Qualcomm Technologies, Inc.

EIR & Core Network Requirements for Blocking Fraudulent Devices

EIR-and-Core-Network-Reqs-1.0.0

November 20, 2018

Revision history

Revision	Date	Description
1.0.0	November 2018	Initial release

Contents

Figures

Tables

1 Introduction

1.1 Purpose

The Equipment Identity Register (EIR) is a Core network element that identifies valid devices. Its main function is to prevent fraudulent devices from accessing the cellular network. EIR maintains a blacklist of stolen or invalid devices which must be blocked. EIR also maintains exception lists of devices that are granted exceptions.

Preventing fraudulent devices from accessing the network is a legal requirement in many countries and responsibility of the regulator to enforce it.

The impact of allowing fraudulent devices on cellular networks is far reaching and affects the entire ecosystem:

- Consumers suffer from mediocre performance and reliability
- Device manufacturers suffer from loss of sales due to unfair competition and pricing pressure
- Operators suffer from inferior quality of service and capacity issues due to sub-standard devices
- Governments suffer due to lost tax revenues, non-compliant device ecosystem, and implications to national security

This document specifies requirements for EIR and the Core network which regulators can leverage in their regulatory framework documents to prevent fraudulent use of handsets in their respective countries.

1.2 Scope

This document is for Regulators and Government officials who draft national policy frameworks to block fraudulent mobile devices in their respective countries.

This document introduces and defines the role of EIR in the Core network and defines key functional requirements that regulators and policy makers can enforce on the Core network elements and EIR for detection and blocking of fraudulent devices.

The requirements in this document can be pulled into a policy framework or Statement of Purpose (SOP) for blocking fraudulent devices.

This document also covers a questionnaire for vendors that regulators can use and an inter-operability test matrix for testing key areas that affect fraudulent device blocking.

1.3 Acronyms, abbreviations, and terms

Table 1-1 Acronyms, abbreviations, and terms

Acronym	Definition
CDR	Charging data record
EIR	Equipment Identity Register
GSMA	Global System Mobile Association
HLR	Home location register
HSS	Home subscriber server
IMEI	International mobile equipment identity
IMSI	International mobile subscriber identity
IWF	Inter-working function
MME	Mobility management entity
MNO	Mobile network operator
MSC	Mobile switching center
MS-ISDN	Mobile station international subscriber directory number
SGSN	Serving GPRS support node
SOP	Statement of Purpose
TAC	Type allocation code

1.4 References and standards

Reference documents that are no longer applicable are deleted from this table; therefore, reference numbers may not be sequential.

Table 1-2 References and standards

Document	DCN or URL
Mobile Application Part (MAP) specification, 3GPP TS 29.002 V15.1.0 (2017-09)	https://portal.3gpp.org/
Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol, 3GPP TS 29.272 V14.5.0 (2017-09)	https://portal.3gpp.org/
Numbering, addressing and identification, 3GPP TS 23.003 (1999)	https://portal.3gpp.org/
Telecommunication management, Charging management; Charging Data Record (CDR) parameter description, 3GPP TS 32.298 V9.2.0 (2009-12)	https://portal.3gpp.org/
Identification cards – Identification of issuers – Part 1: Numbering system, ISO/IEC 7812-1:2017	https://www.iso.org/standard/66011.html
Documentation on DIRBS GitHub repositories	https://github.com/dirbs

2 EIR and Central EIR Architecture

2.1 EIR architecture

EIR is a Core network element that interfaces with MSC, IWF, SGSN, and MME to provide device validation capabilities for devices, operating on following access networks:

- 2G (CDMA/GSM)
- 3G(UMTS)
- 4G (LTE)

Figure 2-1 shows components of 3GPP network architecture that interface with an EIR when it is deployed in an individual operator's network.

