPS

Hi, John

Total IMEIs
196,578,977
Monthly Average
58,480 | ↑2.5%

Total Valid IMEIs
146,522,917
Monthly Average
43,746 | ↓2.1%
62%

Total Invalid IMEIs
26,123,933
Monthly Average
3,746 | ↑1.1%
38%

Total Paired IMEIs
34,423,933
Monthly Average
7,346 | ↑0.1%
65%

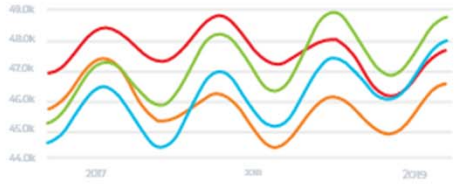
Total Stolen IMEIs
423,933
Monthly Average
746 | ↑0.1%
22%

Total Blocked IMEIs
233,933
Monthly Average
346 | ↑4%
20%

Operator Wise IMEIs
143K

Operator1	143,564,77
Operator2	1,564,77
Operator3	85,564
Operator4	55,664

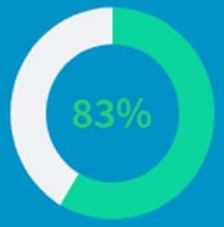
Operator Wise Trend



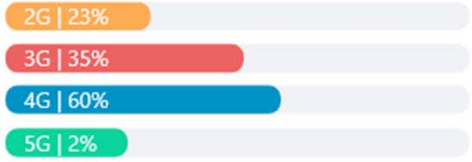
DRS IMEIs
113K

Jan 4K | Feb 7K | Mar 9K

Devices | 83K



Technology Wise Devices



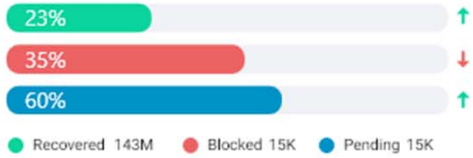
IMEIs Pairing

Paired	143,564,77
Unpaired	1,564,77

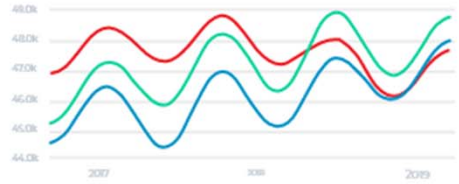
Operaor Wise IMEIs Pairs

Operator1	143,564,77
Operator2	1,564,77
Operator3	564
Operator4	564

Stolen Devices
43K



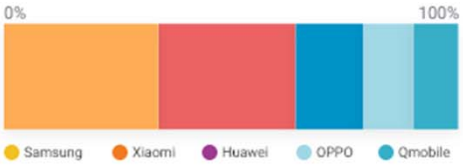
Stolen Devices Trend



Operator Wise Blocking

Operator1	143,564,77
Operator2	1,564,77
Operator3	43,756
Operator4	34,564

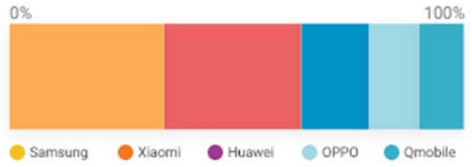
Top Registered Brands



Pairs Created

Active	143,564,77
Deleted	1,564,77
Permanent	564
Temperory	564

Most Stolen Brands



DIRBS View

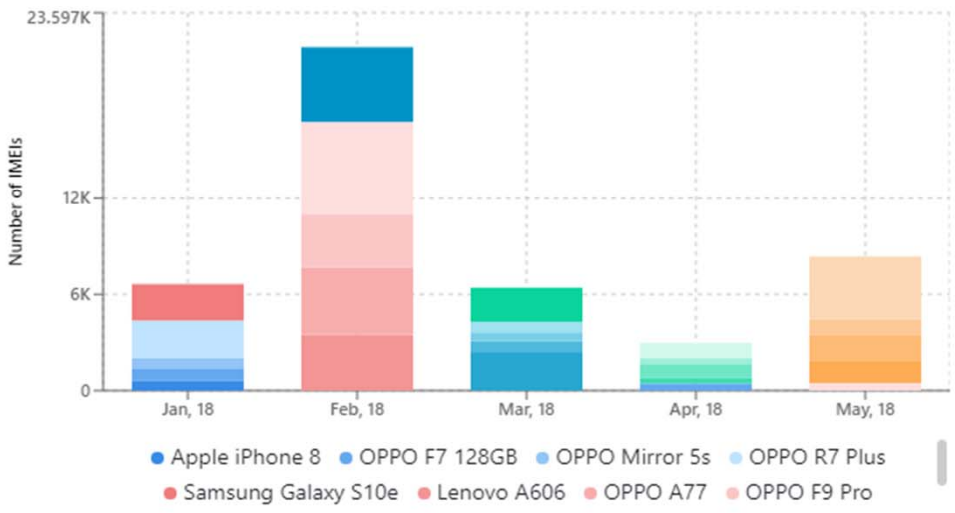
Hi, dv_authority

Home / Core / Range Graphs

Unique IMEIs	Compliant IMEIs	Non Compliant IMEIs	Black List IMEIs	Exception List IMEIs	Notification List IMEIs
2,683,996	909,220	1,774,776	1,175,485	1,201,258	751,053

