IMEIU-Registry

System on registration and maintenance of the IMEI codes

System Description Document

Version: 2.1
Date: 13-January-2016

Table of Contents

1. Introduction

1.1. Definitions & Glossary of Terms

The following terms and abbreviations are used in this document:

Administrator – the company-hoster of the IMEIU-Registry system

Administrative rights – the permission of access level to IMEIU-Registry functions that can have and must have system admins only

Application – applications (electronic form or packet file) for the import of radio electronic means

Certificate of conformity – a document certified by the National Regulatory Authority that the supplied (imported) radio electronic means meets the required specifications

Customer – entity that issued the RFP of “Administrative and Technical Requirements”

Customs – the Customs Authority

End-users – subscribers of mobile operators

NRA – National Regulatory Authority

Operator – an employee of the Customs, which performs data processing and other operations with CUSTOMS-IMEI software

Permit – a Customs document (declaration) according which the import of the radio electronic means has been allowed

Radio electronic means – SIM card based devices

Stakeholders – Customs, Tax Service, Law Enforcement Authorities, National Regulatory Authority

Telco – telecommunication operator that supports and carries out number portability processes as participant of the IMEIU-Registry

1.2. General

The document describes the properties and parameters of the system on registration and maintenance of the IMEI codes IMEIU-Registry (hereinafter – IMEIU-Registry) based on a central database the IMEI codes (hereinafter – IMEIU CDB).

The IMEIU-Registry system was developed by “**Technical Center of Internet LLC**” (Ukraine, Kiev).

The document contains the organizational and general technical proposals to meet the implementation.

“IMEIU-Registry” is the brand name and has protection of intellectual property in accordance with legislation of Ukraine.

1.3. Overview

IMEIU-Registry has been designed to manage the main goals:

- monitoring and control usage of SIM based devices mobile networks of the country implementation in on-line/real-time mode,
- monitoring and support of the Law Enforcement Authority activities on antiterrorism, antifraud, antitheft etc.,
- support and maintenance of the process designated to control and optimize procedures of importing and registration of radio electronic devices, thus, resulting in the increase of state revenues.

The Stakeholders of IMEIU-Registry are Customs, Tax Service, Law Enforcement Authority, NRA, Importers, and Telcos.

All Stakeholders have possibility work within IMEIU-Registry environment via separate Automated Working Stations (hereinafter – AWS). The AWSs allows have access to IMEI CDB, but only in accordance with rights and roles of Stakeholders.

IMEIU-Registry allows to operate with options relating to the management of the mobile numbers as well as personal numbers and non-geographic numbers if they use in mobile networks via SIM based devices.

The crypto subsystem of IMEI-URegistry is fully compliant the requirements and security standards both international and Ukrainian. The use of cryptographic mechanisms may adopted the requirements of the legislation of the country implementation if needed.

The IMEIU-Registry system uses brand solutions for servers, routers, firewalls, DMBS.

During implementation, as additional option, can be realized the delivery and launch of SMS/Email-Center for sending service messages (not from network of operators who can sabotage on various reasons some types of messages). It is an element for further expansion of system towards of number portability.

IMEIU-Registry forms the technological base for decisions:

- to integration with worldwide centralized IMEI Databases
- on number portability in the mobile and fixed networks;
- on technology using the personal numbers.

1.4. Abstract

This document describes:

1) general principles of the IMEIU-Registry;
2) general features, options and possibilities of the IMEIU-Registry;
3) functionality of the IMEIU-Registry;
4) components of functional structure of the IMEIU-Registry;

5) functions and full kit of the Stakeholders' Automated Working Stations of the IMEIU-Registry;
6) FAQs.

