PortingXS CEIR solutions

"Preventing and detecting fraud: together" is the theme which this service is based on, according to PortingXS.

The global number of stolen phones, counterfeit phones and illegal imports is increasing drastically. For the same reason awareness of this distressing situation grows within the worldwide Regulators' domain. Considering the enormous and various impact within all the stakeholders as well as country specific situations, there is no "best solution, one size fits all". It requisites thorough investigation case by case, gathering information on the current footprint as well as the targeted future goals.

Implementing a central solution like CEIR (MDMS, DIRBS etc.) would decrease the number of trading stolen, illegal and counterfeit phones and in short-term would result in public safety and awareness by registering and checking the status of mobile phones. Examples of long-term results are decreasing network pollution and reduce loss of customs duties and other taxes.

Besides earlier mentioned national impact and effects, the personal and business impact in case of loss or theft of mobile phones can also be considered worrisome. The data carried by and stored on mobile phones nowadays can be considered irreplaceable, where value of data can hardly be expressed in numbers e.g. personal/business data, bank account details, pictures/media.). As a result of the recent introduction of GDPR, the consequences of data breaches due to mobile phone theft, should also be kept in mind.
Currently, in case of theft or loss of a mobile phone where there is no CEIR in place, the consumers holds the responsibility to have the Operator block the sim card as soon as possible, as well as having a tracing solution and/or blocking solution in place for the mobile device. This Central Equipment Identity Register for IMEI will enable mobile service providers to block all services to those handsets that are reported lost or stolen, in order to prevent their misuse.

One of many effective solutions that introducing IMEI blacklisting will enhance is that it discourages mobile theft worldwide. This can only be effective beyond borders when global coverage is in place. Not participating as a country will pave the way for criminals and terrorists.

Functionalities Central Equipment Identity Register (CEIR) application

The main functionality of the Central Equipment Identity Register (CEIR) application for IMEI is the registration of telecommunication devices, using the IMEI as a unique identifier. The CEIR application for IMEI can be used by different target groups.

The strength and success of the application depends on the different stakeholders working together.

Given the fact many stakeholders are involved, the solution can be consulted by all, with a variety in access and authorization level. In case of a change in status, this change will be available and -depending on business ruling- taken measures will be effective immediately.

In the centralized database the stakeholders can share and search IMEI registrations, where all known IMEI's are gathered (among which are the lost, stolen, counterfeit or illegal mobile phones) and can be used to prevent misuse in all networks by blacklisting them.

Depending on the specific requirements and business rules, defined per country, the central solution can comprise several functionalities, such as:

- checking and (temporarily) blocking IMEI's on the networks due to the lost, stolen, unknown or illegal import, greylisted or blacklisted status,
- adding IMEI's to either white- or blacklist by Customs, OEM's, Retailers etc.

Stakeholders

The database can be used by different sectors, access and authorization level varying per stakeholder. Possible stakeholders and sectors using the CEIR, are:

- Consumers
- Telecom operators
- Government/ Regulator
- Police / Law enforcement
- Customs
- Insurance companies
- Financial sector
- Second hand traders/platforms
- Business corporations

The CEIR application allows the device owners to register their device in the central database. During the registration phase it allows for different types of registration, such as: new registration, stolen, found, check, unregister and/or destroyed.

Using web portal or web browser the CEIR can be checked for status information. Secondly it allows for automated connections to different stakeholders for distribution of registrations or status checks etc. Connecting via web services also allows for further integration into other devices or apps.

Batch access is also allowed for authorized users. Different protocols, such as XML, CSV, etc. allow for batch actions to register, checks and report. Every IMEI owner can receive notifications when the status of an IMEI changes. These notifications can be received via email, text messages, social media, push/ pull mechanisms and delta updates, depending on the connection type of the user.

Get in contact

Would you like to explore the possibilities for CEIR services? Please contact the team:

m.louwsma@portingxs.nl
+31 70 219 99 99
www.portingxs.com