Consumer-centric framework for combating counterfeit and stolen information in practice

mediafon datapro

Counterfeit, tampered and stolen devices

- Consumers are attracted towards **counterfeit, tampered and stolen devices** due to a perceived **cost advantage**. Counterfeit and tampered vis-à-vis genuine devices with similar features. However, due to lack of awareness among consumers of other possible risks and costs associated with use of these devices, the proliferation of counterfeit and tampered devices is increasing day by day.
- **ITU-T Q.5054** recommendation aims to provide a **consumer centric framework** through a unified platform considering possible scenarios and a multipronged approach for combating counterfeit and stolen mobile telecommunication/ICT devices.
- The implementation of a Reference unified platform framework (RUPF) is a collaborative effort by key stakeholders, which include consumers, regulators, MNOs, TAC allocating bodies, OEMs, customs and excise, and LEAs.

Consumer-centric technology solutions

ITU-T Q.5054: *"Consumer-centric technology solutions may also generate a cascading effect in controlling the proliferation of counterfeit, tampered and stolen mobile telecommunication/ICT devices as the rejection of such mobile telecommunication/ICT devices by end consumers will create a huge disincentive and substantial uncertainties for players involved in the unauthorized manufacturing and trade of counterfeit and tampered ICT devices."*

Experience shows that many countries continue to implement the minimum CEIR configuration:

- Start with a lost or stolen device and continue with blocking due to an invalid TAC.
- Use scheduled file-sharing mechanisms for CEIR <> EIR integration.
- **Eliminate any interaction with the consumer** and thus avoid customer dissatisfaction.
- Select a solution that only meets the minimum requirements.

This leads to project failure and the need to restart with a new solution instead of continuing with the existing one.

Limiting access to Permitted (White) list

ITU-T Q.5054: *"The platform is likely to be target of cyberattacks by different sources and impacted parties. Counterfeiters may also try to gather the details of TAC codes and valid IMEI range being maintained in CEIR to use them for IMEI replication or cloning."*

The practice shows that:

- We need to limit access by mobile network operators (MNOs) and other interested parties to the Permitted (White) list. **They shouldn't have access to the Whitelist**. Instead, to minimize the risk of disseminating the whitelist, CEIR publishes a blacklist override (BLO) list, which is specific to each mobile network operator and contains only the IMEI-MSISDN-IMSI triplets for that operator.
- **We need to use Exception list-based model on EIR** side to control all IMEI-MSISDN-IMSI detected in the network. This will allow to:
  - Instantly track stolen devices with any newly registered IMEI-MSISDN-IMSI triplet.
  - Detect any other unusual user behavior, such as multiple IMSIs linked to a single IMEI within a certain period of time.
  - Detect SIM boxes.

mediafon datapro

RUPF security and privacy considerations

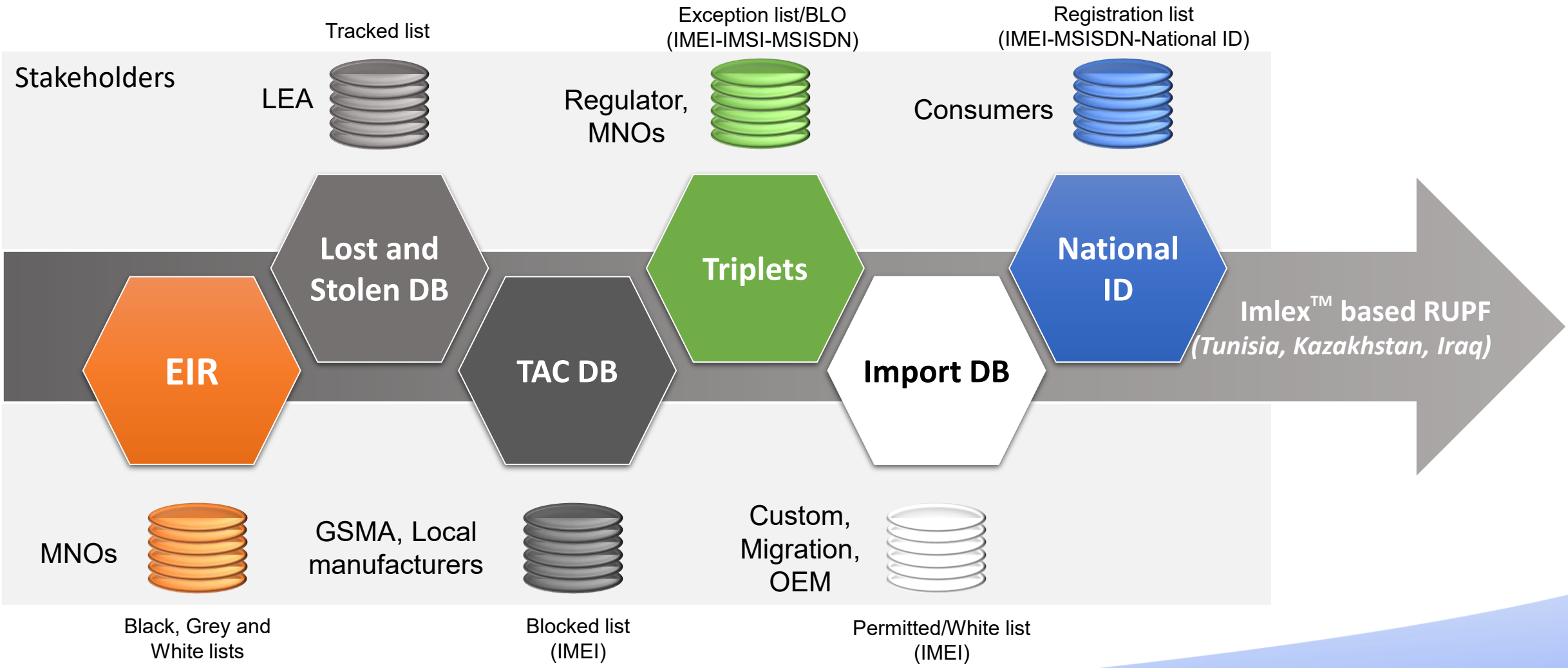
ITU-T Q.5054 Recommendation: *"The RUPF is not expected to store any consumer-specific data such as name, address, date of birth or any other personal identifier. Only IMEI-MSISDN combinations may be captured on a case-to-case basis for stolen or blocklisted devices per the requirements of platform features and functionalities."*