Applied Filters: Granularity: **monthly** Date Range : **2019-01-01 - 2019-08-05** Trend Quantity : **5**

Registration List Top Models by IMEI Count



Top Model Details *(Representing 26.05% of total count)*

Model	Make	Device Type	Brand	RAT	Count
OPPO Neo 5s	Oppo	SmartPhone	Oppo	2G	6,522
Samsung Galaxy Note 9	Samsung	SmartPhone	Samsung	2G,3G	4,829
OPPO A77	Oppo	SmartPhone	Oppo	2G	4,540
Lenovo A606	Lenovo	SmartPhone	Lenovo	2G	3,994

DIRBS View

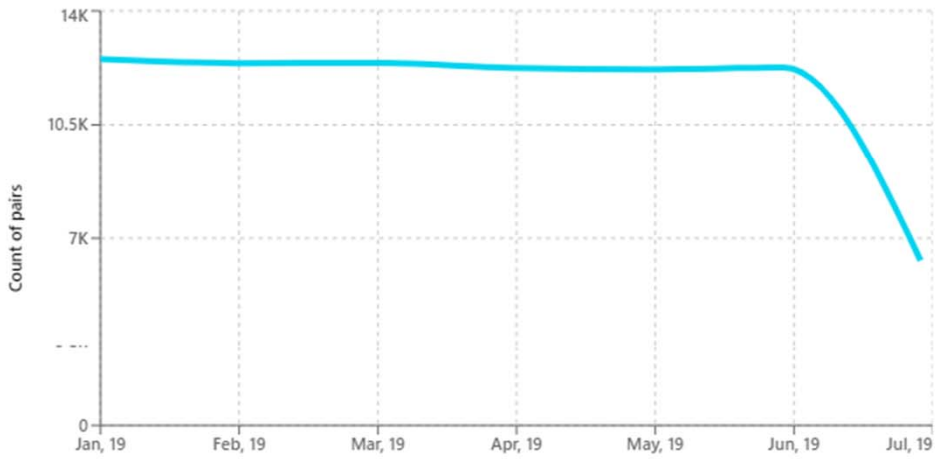
Hi, dv_authority

Home / DPS

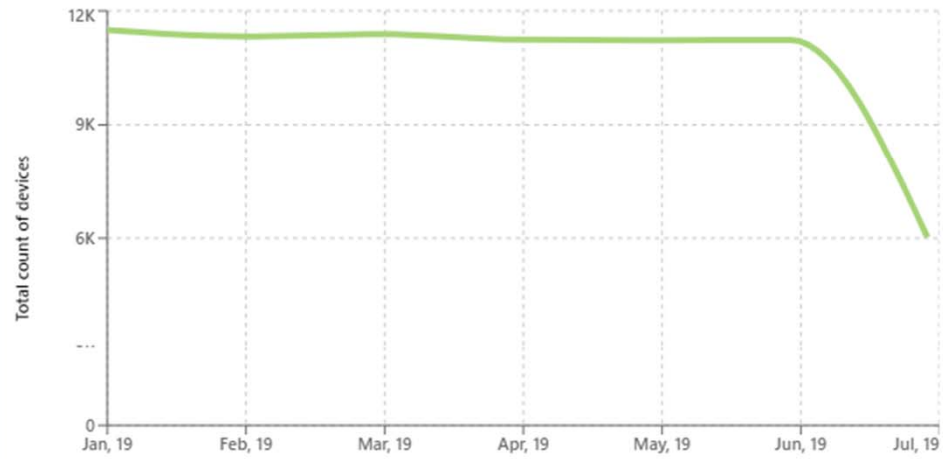
Paired Devices	Paired IMEIs	Paired IMSIs	Paired MSISDNs	IMEI-IMSI Pairs	IMEI-MSISDNs Pairs
97,048	274,307	315,442	349,269	1,219,555	1,219,588