2. The general principles of the system.

The organizational and technical offer provide the **"turn-key" solution**.
The system interacts with the operator' EIR in accordance with the protocols that are defined for the exchange of information with the EIR/HLR by GSMA documentation. If mobile operator does not have the EIR, the system can interact with HLR in accordance with the data formats and protocols for this interaction.
All technical decisions of the IMEIU-Registry system based on cloud technology. It mean that main and backup sites can be located in any accessible and suitable of the Customer datacenter.
Access to Telcos' EIR or HLR data from the IMEIU-Registry is provided through secure IP-channels, cryptography equipment, and either via pair FTPS-server/client or via pair EPP-server/client.
There are two remote Administrator clusters - the main site and backup site. One more Administrator cluster can be located directly in the Administrator office and provide monitoring of subsystem and backup of IMEI CBD. This cluster must be located on secure premises in separate rack. If such option is not available, this cluster can be located at any compliant location which is different from the main and backup sites.
All client software and hardware is located on Stakeholders' clusters only: Customs, Tax Service, Law Enforcement Authorities, and National Regulatory Authority (NRA).
Thus, the system can provide data exchange in all cases and with any configuration of technical structure of mobile operator.
The mirror of the triplets IMEI/IMSI/MSISDN in "white", "grey" and "black" lists can be stored only in IMEI CDB.
The mobile operators and Stakeholders get all relevant information about subscriber numbers after processing in the system.
The system allows only authorized parties to access to "white", "grey", "black" lists. Only authorized parties can provide the information and conditions for transfer triplets IMEI/IMSI/MSISDN from one to another list. Only Administrator must provide the realization of transfer.
The authorization of parties can be provided only according to procedures and policies that must be approved under legislation of Cambodia.
The system provides the ability to work in three modes of access:

- using WEB for end-users and for support of Automated Working Stations;
- using EPP-protocol, to perform single or group on-line/off-line inquiries in form of xml-structures;
- using FTPS-protocol for data exchange in the form of files.

2.1. Basic technological principles

Basic technological principles of the IMEIU-Registry provides implementation and maintenance of the following workflows:

- providing information for all category of users on the legality of IMEI codes via web-interfaces or/and SMS through public short number (code) in accordance with the National Numbering Plan;
- information exchange of IMEI codes lists with national mobile operators;
- information exchange with Customs, Tax Service, NRA;
- information exchange with Law Enforcement Authorities within the "gray" list;
- information exchange to upload and update the "white", "gray" and "black" lists;
- transmission of the unified electronic permits for import into the workplace Customs;
- receive the electronic copies of customs declarations;
- checking electronic signatures on electronic copies of customs Permits;
- storing the received electronic copies.

3. The general features of the system

3.1. The general features of the system

- continuous operation mode 24*7*365;
- reliability and service availability of not less than 99,9%;
- processing of the incoming IMEI applications in the automatic mode, at least 10,000,000.00 per hour (depends on the computing capacity of the servers may be increased);
- storage of 250M unique triplets IMEI/IMSI/MSISDN;
- reception of 0.25M triplets IMEI/IMSI/MSISDN / 1 sec. from operator’ EIR;
- processing time of updated lists of triplets IMEI/IMSI/MSISDN does not exceed 20 minutes;
- receive files or HTTP-requests from operator’ EIR with updated of the triplets IMEI/IMSI/MSISDN of total subscriber base (can done several times a day).

- actual performance of the solution does not depend on the conditions of the network and can be scaled.

3.2. The functionality of the system

The functionality of the system given in Table 1

Table 1: The functionality of the system

Requirements	Compliance
SIM lock	Automatic and Manual Mode
Exceptional numbers configuration	Yes
Configurable lists	Yes, White/Grey/Black Lists
Centralized Database & Synchronization with operators database of registered devices	Yes
Administrator Web Interface	Yes
Device Repository	Yes
IMEI Preauthorization	Algorithms of the IMEI verification, validation, partial validation, cancel preauthorization
IMEI Authorization	For all cases of device imported for personal and non-personal use, cases of device imported by Importers
IMEI De-authorization	Algorithms of the Full De-authorization / optional can be implemented the Partial De-authorization mode
API functions must include:	
Block a specific IMEI in Database	Yes / Black List
Lock a specific IMEI to MSISDN/IMSI	Yes / Black List / Grey List
Check IMEI status in the database (authorized/blacklisted/locked to a specific MSISDN)	Yes / function of the authorized / blacklisted / locked to a specific MSISDN
Check MSISDN status in the database	Yes / function of the locked to a specific IMEI
Switch a lock rule to another MSISDN	Yes