Experience shows the opposite: using personal data improves consumer security. Using only a national identifier (National ID) offers more comprehensive capabilities:

- It prevents device cloning to a near zero degree. IMEI once registered with one National ID can't be registered with another
- The consumer independently manages all devices and SIM cards connected to them.
- Controls the transfer of devices from the original owner to the new owner.
- After registering with a single National ID, the device can be easily used with any SIM card (MSISDN/IMSI) in use, without the need for additional registration steps.
- CEIR automatically deregisters deceased customers using the National ID.

mediafon datapro

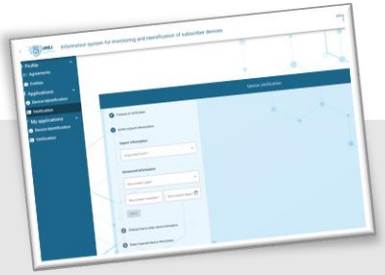
Reference unified platform framework in practice



RUPF in practice (Kazakhstan case example)

The first time a new device is used, the owner will receive a notification about the need to link the device to a national ID

RUPF will check the imported device against customs data, the migration database, the GSMA database, previously submitted applications, and devices already registered in the network and RUPF.



The user can try registering the device again. A verified and registered device guarantees its safe use by its owner.

The user purchased the device abroad

Registration of an ICT device with a National ID

Verifying a device on the Web portal or Mobile App

Verifying the device by the RUPF

Pay for devices exceeding the limit

Reregistration of the ICT device with a National ID

After attempting to register the imported device, the user will receive a notification stating that the device must be verified within 30 days on the Web portal

After the device is verified, its IMEI number will be checked to see if the import limit has been exceeded or if the excess has been paid for. If the conditions are met, the device will be whitelisted.