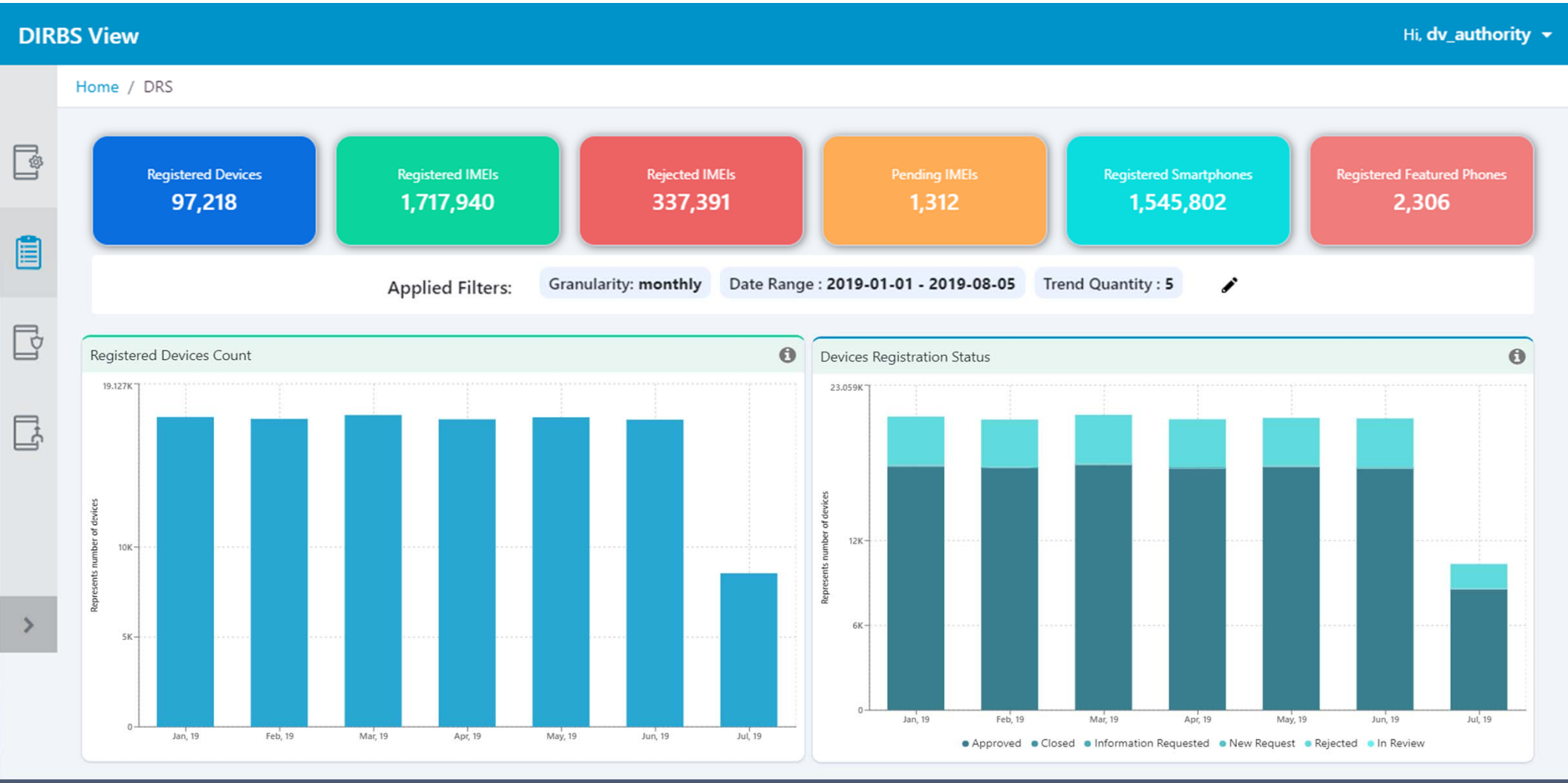
Applied Filters: Granularity: **monthly** | Date Range : **2019-01-01 - 2019-08-05** | Trend Quantity : **5** | Network Operator : **All**

Number of Permanent Pairs



Number of Devices Paired




DIRBS View
Hi, dv_authority
Home / DRS
Registered Devices
97,218
Registered IMEIs
1,717,940
Rejected IMEIs
337,391
Pending IMEIs
1,312
Registered Smartphones
1,545,802
Registered Featured Phones
2,306
Applied Filters:
Granularity: monthly
Date Range : 2019-01-01 - 2019-08-05
Trend Quantity : 5
Registered Devices Count
19.127K
10K
5K
0
Represents number of devices
Jan, 19
Feb, 19
Mar, 19
Apr, 19
May, 19
Jun, 19
Jul, 19
Devices Registration Status
23.059K
12K
6K
0
Represents number of devices
Jan, 19
Feb, 19
Mar, 19
Apr, 19
May, 19
Jun, 19
Jul, 19
Approved
Closed
Information Requested
New Request
Rejected
In Review