Delete a lock rule	Yes
Authorize a specific IMEI in the database	Yes
Logging (any action done by user must be logged)	Yes, mandatory option
Point of sales (POS) interface for 3rd parties/Customer care agents (to allow registration of devices bought abroad by Importers or specific person for personal use)	Yes / for agents via interfaces SOAP, WEB, GUI, EPP
Manual lock features (SMS request to release or open a devices, API request to switch an IMEI to another MSISDN or to release an IMEI)	Yes
Purge Mechanism	The algorithm of the full purging lock rules for inactive subscribers
Time based purge	Configurable period of time set in the range of from 60 minutes
Device Auto Release (free devices whenever their owner becomes inactive)	Yes
Integration with mobile core network of operators	Yes
Alarm Notifications and alerts management over various triggers sent through SNMP, SMPP, SMTP, HTTP etc.	Yes / Integrated solution for SMSC and Email Center
Integration with worldwide centralized IMEI Databases	Yes
Reflection of geolocation	Yes
Fraud detection	Yes, the algorithm of usage of fake IMEIs, potential cloned IMEIs or/and cloned SIM cards, large number of device change request, large number of triggers from operators’ core networks, etc.
Inbound roamer management	Yes

Interface access control (allows service Administrator to create web user accounts and groups (admin, Customer care, marketing etc.) with different access levels and Privileges)	Yes, due to the implemented algorithms of prioritization
Advanced reporting	Yes, IMEIU-Registry system supports reports and customized reporting features, location based reporting etc.
Backup/recovery	Yes, specified through the double (minimal) reservation of the equipment
Localization in languages of the country implementation	Yes, full

The concrete realization of the functionality will be available after familiarization with the specific requirements / features in Technical Requirements of the system. The rules depends and should take the national legislation of the country implementation into account.

3.3. Components of functional structure

The functional structure is aimed at meeting the requirements of the Stakeholders and allows to solve the relevant practical tasks.

The instrumental base of the functional structure for Stakeholders are AWSs.

The functional structure of the IMEIU-Registry includes components:

- The Central Data Base of the IMEI – IMEI CDB;
- interface subsystem;
- subsystem of the automatic maintenance and processing of incoming IMEI applications for the import of radio electronic means;
- subsystem for creation and maintenance of the white/grey/black lists;
- administration subsystem;
- audit and analytical subsystem;
- monitoring and Help-Desk subsystem;
- subsystem of cryptographic security;
- WHOIS service.

WHOIS service is optional and can be included when Customer ordered maintenance of the ENUM service (ENUMU-Registry system). More detailed, please, see item 4. **FAQs**

3.4. Functional structure

Functional structure of the IMEIU-Registry shown on Figure 1.

