GSMA

GSMA Services Showcase Live #9

VoLTE implications for network sunsetting

Wednesday 31 May 2023

Question	Answer	Responder
How are stolen devices handled that have multiple IMEIs?	All known identifiers should be submitted when reporting a device to the GSMA Block List to most effectively block the sale or use of a flagged device.	**Jason Smith, Product Director, GSMA**
How is GSMA's lost/stolen list used by law enforcement?	Law enforcement uses the GSMA Device Check service to access Block List information and query activity of other users. This information helps to provide a more complete picture of device activity with entity names, dates and the reason for actions. Agencies have used this information to identify criminals and as evidence in cases of fraud, theft, money laundering, etc.	**Jason Smith, Product Director, GSMA**
How do countries with their own national database use GSMA's global block list?	GSMA has established a Shared EIR framework to support countries with a national device blocking database. Each participating Operator is provided a Device Registry account which may be managed by a designated 3rd party ("Shared EIR Provider") to help coordinate use. GSMA welcomes national systems to join the global community to combat device crime.	**Jason Smith, Product Director, GSMA**
How will GSMA's new status list help deter crime?	The new status list will provide additional background about devices and the organisations with whom they interact. This information helps prospective buyers to make more informed decisions to avoid troublesome devices and provides law enforcement a clearer historical picture to aid investigations. This increase in available information makes it more difficult for criminals to profit.	**Jason Smith, Product Director, GSMA**
What is the recommended process for verifying a device has been allocated TAC correctly?	Verify that the details or device you hold match the data in GSMA Device Information Services. This can be done by checking GSMA Device Database, GSMA Device Map or GSMA Device Check. Should there ever be any doubt on the validity of a TAC please contact GSMA.	**Tyler Smith, Product Director, GSMA**

How should devices that have invalid TAC or mismatched information be handled? Can they be reported to GSMA?	Invalid TAC or information that doesn't match GSMA Databases should be handled with caution. Devices that do not have Valid TAC should not be allowed to connect to any Mobile Network or be allowed to enter countries for use. If the data doesn't match please contact GSMA to verify and allow the Manufacturer to correct the issue. Can they be reported to GSMA? Yes, please report all issues found related to incorrect information via the GSMA TAC Data Challenge Process which can be found at the following link https://imeidb.gsma.com/imei/tac-challenge?utm_source=homepage-tile	**Tyler Smith, Product Director, GSMA**
What devices require a TAC?	Any device that has that can connect to a mobile wireless network using 3GPP technologies or other wireless network technologies require a TAC. This includes but is not limited to IoT devices, Modems, Gateways, Automobiles, GPS Trackers, Smartphones, Wearables, Feature Phones, etc.	**Tyler Smith, Product Director, GSMA**
How has implementation of DIRBS using GSMA Device database contributed towards development of Telecom Sector within Pakistan?	Implementation of DIRBS using GSMA TAC database has been a game changer for Pakistan. It has helped stop counterfeit, duplicated and cloned devices from being connected on local networks thus helping in improvement of QoS. It has also helped in stopping informal channel imports resulting in increasing legal imports by 100% and contributing significantly towards custom duties collection for the government. It has created a level playing field for local manufacturing which is complimented by a very business friendly mobile manufacturing policy. Till date 33 plants for local manufacturing of mobile phones has been setup and fully operational.	**Nauman Khalid, Director Type Approvals, Pakistan Telecom Authority Regulators**
Are roaming devices also subject to DIRBS processes?	Roamers are exempted from the process of DIRBS and allowed services without any disruption.	**Nauman Khalid, Director Type Approvals, Pakistan Telecom Authority Regulators**

Can you please elaborate more about identification and how the treatment for duplicate IMEI cases? Especially in step 3 and 4 in your slide before, how you use MSISDN to determine the compliant case and non-compliant case for duplicate IMEI?	Duplicated IMEIs are identified from mobile operators data dumps, whereby if an IMEI is seen on local networks on more than 3 MSISDN, it is flagged under duplicate category. After this, we inform all such users through SMS that they may be using a duplicated IMEI on a replica device and ask such users to provide IMEI 1, IMEI 2, Serial Number and Colour of device which is cross checked with the relevant manufacturer. Genuine device IMEI validated by Manufacturer is paired with the MSISDN and remaining devices are blocked for use on local networks.	**Nauman Khalid, Director Type Approvals, Pakistan Telecom Authority Regulators**
For the cases that we have duplicate IMEI data that older than 1 year and without log time data attached to it (it only says this IMEI used in 8 devices without data which one input first), do you have any suggestion what is the suitable way to tackle this issue?	It is suggested that duplicated IMEIs that are active on local networks should be addressed as they are connected on local network and contribute towards poor QoS. If any duplicated IMEI that is inactive and not being used on local networks should not be catered for.	**Nauman Khalid, Director Type Approvals, Pakistan Telecom Authority Regulators**
Your agency (ZITiS) was founded in 2017. What advantage does ZITiS bring to the German Security Architecture?	As a central service provider for federal authorities with security tasks, we can spend almost 100% of our time to develop and research innovative technical solutions, tools and methods that contribute to maintaining internal security in Germany.	**Christian Dressler, Senior Expert Mobile Security, ZITis**
How often do you use the GSMA-Device Database at ZITiS?	Every week we get several requests from the federal authoities regarding the IMEI/TAC of Smartphones, IoT-Devices, Vehicels and more. That's why we decided to ask for ‚Official Service Provioder' level of the GSMA-Services.	**Christian Dressler, Senior Expert Mobile Security, ZITis**
Could you again explain why moving IoT-Devices' are of special interest for law enforcement agencies?	We all see, that more and more objects of public life are connected to the internet via LTE ans 5G technology. So in almost any investigation the law enforment agencies have to deal with IoT-Devices and with IMEI/TAC. So, moving IoT-Devices can help to identify moving criminals.	**Christian Dressler, Senior Expert Mobile Security, ZITis**
How did you find out the TAC numbering Schemes for Smartphone suppliers?	Short question, short answer: like many discoveries in history accidental!	**Christian Dressler, Senior Expert Mobile Security, ZITis**