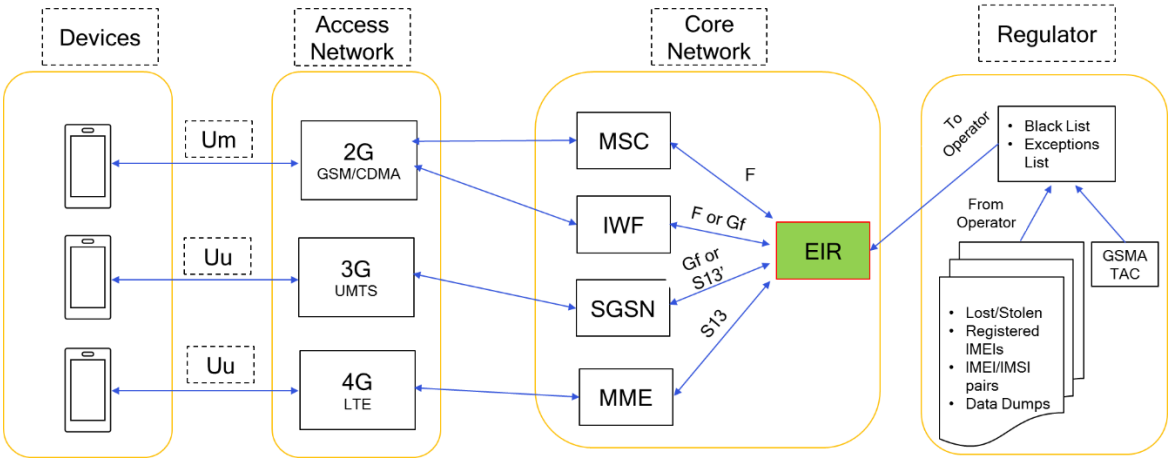

Figure 2-1 Individual operator EIR deployment

Table 2-1 lists Core network elements and their interfaces.

Table 2-1 Core network elements

Element	Function
EIR	▪ Identifies valid devices and allows them to access cellular service ▪ Main function is to prevent fraudulent devices from accessing cellular network
Mobile switching center (MSC)	Interfaces with EIR over MAP protocol F interface[1]
Serving GPRS support node (SGSN)	Interfaces with EIR over MAP protocol using GF interface[1] or Diameter Protocol using the S13 interface[2]
Mobility management entity (MME)	Interfaces with EIR using S13 Diameter protocol[2]

Element	Function
Regulator	▪ Provides blacklist (contains International mobile equipment identities (IMEIs) which must be blocked and exceptions list (with IMSI/IMEI pairs that are granted exceptions) to the Mobile Network Operator ▪ Lists generated by processing GSMA type allocation code (TAC) data, stolen device data, device registration data (from device importing entities), IMEI/IMSI pairing data, and operator data dumps ▪ EIR uses these lists to block fraudulent devices or grant exceptions as needed
1 Defined in *Mobile Application Part (MAP) specification* (3GPP TS 29.002) 2 Defined in *Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol* (3GPP TS 29.272)	

2.2 C-EIR architecture

Central EIR (C-EIR) generally refers to an architecture with a centralized database, typically maintained by a regulator, that manages and distributes lists (e.g. blacklist) to operator EIRs. This node does not perform EIR functions such as blocking; it simply manages and distributes lists that operators use to provision their own EIR(s) in their network.