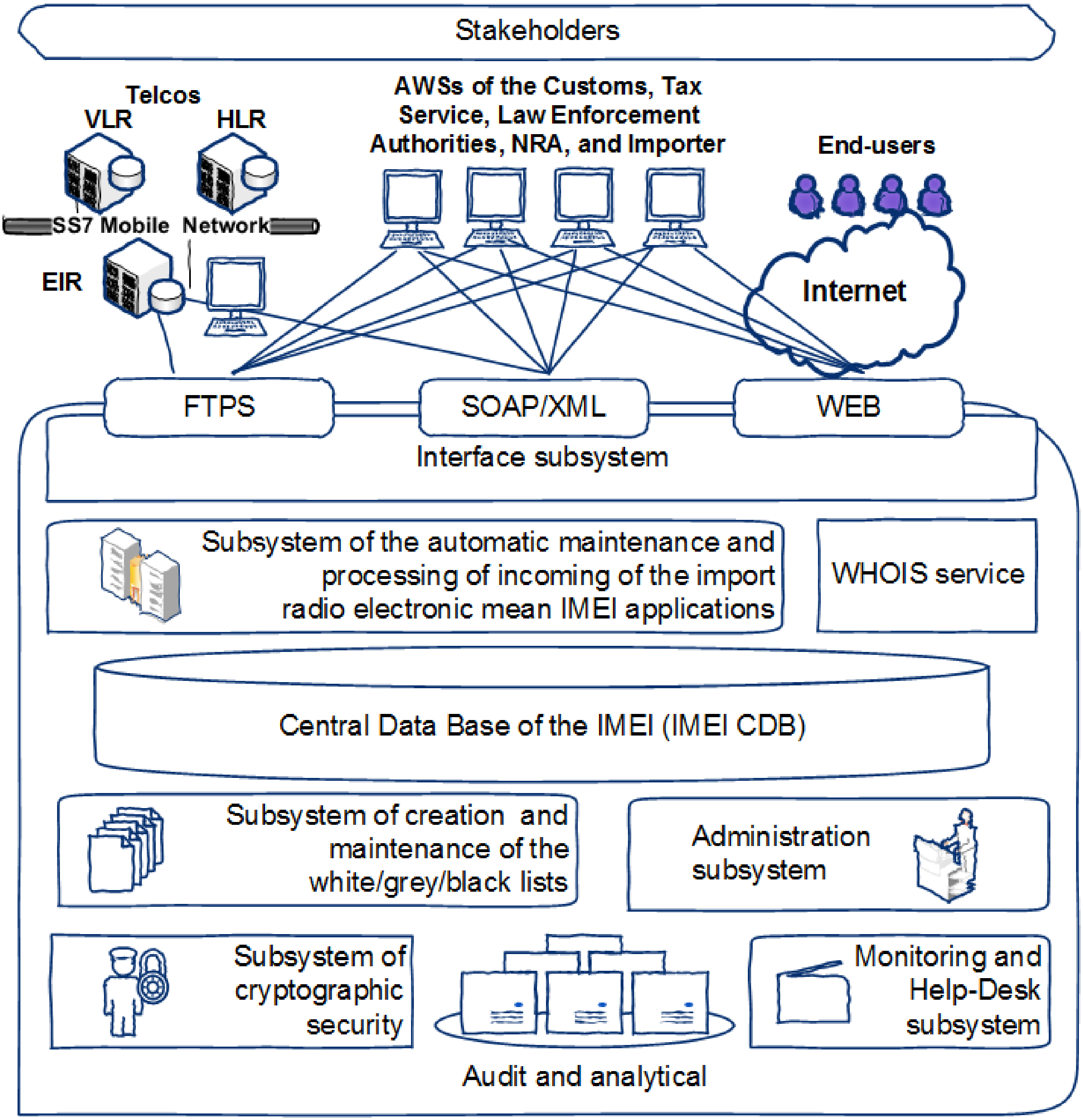
Stakeholders
Telcos
VLR
HLR
SS7 Mobile Network
EIR
AWSs of the Customs, Tax Service, Law Enforcement Authorities, NRA, and Importer
End-users
Internet
FTPS
SOAP/XML
WEB
Interface subsystem
Subsystem of the automatic maintenance and processing of incoming of the import radio electronic mean IMEI applications
WHOIS service
Central Data Base of the IMEI (IMEI CDB)
Subsystem of creation and maintenance of the white/grey/black lists
Administration subsystem
Subsystem of cryptographic security
Audit and analytical
Monitoring and Help-Desk subsystem

Figure 1. Functional structure of the IMEIU-Registry

3.5. Automated Working Stations of the Stakeholders

The functional structure of the IMEIU-Registry includes the remote Automated Working Stations:

- “**Importer-IMEI**”, interactive software of the Importer to run the IMEI codes registry of mobile phones;
- “**Customs-IMEI**”, interactive software of the Customs on maintaining the database of Importers;
- “**LEA-IMEI**”, interactive software of the Law Enforcement Authority on maintaining the database of IMEI codes;
- “**Tax-IMEI**”, interactive software of the Tax Service on maintaining the database of Importers;
- “**NRA-IMEI**”, interactive software of the National Regulatory Authority on maintaining the database of the Certificates of conformity;
- “**PoS-IMEI**”, interactive software of the customers to run the IMEI codes of mobile phones registry for personal use;
- “**ADMIN-IMEI**”, interactive software of the Administrator on maintaining the database of IMEI codes.

The quantity of AWS can be configured on requirements of Customer, i.e. some AWS can absent in final configuration implemented system. The final quantity and configuration of the AWSs depends from Technical and Organization Requirements of the Customer.

