GSMA Showcase Live
Device Identification and Device Verification
February 15th, 2023
About Invigo

> What we do and how the GSMA Device Database helps

- A global leader in remote Device and SIM Management solutions for mobile operators
- 1B+ devices detected and 500M+ devices configured by our solution since 2004
How device identification helps operators

> Device Management Use Cases

> Subscriber’s triplets (IMSI, IMEI, MSISDN) detected on legacy and 5G core network
> Subscriber's device model and attributes identified thanks to the GSMA Device Database
How device identification helps operators

Device Detection & Seamless Configuration

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Marketing Name</th>
<th>Technical Name</th>
<th>Year</th>
<th>OS</th>
<th>Volte</th>
<th>Device Type</th>
<th>Dual sim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>iPhone 13 PRO</td>
<td>A2638</td>
<td>2021</td>
<td>iOS 15.x</td>
<td>Yes</td>
<td>Phablet</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Device Information: Apple A2638/Apple iPhone 13 PRO

- **Id**: aBskSh
- **Manufacturer**: Apple
- **Model**: Apple A2638/Apple iPhone 13 PRO
- **Picture**: apple_iphone_13_pro.jpg
- **Release Date**: 2021
- **GSMA Manufacturer**: Apple Inc
- **Marketing Name**: iPhone 13 PRO
- **Technical Name**: A2638
- **Device Type**: Phablet
- **Predecessor Model**: N/A
- **OTA Support**: Yes

Detected subscribers: 1

Download

1/1
How device identification helps operators

> Advanced Device Reporting

> Informed network investment decision for 5G, eSIM, VoLTE, etc.
> Deal negotiation with device manufacturers
How device identification helps operators

> Device based Promotions

Preferential tariff applied for subscribers changing to a Samsung device
How device verification helps law enforcement

> The Problem of Device Fraud

- Substandard Devices with Illegitimate IMEIs
- Illegally Imported Devices
- Stolen Devices
- Devices with Duplicate IMEIs
- Devices with Changing IMEIs
How device verification helps law enforcement

> The Impact of Device Fraud

**Security Risks**
- Use of counterfeit and cloned devices for criminal acts
- Mobile device theft

**Lost Public Revenues**
- Lost tax revenues
- Lost custom revenues
- Investment needed to fight corruption

**Health and Environmental Risks**
- Higher power emissions
- Risk of battery explosion
- Use of hazardous substance

**Degraded Customer Experience**
- Lower quality of service
- Non-compliance with standards
- No approval process or quality control
How device verification helps law enforcement

> Our Approach in Fighting Device Fraud

1. **Device Identification**
   Device IMEI mapped to device brand and model thanks to the GSMA Device Database

2. **Device Verification**
   Detected device characteristics compared to the identified device features

3. **Failed Identification or Verification**
   Mismatch: An old feature phone detected on the 5G network! Or a failed device identification

4. **Block Fraudulent Devices**
   EIR (Equipment Identity Register) at operators integrated with a central country-wide EIR and with the GSMA global IMEI database