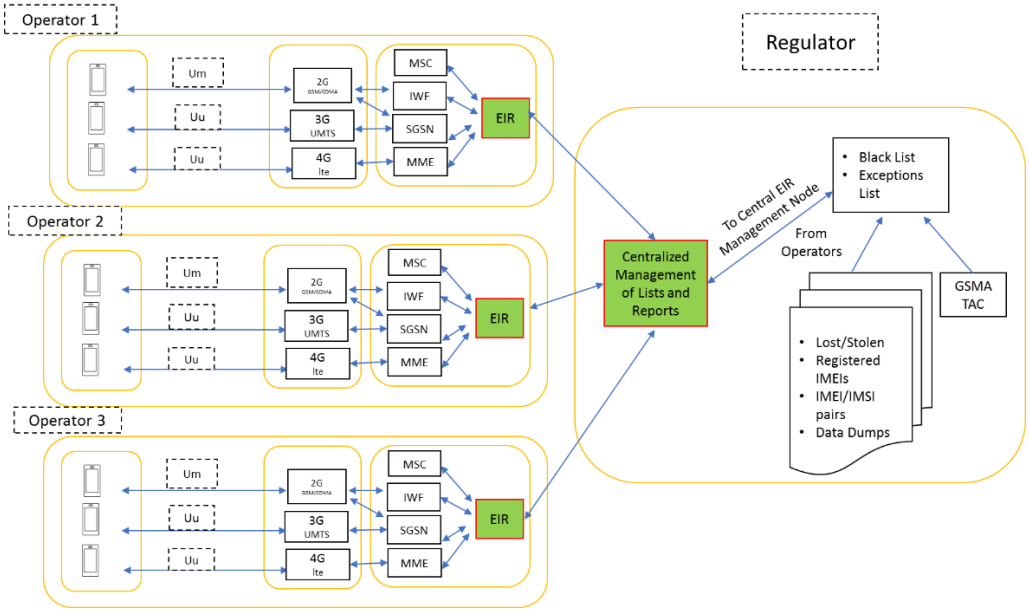

Figure 2-2 Typical C-EIR architecture & Interfaces

DIRBS operates as a C-EIR that manages and distributes blacklist, exceptions lists, and notification lists to operators for EIR provisioning and notification of customers. The C-EIR concept enables:

- Central management of lists across operators to ensure consistent behavior on all operator networks (e.g. adding a device to the blacklist managed by the C-EIR ensures that it will be blacklisted by all operators)
- Centralized analysis across operators to provide more effective identification of fraudulent activity such as cloning (e.g. the same cloned identifier can be observed in multiple networks)

- Centralized reporting to identify trends and compliance across operators

Because the C-EIR is not involved in real-time functions such as IMEI authorization during registration and/or call attempts, it has significantly lower availability and latency requirements than an actual EIR network element. As such, data transfer between C-EIR and operators can be done infrequently (e.g. daily data dumps and list distributions). These data transfers are facilitated with mechanisms such as dedicated VPN links, automated API calls, and/or automated SFTP transfers may be used between each operator and the C-EIR.

2.3 Alternate C-EIR concept

A less common interpretation of the C-EIR concept refers to an architecture with a centralized network element that acts a large EIR for all operators (i.e. in place of separate operator EIRs). Henceforth referred to as C-EIR$_{Alt}$ in this document, such implementations are uncommon in practice as they inherently introduce a network element that is not controlled by the operator but has the potential to impact customer experience with the operator's network.

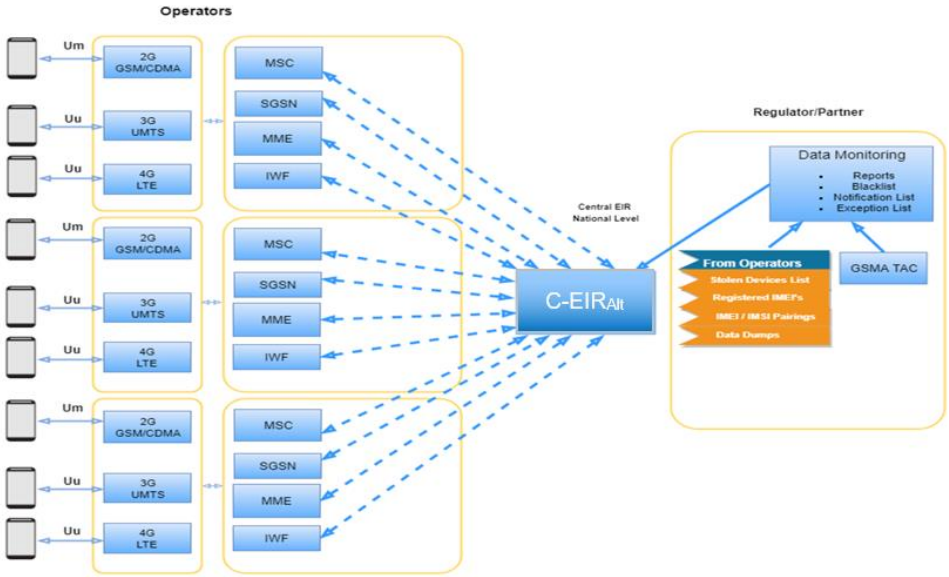

Figure 2-3 C-EIR$_{Alt}$ concept

While conceptually possible and providing similar benefits to a typical C-EIR implementation, this C-EIR$_{Alt}$ concept has several challenges that typically prevent it from being deployed:

- Operators have no control over the network element (C-EIR$_{Alt}$) that could potentially introduce IMEI authentication latency and that is responsible for blocking their subscribers
- Interoperability testing is required for all MSC, SGSN, MME, and IWF network elements that will make be making queries to the C-EIR$_{Alt}$
- In the event of a C-EIR$_{Alt}$ failure, all mobile users across all operators could be affected
- C-EIR$_{Alt}$ needs to be designed to scale to support all IMEI authentication traffic across all operators without introducing latency that could impact customer experience

3 High Level Call Flows

Table 3-1 lists the 3GPP messages that Core network elements (MSC, SGSN, MME) send to the EIR for IMEI validation requests.

Table 3-1 3GPP references – IMEI validation commands

Interface	Protocol	Operation/command	3GPP ref
F	MAP	Check IMEI	*Mobile Application Part (MAP) specification* (3GPP TS 29.002)
Gf			
S13	Diameter	ME-Identity-Check-Request/Answer (ECR/ECA)	*Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol* (3GPP TS 29.272)
S13			

3.1 GSM/UMTS call flow

Figure 3-1 shows the high-level call flow during IMEI validation request on GSM/UMTS network.

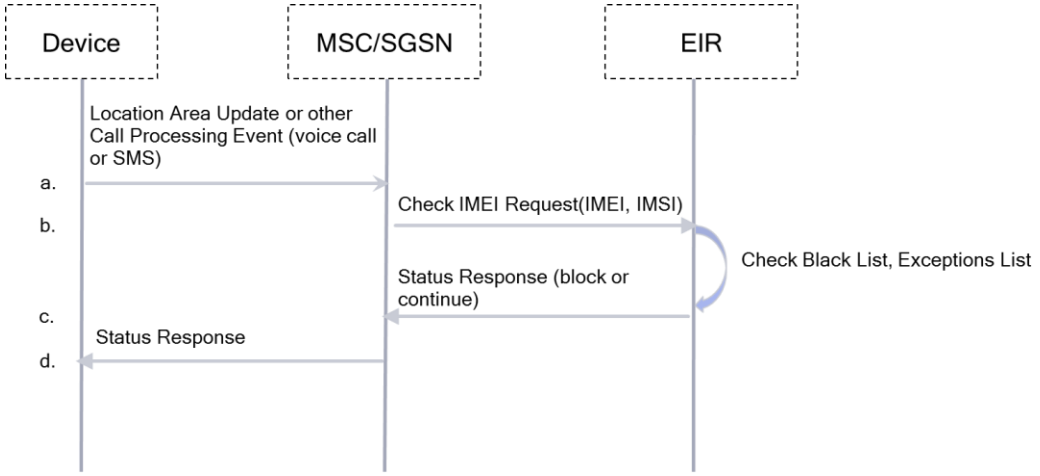

Figure 3-1 GSM/UMTS IMEI validation request

The GSM/UMTS call flow takes the following steps:

1. Device sends Location Area Update or a call processing event to the MSC/SGSN.
2. MSC/SGSN configured to send IMEI and IMSI in Check IMEI request at every "n" LAU or call processing signaling events. In this case, the MSC/SGSN sends a Check IMEI request to EIR (see Section 7.2).

3. EIR extracts the IMEI and IMSI fields from Check IMEI request message and checks them against the blacklist and exceptions list.
4. EIR sends a response back to MSC/SGSN to either block or allow the IMEI.
5. Device receives a response from MSC/SGSN.