3.5.1. Importer-IMEI

The **Importer-IMEI** is the maintenance software that helps to enter, edit, view, search and export the data about the IMEI code within relevant Permits and Certificates of conformity into IMEI CDB and provides performance of the AWS functions:

1) entering and editing the IMEI codes into IMEI CDB;
2) viewing of the list of the IMEI codes with possibility of viewing and the printing of detailed information on a specific code (terminal type, No. of permit, etc.);
3) editing and change of accessory of the specific chosen IMEI code on "white", "gray" or "black" lists. The system stores information about dates, phones etc. that added to different lists. Change of parameters and parameters' value of the IMEI code of the mobile phone in the list;
4) definition and change of the technological status of the specific IMEI code;
5) search of codes by certain criteria (date of introduction, belonging to a group, technological status, and Importer);
6) the ability to determine how to create the IMEI code in the registry (manual or automated);
7) viewing a list of files used for automated entering IMEI codes into the IMEI CDB with the reflection of the comment field;
8) export IMEI codes belonging to the "black” list in the file of a pre-defined format.

3.5.2. Customs-IMEI

The **Customs-IMEI** is the software for Customs purposes on maintaining the database of importers and can produce:

- enter, edit, view, search and export the data about importer;
- search, view and export the relevant information about mobile devices and IMEI codes that got the permission on import,

and provides performance of the AWS functions:

1) entering and editing the information about Importers companies;
2) list of Importers who are brought in system with possibility of display of full information on the chosen Importer;
3) search of Importers using the data fields;
4) input and editing these Permits for import of radio electronic means. In case of manual entering of Permits into the DB the operator chooses type of the Permit, the Importer from the reference book on Importers, chooses radio electronic means from the reference book on radio electronic means and fills all fields;
5) revision of the list of the brought Permits with possibility of viewing of detailed information;
6) printing of the data within Importer and/or Permit.
7) search of Permits in certain criteria (is defined by the Customer);
8) removal of the statement from a DB only when wasn't made the decision on refusal or on issue of the import license; At a stage of creation of system the full set of the reasons for which it can be refused the Permit will be defined;
9) an import permit issued for a period of N months (to be specified in the design stage), but this period may be extended further by M months (to be specified in the design stage);
10) formation and printing expense of the applicant, followed by registration of the financial events;
11) revision of the list of permissions created with the ability to view detailed information;
12) printing the selected authorization;
13) formation in the form of authorization in accordance with the legislation and the transfer of such a Permit to Customs;
14) searching for details of Permits or authorization issued for a specified period.

3.5.3. LEA-IMEI

The **LEA-IMEI** is the software for Law Enforcement Authorities purposes on maintaining the database IMEI codes and can produce:

- enter, edit, view, search and export the data about subscriber’s numbers associated with IMEI codes that have been included or excluded in / from “grey” or “black” lists;
- search, view and export the relevant information about mobile devices and

IMEI codes associated with subscriber’s numbers;

- receive the cross-information from Customs and NRA,

and provides performance of the AWS functions:

1) formation of the “gray” and/or “black” lists in accordance with the decisions of the Law Enforcement Authority according to the legislation;
2) editing, selecting, viewing and saving of accessory of the specific chosen IMEI code on "white", “grey” or "black" lists; the IMEIU-Registry system stores information about dates, phones etc. that added to different lists. Change of parameters and parameters' value of the IMEI code of the mobile phone in the list;
3) ensuring access to "gray" and "black" lists on the basis of the given-out access rights;
4) transfer files that were prepared by LEA-IMEI to the IMEI CDB;
5) receive file in accordance with the requests to IMEI CDB include geolocation data;
6) searching for details in the colored list within a specified period.

3.5.4. Tax-IMEI

The **Tax-IMEI** is the software for Tax Service purposes on maintaining the database of importers and can produce:

- enter, edit, view, search and export the data about Importer;
- search, view and export the relevant financial information about Importer within the permissions on import,

and provides performance of the AWS functions:

1) entering and editing the information about Importers companies;
2) list of Importers who are brought in system with possibility of display of full information on the chosen Importer;
3) search of Importers using the data fields;
4) search of Permits in certain criteria (is defined by the Customer);
5) removal of the statement from a DB only when wasn't made the decision on refusal or on issue of the import license; At a stage of creation of system the full set of the reasons for which it can be refused the Permit will be defined;
6) an import permit issued for a period of N months (to be specified in the design stage), but this period may be extended further by M months (to be specified in the design stage);
7) formation and printing expense of the applicant, followed by registration of the financial events;
8) searching for financial details connected with Importer within a specified period.

