CONTRIBUTION TO:

ITU EVENT ON COMBATING COUNTERFEIT AND SUBSTANDARD ICT DEVICES

ITU Headquarters, (Geneva, Switzerland, 17-18 November 2014)

Submitted by: Ukrainian National Information Systems (**UNIS)**

Contact point: **Keith Mainwaring**

keith.mainwaring@ukrainesystems.com

+46 76 107 6877

Case Study – Limiting the use of contraband and counterfeit mobile devices in the Ukraine

Introduction

A system was launched in Ukraine in 2009 to combat the illegal importation of mobile devices based on the registration of mobile device IMEIs (International Mobile Equipment Identities). This system (the Automated Information System for Mobile Terminal Registration in Ukraine – AISMTRU) has been extremely successful on two counts – firstly, in 2008 only about 7% of mobile devices were legally imported into the Ukraine whereas two years later this situation was completely reversed with only 7% of mobiles in use not having been legally imported and secondly, as 93% of mobile devices were entering the country through legal channels, tax revenues increased substantially by US$ 1000 million between 2009 and 2013. Currently, approximately 170 million mobile devices are registered on the system. Although the system was primarily aimed at ensuring that mobile devices entered the market by legal channels it is likely that the number of counterfeit devices has also decreased substantially as one can safely assume that many counterfeit devices enter the market illegally. This type of technical solution could also be used to more specifically combat the spread of counterfeit and substandard ICT equipment in general – not only mobile devices.

The following describes the technology and operation of this system in more detail.

Principles of operation

IMEIs are used in the Ukraine to create a database of those devices that have been legally imported into the Ukraine. The following lists are maintained: a "white list" of those devices that have been legally imported, a "grey list" of devices of unconfirmed status and a "black list" of devices that will be denied service. Access is provided to the regulatory and customs authorities, network operators and the general public with appropriate levels of access privileges. The processes are as follows:

Interaction with importers and customs service

Step 1

The National Regulator registers an importer in the registry of accredited importers

Step 2

The importer receives an import permit (if required), pays the necessary VAT/Taxes and imports the equipment into the country

Step 3

The government Customs Service verifies shipping and sends the information to the Regulators database

Step 4

The Importer submits the IMEI codes for all imported devices for inclusion in the system's "white" list

Interaction with mobile operators

Step 1

The mobile operators send to the National Regulator a list of the IMEI codes of all registered devices in their networks

Step 2

The system automatically processes the IMEI code list, while also recording the details of the new IMEI codes in the National Regulator's database

Step 3

The mobile operators receive updated versions of the "gray" and "black" lists from the system

Step 4

The mobile operators send SMS messages to customers with devices in the "gray" list and terminate service for users of "blacklisted" devices

Interaction with end users (subscribers)

Step 1

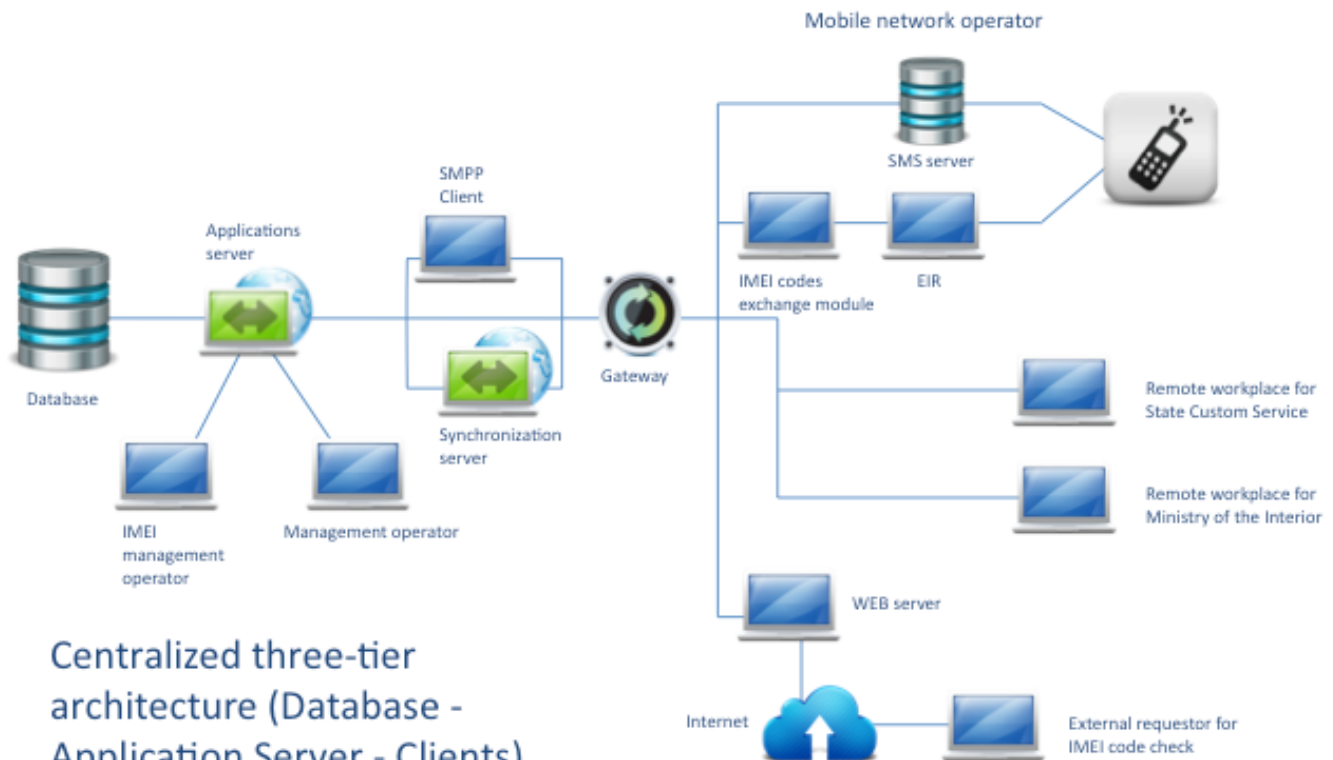The buyer chooses the mobile device, that he/she wants to purchase

Step 2

The buyer checks that the device is in the "white" list by sending a Web or SMS query to a designated address of the system

Step 3

If the system indicates that a specific device was illegally imported into a country, the buyer refuses to make the purchase

System Architecture

The system architecture is as follows:

Mobile network operator

SMS server

SMPP Client

Applications server

IMEI codes exchange module

EIR

Gateway

Remote workplace for State Custom Service

Database

Synchronization server

Remote workplace for Ministry of the Interior

IMEI management operator

Management operator

WEB server

Centralized three-tier architecture (Database - Application Server - Clients)

Internet

External requestor for IMEI code check

Conclusion

This type of system architecture has proved to be very effective in ensuring that mobile devices are imported in accordance with national regulations in the Ukraine and should be considered for application to combating the spread of counterfeit and substandard ICT equipment.