3.2 LTE call flow

Figure 3-2 shows the high-level call flow during an IMEI validation request on the LTE network.

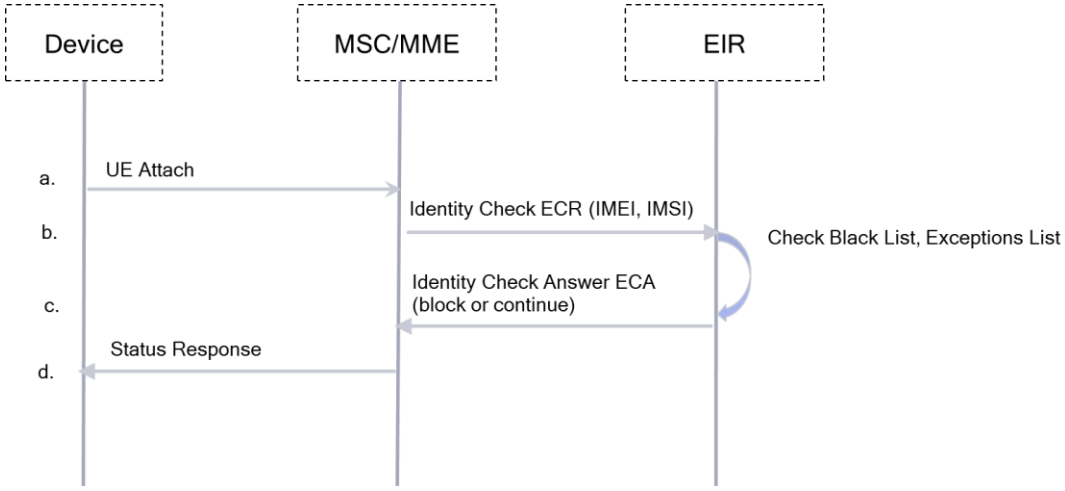

Figure 3-2 LTE IMEI validation request

The LTE call flow takes the following steps:

1. Device sends UE attach event to the MSC/MME.
2. MSC/MME is configured to send IMEI and IMSI in Identity Check ECR request at every “n” UE Attach signaling events. In this case, the MME sends an Identity Check ECR request to EIR.
3. EIR extracts the IMEI and IMSI fields from the Identity Check ECR request message and checks them against the blacklist and exceptions list.
4. EIR sends an Identity Check Answer back to MME to either block or allow the IMEI.
5. Device receives a response from MME.

4 IMEI Authentication & Blocking Logic

On a signaling event from a mobile device (event can be a device registration, location area update, data call set up, sending an SMS, etc.) the Core network element (MSC, SGSN, MME) may send a request for IMEI validation to the EIR (see Figure 4-1).

EIR obtains an IMEI/IMSI pair from the incoming Check IMEI message request and takes the following actions:

- Allows service if the IMEI is not on the blacklist
- Allows service if IMEI is on blacklist and if IMEI/IMSI pair is on exceptions list
- Blocks service if IMEI is on blacklist and IMEI/IMSI pair is not on exception list