3.5.5. NRA-IMEI

The **NRA-IMEI** is the software for NRA purposes on maintaining the database Certificates of conformity of importers and can produce:

- enter, edit, view, search and export the data about IMEI codes associated with Certificates of conformity and importers;
- search, view and export the relevant information about mobile devices and IMEI codes that got the Certificates of conformity;
- receive the cross-information from Customs and Importers,

and provides performance of the AWS functions:

1) an import permit based on Certificate of conformity issued for a period of N months (to be specified in the design stage), but this period may be extended further by M months (to be specified in the design stage);
2) revision of the list of permissions (Certificates of conformity) created with the ability to view detailed information;
3) printing the selected authorization;
4) formation in the form of authorization based on Certificates of conformity in accordance with the legislation and the transfer of such a permit to Customs;
5) searching for details of permits or authorization based on Certificates of conformity and issued for a specified period.

3.5.6. PoS-IMEI

The **PoS-IMEI** is the maintenance software that helps to enter, view, search, and check the data about the IMEI code of radio electronic means that have been imported by end-user for personal use or are already registered in mobile network.

The **PoS-IMEI** provides performance of the AWS functions:

1) checking IMEI code of user’s mobile device on correctness and presence in the IMEI CDB;
2) entering the IMEI codes into IMEI CDB.

3.5.7. ADMIN-IMEI

The **ADMIN-IMEI** is the software for Administrator purposes on maintaining the database IMEI codes and can produce:

- search, view, and export the all type of data about IMEI codes associated with triplets;
- search, view, and export the information about the presence in the colored lists (“white”, “grey”, “black”), IMEI codes system status, and current status ones;
- search, view and export the relevant information about mobile devices and IMEI codes associated with subscriber’s numbers;
- management of the access rights, verification, validation, and authorization of the operators of the third parties;

- receive the cross-information from Importers, Customs, Law Enforcement Authorities, and NRA,

and provides performance of the AWS functions:

1) user account control: create a new user (new account and define the user’s EDS certificate); introduction of the updated certificates of users; changes the account; removal of the user; lock / unlock users; create, edit, delete user roles;
2) viewing of a log: viewing a list of events; search events by date or user-initiated event; cleaning event log entries for which the expired retention period;
3) formation of specific reports: select reports from the pre-defined reports list; generate reports, viewing and printing them on paper or save reports to a files;
4) management of audit log;
5) management of the dataflow noticed as remote: revision of the list of remote applications for import, import licenses, IMEI codes of mobile devices; search for information in the list of deleted records; the ability to recover deleted records;
6) settings of the cryptographic parameters of the IMEI-URegistry: configure the databases; settings parameters of the system elements; configure the certificate store; settings storage of private keys in the system; initiation and modification of an EDS certificates; initiation and modification the list of the certificates authority; adding and remove certificate revocation lists;
7) searching for details in IMEI CDB for a specified period.

4. FAQs

In this item we give answers to most frequently asked questions.

Q: Can your solution be integrated with IMEI/EIR systems of the mobile operators? Will your solution request to make the deep upgrade of all systems?
A: Our solution allows harmonization with IMEI systems of the mobile operators. IMEIU-Registry system can obtain data as well as from EIR or HLR of the mobile operators, and from, for example, use the CDR.
All future interoperability with the mobile operators IMEI systems do not request a special deep upgrade of the software ones. The data exchange between IMEIU-Registry and IMEI/IER systems of mobile operators are provides through files which contain standard data and standard presentations of the formats ones. Such exchange provides by special software (gateways) which will created by TCI on relevant technical requirements of mobile operators.

Q: Will your solution demand the changes and modernization of the hardware of the mobile operators?
A: No. The system does not require the upgrade or new hardware of the mobile operators.