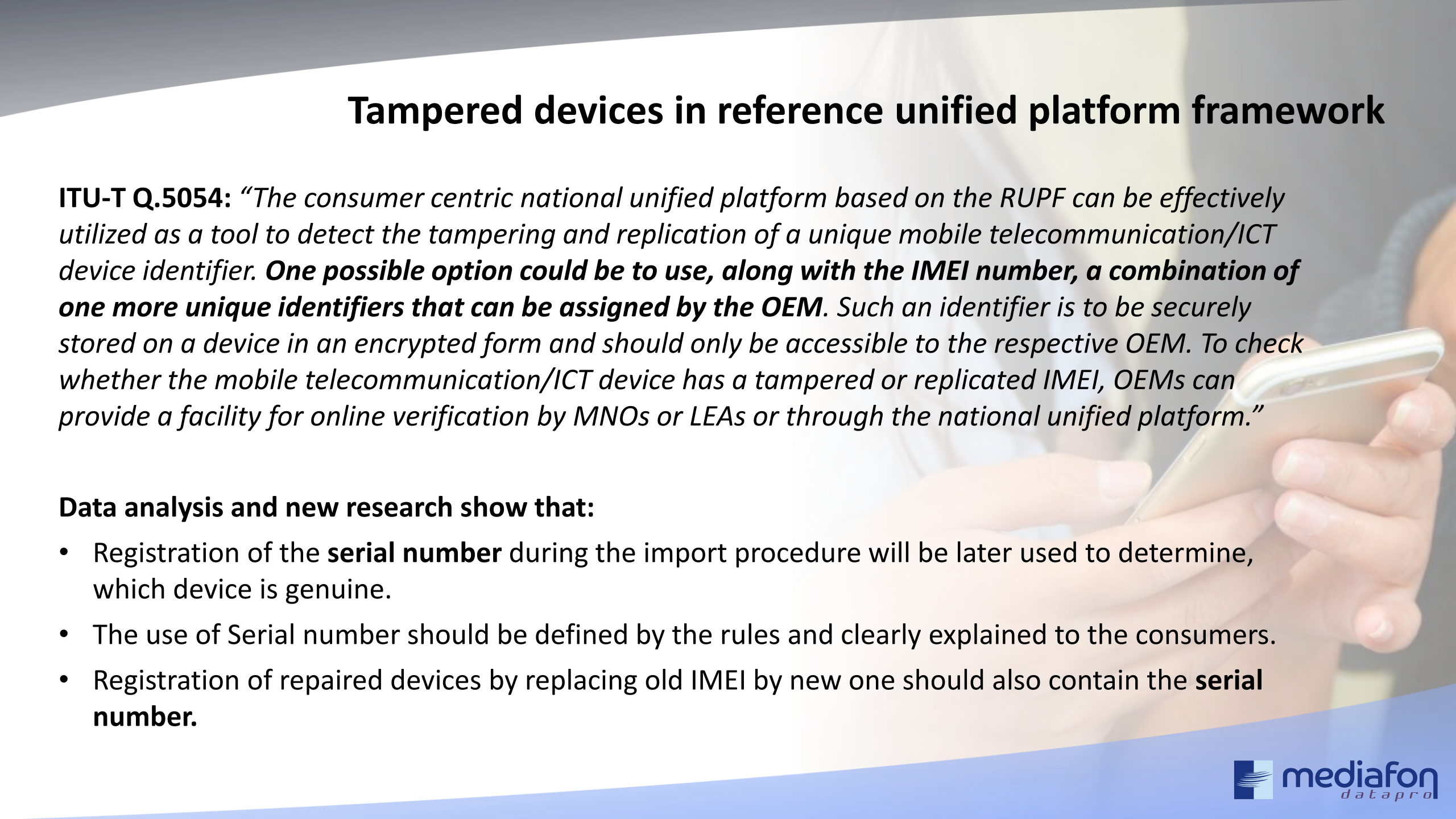
mediafon datapro

Tampered devices in reference unified platform framework

ITU-T Q.5054: *"The consumer centric national unified platform based on the RUPF can be effectively utilized as a tool to detect the tampering and replication of a unique mobile telecommunication/ICT device identifier.* ***One possible option could be to use, along with the IMEI number, a combination of one more unique identifiers that can be assigned by the OEM****. Such an identifier is to be securely stored on a device in an encrypted form and should only be accessible to the respective OEM. To check whether the mobile telecommunication/ICT device has a tampered or replicated IMEI, OEMs can provide a facility for online verification by MNOs or LEAs or through the national unified platform."*

Data analysis and new research show that:

- Registration of the **serial number** during the import procedure will be later used to determine, which device is genuine.
- The use of Serial number should be defined by the rules and clearly explained to the consumers.
- Registration of repaired devices by replacing old IMEI by new one should also contain the **serial number.**



Monitoring of deceased and inactive consumers

1. Periodically move the scheduled devices from Exception list to Old devices list

2. Request operator to deregister IMEI from Exception (BLO) list

Exception list (BLO)

Imlex™ CEIR

Temporal list for de-registered IMEIs

EIR

Old device User

5. Reregister devices found in Old devices with previous status

4. Request CEIR to check “New” device

3. Old device detected by the network

Key recommendations for a successful RUPF implementation

Mandate a RUPF: The regulator must compel all MNOs to participate. This is non-negotiable for success.

Integrate with the GSMA Global Database: This is a force multiplier that extends a nation's security perimeter globally.

Implementation of the latest technologies and developments: Using the exclusion list for full registration, serial numbers, national ID and tracking of old devices.

Harmonize Regulations: Countries must align type approval processes and technical standards to facilitate legitimate trade while impeding illicit flows.

Invest in Capacity Building: Train customs, police, and regulatory officials on device identification and the use of verification tools.

Empower Consumers: Launch ongoing awareness campaigns to create a market that rejects counterfeit goods and values security.


mediafon
datapro
Thank you!
Visit our websites at:
www.mediafondatapro.com
Or contact us info@mediafondatapro.com