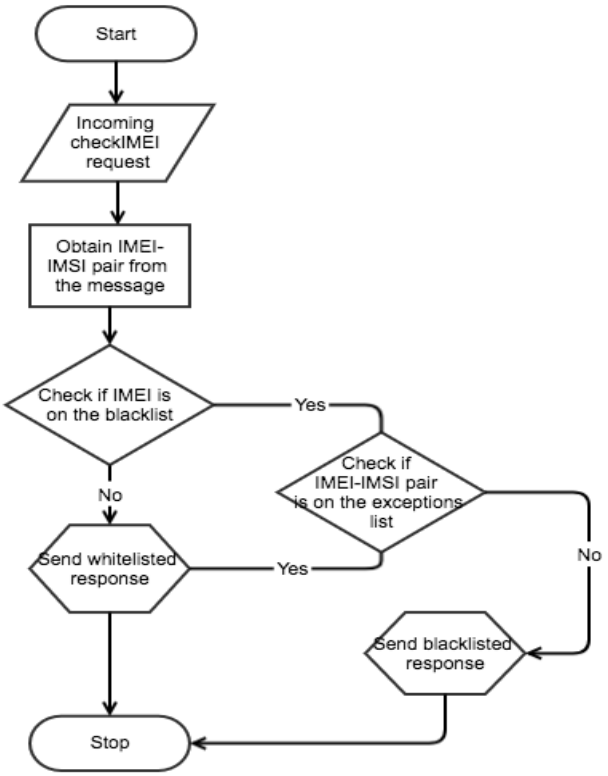

Figure 4-1 IMEI authentication & blocking logic

5 Regulatory Requirements

This chapter covers key requirements for regulatory authorities to enforce in their respective countries. Regulatory authorities are empowered by local governments to develop frameworks to block stolen phones, fraudulent phones with non-standard identifiers, and smuggled phones. As part of the development framework, regulators prepare a Statement of Purpose (SOP) containing requirements that all operators in the country must adhere to.

Requirements in this chapter can be added to regulator SOPs.

5.1 Core Network Requirements

Figure 4-1 shows that incoming Check IMEI request and key Core network requirements are dependent on contents of the Check IMEI request.

5.1.1 (CN-01) Presence of IMEI & IMSI in IMEI validation requests

Regulators must enforce that the Check IMEI message and ME Identity Check Request message contain both the IMEI and IMSI of the mobile device.

Most network elements (MSC, SGSN, MME) support enabling of IMSI in IMEI validation requests via a IMSI configuration flag (e.g. IMEICHKWITHIMSI). Mobile network operators must enforce that IMSI is present in IMEI validation requests sent to the EIR.

5.1.2 (CN-02) Presence of MS-ISDN in IMEI validation requests

If Network elements (MSC, SGSN, MME, IWF) support sending MS-ISDN field in IMEI validation requests via configuration settings, the MS-ISDN field should be sent in Check IMEI message and ME Identity Check Request message.

5.1.3 (CN-03) IMEI validity

The regulator must enforce that IMEI sent to EIRs by the MNO Core network elements (MSC, SGSN, MME, IWF) is valid and follows the structure of the IMEI specified in *Numbering, addressing and identification* (3GPP TS 23.003).

A mobile device is uniquely identified by its IMEI. IMEI sent by network elements for IMEI validation at EIR must contain the valid 14 digits and IMEI must be encoded as decimal digits only. For additional information, see Chapter 10.

5.1.4 (CN-04) Malformed IMEIs blocking

The regulator must enforce that malformed IMEIs must be blocked by MNOs at the edge of the network typically at the Core network elements (MSC, SGSN, MME, IWF). This reduces non-standard data processing burdens on EIR and propagation of malformed IMEIs throughout the network and in call data and billing records. For IMEI examples and testing, see Chapter 0.

5.1.5 (CN-05) Operator data dumps

The regulator can request operator charging data record (CDR) dumps for detection of malformed IMEIs in the network and for other analysis that results in blacklist and exceptions list generation. Consumers are charged for data sourced from different fields in different types of CDRs produced in the operator's network, e.g., SMS, packet data, voice call.

CDRs from some session types must be excluded, i.e., emergency calls, and calls already blocked by EIR. For details on operator data dumps contents and requirements, see DIRBS_Operator_Data_Requirements.pdf at https://github.com/dirbs/Documentation

5.2 EIR requirements

Figure 4-1 shows the EIR logic blocks for blocking a fraudulent device and key EIR requirements for handling blacklist and exceptions list.

5.2.1 (ER-01) Storing blacklist and exceptions list

EIR must store blacklist and exceptions list provided by the regulator at requested intervals. Blacklists and Exceptions lists are typically generated daily. List generation frequency must be mandated by the regulator.

5.2.2 (ER-02) IMEI/IMSI override logic

EIR must extract IMEI/IMSI pairs from the IMEI validation request messages on MAP and diameter interfaces. The EIR must support IMEI/IMSI override logic to ensure IMEI pairs present in an exceptions list can continue to access cellular service even if the IMEI is on the blacklist.