Q: Will your solution do Real-time Device detection?

A: Yes. Our solution do Real-time Device detection.

Our solution supported Real-time Device Detection on demand of the Telco or send relevant command to Telco. If the subscriber introduced new device or changes the device in network, any Stakeholder of the System gets the opportunity to demand new system configuration triplets (IMEI/IMSI/MSISDN) and determine devices. In this case, the device detection and the formation of new triplets happening in real time.

This scheme used the links based on IP-technology, which makes the System flexible and easily customizable.

Q: Your solution needs CDRs in order to prevent cloning or without use of CDR’s can prevent cloning?

A: Our solution can use any information from Telco’s network that can performed in any formats.

The Call Detail Records only one of ways for prevent cloning. For example, Administrator can to receive relevant information using possibilities of the directly HLR/VLR formats with analysis of "white", "grey" and "black" lists.

The IMEIU-Registry can support any ways and is customizable during implementation stage.

If device will detected as cloned IMEI it marked in CDB by a special flag (in fact could be considered illegal).

The IMEIU-Registry allows to remotely disconnecting stolen phone after (a) filed statements and (b) proof of the fact that the phone is stolen.

Q: Will your solution provide real-time SIM Registration Verification module within same solution database, and deny access to non-registered SIMs?

A: Yes. Please note, such verification option depends from agreement between Telcos and Administrator about transfer and storing the plans on issue SIM cards. If such agreement will be reached, the IMEIU-Registry will provide the opportunity the real-time SIM Registration Verification. For non-registered SIM cards will be provided the mode "access denied".

Additional (enhanced) option of the IMEIU-Registry is protects the network by prohibiting the registration of specific handsets according to precise characteristics (brand, model, specific capability, etc.)

Q: Will solution do real-time device detection (voice and data core networks)?

A: Yes. System will support the solution of the real-time device detection.

Please note, the IMEIU-Registry could not perform the directly action on devices detection (voice and data core networks) without round-trips to networks of mobile operators. Because such actions are the technical privilege of Telcos only.

Authorized Stakeholders can issue these requests and the IMEIU-Registry will provide intelligent interface for such tasks.

Q: Will solution do real-time blocking of cloned devices?

A: Yes. See, please, answer to item 2.

Please note, "real time" mode can be calculated once it is proved that the phone or device being used illegally. The same request to blocking of cloned devices may also occur from authorized Stakeholder only.

Q: Does solution have support for multiple languages including languages country of implementation (for web interface, information SMS etc.)?
A: Yes. Full support all needed languages for web-interface, SMS and email notices, a codes and disclosure of their content, a help messages etc.
The IMEIU-Registry can support multiple languages simultaneous.

Q: Will solution send alert to administrators upon exceeding a pre-defined level of success or failed authorization?
A: Yes. Every failed authorization action will generate special alarm check-ticket that will be send to the admins.

Q: Will solution do device ownership transfer by SMS keyword (allow another MSISDN to use my device)?
A: Yes. For subscribers (end-users) of many Telcos the option of device ownership transfer by SMS keywords is actual.
Please note, usability of this option must provide in accordance of the Telcos procedure or the unified procedure of National Regulatory Authority. IMEIU-Registry take into account a special nuance of procedure and IMEIU-Registry settings can be adjusted in accordance with such procedure, for example:

- both the releasing account holder (Releasor) and accepting account holder (Acceptor) must have active Telcos accounts and registered online accounts.
- if the Acceptor does not have an active Telcos account, Acceptor should call <phone-number> to establish an account.
- if the Releasor or Acceptor doesn't have a registered online account, please go to <web-site-uri> to register.
- the Releasor must provide the Acceptor's account number in order to initiate the online process.
- the Acceptor must complete the Change of Ownership Online Request Form after the Releasor has completed and submitted the online form.

Q: Will solution do authorization based on valid and pre-authorized custom ID (or equivalent ID ..)?
A: Yes. Any actions, actors and objects within the IMEIU-Registry have their own and unique ID that allows strong identification and journaling.