DIRBS View

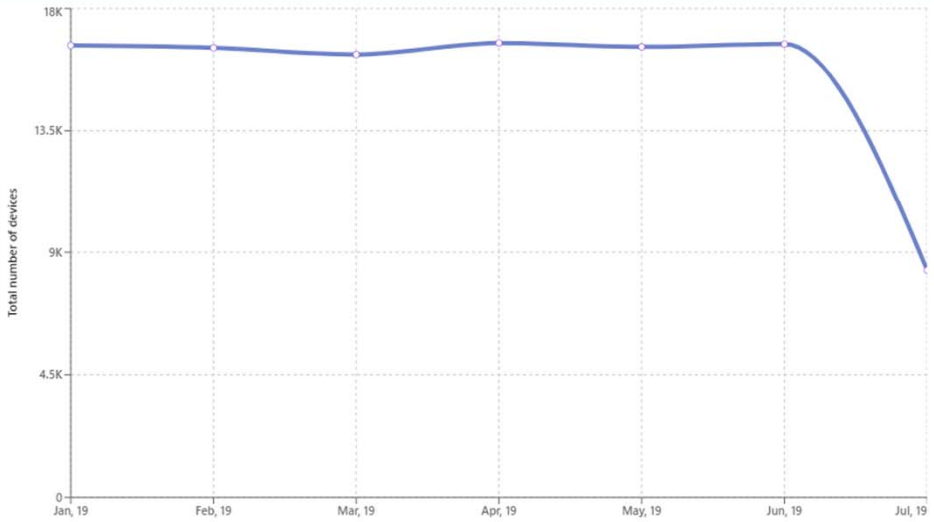
Hi, dv_authority

Home / LSDS

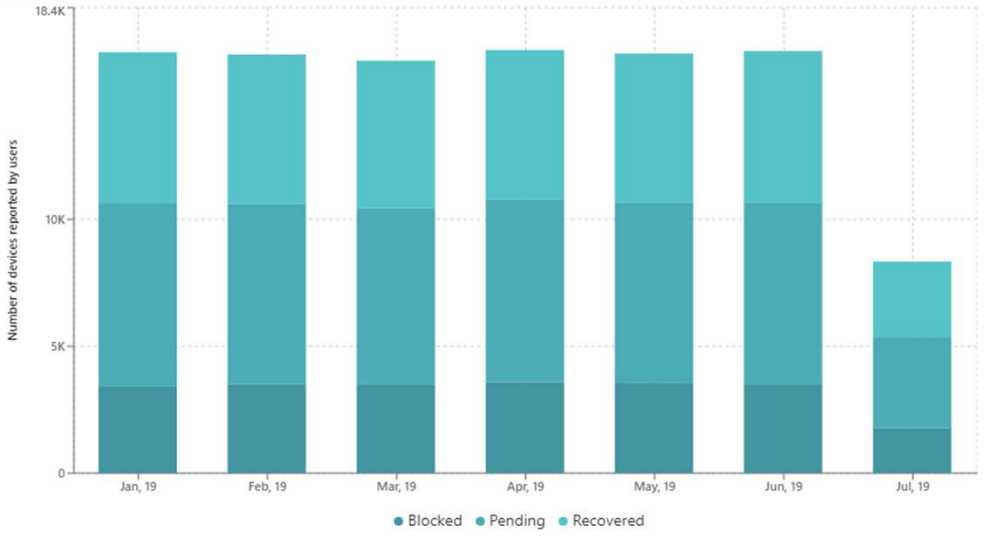
Stolen Devices	Reported Devices	Lost Devices	Recovered Devices	Pending Devices	Blocked Devices
1,410,984	1,662,772	248,429	596,681	712,169	350,436

Applied Filters: Granularity: **monthly** Date Range : **2019-01-01 - 2019-08-05** Trend Quantity : **5**

Number of Reported Devices



Status of Reported Devices



Government

- Reduced stolen devices
- Protect Import duties, sales tax
- Telecom policy (certification, safety)
- Consumer protection and safety
- Environmental protection
- Security (cyber, criminal)
- Intellectual property protection

Mobile Network Operators

- Reduce sub-standard device impact on network capacity, lower costs
- Reduce churn through better experience (improve capacity, fewer drops)
- Enables device business (white label)
- Enables small installment plans with better controls

Manufacturers

- Level playing field, fair competition
- Prevent loss of sales
- Copyright / trademark protection
- Secure margins
- Brand equity / image
- Encourage investment

Consumers

- Access to legal devices, with warranty
- Decreased incentives for phone thieves
- Protection from hazardous substances (Lead, Cadium).
- Fewer bad devices inefficiently using capacity
- Quality connection (dropped calls, handover)
- Quality experience (battery, camera, display)
- Protection from malware / data protection
- Protection from excess radiation

Thank you

For more information, visit us at:
https://github.com/dirbs

Contact:

Khalid Khan
Chairman
Central Asian Cellular Forum
khalid@3gca.org