Government Solutions

Compulsory Phone Registration (CPR)

Since the very first introduction of mobile phones, mobile devices directly became a target for criminals. Mobile device theft is quite often driven by a potential demand on the black market. With growing prices for specific models of mobile phones, it also becomes a target for the “grey” dealers who are smuggling high-value devices into the country avoiding import taxes. This not only impacts overall country revenues but clearly causes a lot of inconvenience for potential buyers, as these devices won’t be accepted by official dealers and therefore cannot hold the warranty or ensure the expected quality of service.

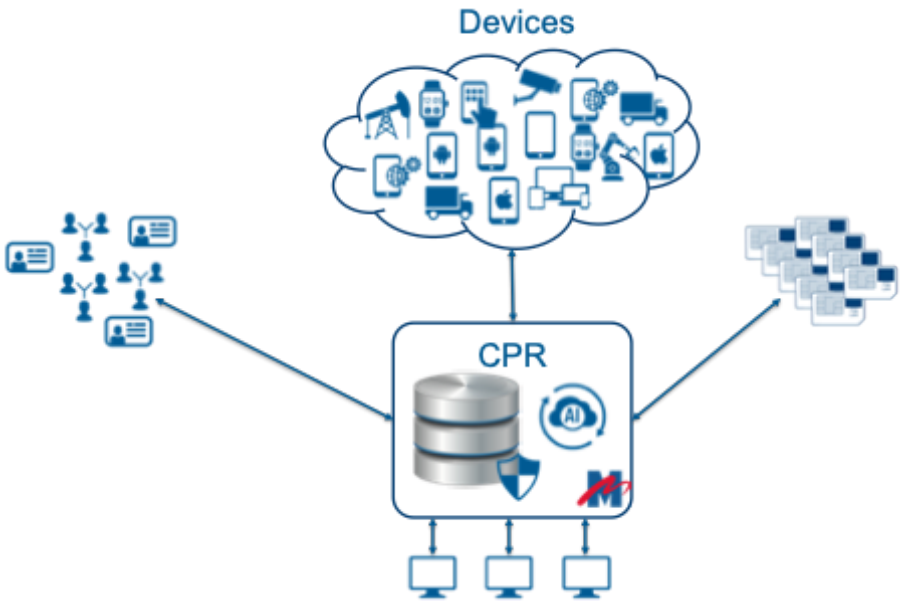
At the same time, uncontrollable distribution of SIM cards and cheap mobile devices support a number of fraudulent or criminal activities. These activities range from the typical mobile fraud leveraging sim-boxes and spam concepts all the way to the terroristic activities or public safety attacks frequent in many regions.

Traditional simple solutions based on device black-listing through operator-based Equipment Identity Register (EIR) solution is not always efficient on a countrywide scale in some regions. Mavenir, in collaboration with several governments, has developed a new generation solution to help control the device market and SIM card distribution.

CPR overview

Mavenir Compulsory Phone Registration (CPR) system has been designed to simultaneously track millions of devices and SIM cards at the same time. Unlike traditional “EIR” device's blacklist approach, CPR is using the concept of a whitelist. This puts totally different requirements on technology, design reliability, and fraud prevention capabilities. Mavenir CPR front-end enables smooth integration into mobile operator networks without the need for complex routing designs by plugging right in front of existing EIR implementations in a transparent way. This allows for a fast launch, preserving existing IMEI validation logic.

On top of provisioning the whitelist of IMEIs, CPR enables the linking of the devices with the SIM cards and their owners. This approach not only prevents traditional mobile fraud scenarios but also helps governmental law enforcement agencies prevent criminal activities from a simple mobile phone theft to the tracking of large multi-national terroristic networks.



Whenever CPR solutions are enforced in the country, fraudsters and criminals are looking for ways to bypass the enforcement, fake IMEIs, registrations, etc.

Mavenir CPR includes advanced Anti-Fraud module based on the latest generation real-time Machine Learning algorithms. That not only enables fraud prevention, detects IMEI duplication as well as suspect SIM registrations, but also minimizes the probability of false-positives preventing an impact on normal mobile users. Machine Learning technology also enables the system to deal with different types of the devices and device usages, distinguishing between smartphones, feature phones and IoT devices of different nature.

Overall CPR features include, but are not limited to:

- Registration DB supporting hundreds of millions of records
- Integration with Central EIR DB
- Device tracking
- Auto device registration
- Device recognition
- IMEI-IMSI locking
- National-ID locking
- Support for various policies
- Fraud prevention
- Integration with external IT systems
- Business Intelligence

A comprehensive set of APIs enables integration with various governmental, commercial, and retail systems. This allows a streamlined registration process and quickly introduces a country-wide convenient registration network.

Built-in anti-fraud & security system

Clearly, countrywide mobile device registration enforcement, together with SIM registration, would drive fraudsters and criminals to explore ways to by-pass the system. The number of devices can be broken and the IMEI can be cloned. This clearly would not only impact country laws but also would have the risk of negative impact on individual citizens, as jail-broken devices won't be properly supported by handset vendors, at the same time individuals are exposed to the risk of losing their personal data to criminals with potentially bad consequences to themselves and their families.

Currently known rule-based or statistical methods detecting IMEI cloning can easily be bypassed, as any security measure defined by a technical rule can be detected and compromised. Mavenir's Fraud Detection Module integrated into the CPR system is based on real-time Machine Learning technology, featuring the latest developments in Machine Learning technique. A dedicated ML model is specifically tailored to the conditions of target deployment country and capable of detecting with an extremely high level of accuracy compromised equipment and fraudulent activity.

In addition to that, any suspicious activity detected through constant benchmarking of behavioral models, the system detects criminal activities, sending preventive alerts to law enforcement bureaus. This approach not only prevents fraudulent activities but also ensures public safety and security.

CPR Benefits:

For Subscriber:

- Guaranteed quality of the equipment
- Protection against theft
- Less crime, more safety
- No fake premium phones

For Government:

- Additional tax revenue
- Import tax protection
- Allow fair competition by eliminating the Grey market
- Attract foreign investments from global brands
- Civil safety

For Operator:

- Protection for equipment sale revenue
- Better service quality with the elimination of illegitimate handsets
- Known equipment on the network
- Subscriber profiling and customized offerings