Q: Will solution do IMEI verification and validation based on importers' purchased invoice?
A: Yes. The system has several modes of entering information to the IMEI CDB. One of the modes allows input of information by entering importers' invoices. Information can be input for one or several invoices. The amount of data in one invoice is not limited.

Please note, the IMEIU-Registry settings for invoices should adjusted in accordance of national legislation.

Q: Will solution do instant Verification?
A: Yes. The IMEIU-Registry handles these operations instantly.

Q: Will solution do instant Validation?
A: Yes. The IMEIU-Registry handles these operations instantly.

Q: Will solution do instant Pre-authorization?
A: Yes. The IMEIU-Registry handles these operations instantly.

Q: Will solution do instant Authorization?
A: Yes. The IMEIU-Registry handles these operations instantly.

Q: Will solution handle different authorization scenarios (e.g. Importer, Personal Use, Local Manufacturer)?
A: Yes. The IMEIU-Registry can handle different authorization scenarios for roles and access rights of Stakeholders. Scenarios can be described in configuring the system in the framework of the access rights, roles, number of workstation etc. for different Stakeholders.
The number of Stakeholders are not limited.
Hierarchy of access rights and roles with respect to the possibilities of activity determined and controlled by the Administrator via module “Administrator’s Dashboard”. Stakeholders have the possibility of correcting their access rights and roles within the framework of their competence only.

Q: Will solution integrate with SIM Registration Database (allow only registered SIMs to attach) or Embedded SIM Registration Database?
A: IMEIU-Registry allows adjusted scenario for integrate with SIM Registration Database by way on 2 options:

- for registered SIMs and “permission mode” for ones,
- for non-registered SIMs and “blocking mode” for ones.

Q: Is solution a non CDR based solution (or need any specific CDR’s, please explain)?
A: IMEIU-Registry handles the data based on extracting information from CDR Log files. IMEIU-Registry can adjusted and handle the formats of CDR. IMEIU-Registry not requires any specific CDR's formats.
Please note, IMEIU-Registry does not detect data directly from signaling network (SS7, SIGTRAN) but performs the function of mediation system between Telcos and other Stakeholders.
In this case, the IMEIU-Registry forms IP-based interfaces by which any data are available from any sources from operators signaling network. From another hand, these IP-based interfaces can be easily adjusted in accordance with the actual needs of Stakeholders without pressing against the limits of the SS7 protocols.

Q: Does solution provide web based interface for PoS?

A: Yes. The solution of IMEIU-Registry allows provide web-based interface for PoS and integrate the web-interfaces of the payment systems.

Q: Does solution support for Inbound Roamers case?
A: Yes. IMEIU-Registry supports the roamers.
After Roamer registered in one of the national mobile network, the relevant operator (which has recorded data in VLR) sends a message about the fact of Roamer registration into the IMEIU-Registry. The IMEIU-Registry includes Roamer in the "grey list" for the period defined by law. If Roamer has exceeded the term of stay in the "grey list" is will generate a notification about this fact. This notification can send to relevant government authority.

Q: Will solution retrieve Location Information (CGI) from Core Network messages when available?
A: Yes. For realization of this option the IMEIU-Registry uses the possibilities of the ENUM protocol, including data from SS7 fields Location Number, Location Area Code and Cell Global Identity.
In addition, the ENUM functionality can be used to handle the emergency service calls.
Please note, the geolocation accuracy depend from characteristics of mobile networks.

Q: Will solution provide EIR Alert (send triggers to external nodes upon detecting a specific IMEI)?
A: Yes. IMEIU-Registry will generated “Alarm” signal if identifying cases that data in triplet is will disagree by allowed policies. It mean that the “Alarm” will be sent to Telco (from which EIR came the suspicious triplet) information about mismatch of triplet data and data in “white” list. The information about triplet will be excluded from “white” list and transferred into “grey” list. This situation will persist until data validation will received or until the triplet time in “grey” list expires. If control time has expired and will not receive confirmation data validation the information about triplet will transferred into “black” list.
In any case, the Depositary of all of the lists (“white”, “grey”, “black”) have Administrators only. Telecommunications companies and other Stakeholders should conduct the verification procedure. It allows the government authorities to control the real situation on market of the use of mobile devices not invest in heavy solutions based on SS7 protocol.