5.2.3 (ER-03) Blocking IMEIs on blacklist

EIR must block IMEI present in the blacklist if the IMEI/IMSI pair is not on the exceptions list.

5.2.4 (ER-04) Capacity and scaling

EIR must have enough storage and backend processing to ensure blacklists and exceptions lists can be loaded in databases. These lists are expected to grow over time so storage and data processing needs must be planned accordingly.

6 Malformed and Invalid IMEIs

This chapter provides examples of malformed and invalid IMEIs and instruction on how to:

- Block at Core network elements
- Engage with operators to understand network implementations
- Conduct small-scale inter-op testing for detecting network behavior

6.1 Malformed international mobile equipment identities

Fraudulent devices may use malformed IMEIs on purpose to evade network detection for illegal activities and blocking such devices becomes difficult if non-standard compliant IMEIs propagate the network. The regulator must enforce a policy to stop devices with malformed IMEIs from network access. Malformed IMEIs must be blocked at MSC, SGSN, MME.

Network elements may sometimes mask malformed IMEIs with a decimal IMEI number to allow service and it becomes difficult to trace these IMEIs in call data records or network traces.

NOTE: Blocking a malformed IMEI can be implemented at EIR but it is a non-standard procedure and requires additional support from the EIR vendor for entering a list of malformed IMEIs and blocking them in an EIR increases costs.

Table 6-1 Malformed IMEI examples

S.No	Type	Example	Notes
1	NULL IMEI	“ ”	Difficult to track as Core network elements can mask a NULL IMEI with a number which then propagates through the network and shows up in CDRs
2	IMEIs with Hex characters or Alphabets	"DEABFCDE2ABFEC", "MNVZLKvuGSQWRTY"	
3	Invalid Length too long	"567123098764107642"	
4	Invalid Length too short	"5671230”	

6.2 Inter-op testing

Sometimes MNOs are not aware of types of fraudulent and malformed IMEIs accessing their network. The presence of malformed IMEIs on network can be detected by examining call data records as a starting point. If malformed IMEIs are detected in the call data records, additional understanding and engagement with the MNO network is needed by a data driven process.

This process includes:

- Requesting call data records (CDR) data dumps and analyzing them to identify instances of malformed IMEIs
- Generating a report that breaks down the type of malformed IMEI categories seen (NULL IMEI, Alphanumeric, Hex, All 0s, repeating digits, etc.)

- Engaging with operators to understand network and vendor specific implementations:
  - Share operator questionnaire to further understand their Core network and EIR implementations (see Chapter 8)
  - Conduct inter-op testing, i.e., adversarial tests are conducted with devices having malformed or invalid IMEIs (see Chapter 9)

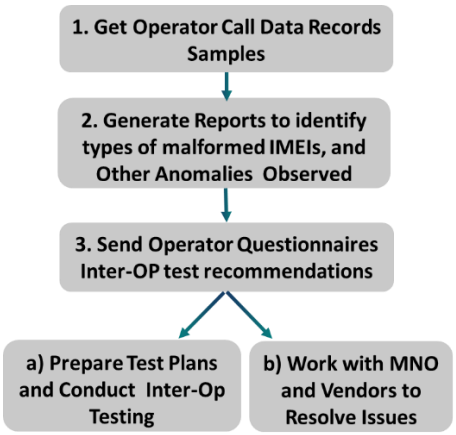

Figure 6-1 Malformed IMEI detection and test process

7 Other EIR Considerations

This chapter provides guidelines on factors that affect EIR capacity, performance, and pricing.

7.1 Capacity

Storage and backend processing must determine capacity requirements in an EIR. The number of entries in the lists (blacklist and exceptions list) that can be provisioned in the EIR database determine storage needs. The hardware architecture determines processing needs. The EIR solutions offered by vendors can scale to support hundreds of millions of subscribers.

The EIR can be offered as a standalone node or as a combo solution that bundles multiple logical network elements together in a single hardware box. In the combo solution, hardware resources are shared among the local nodes. The most common example of EIR bundling is with a home location register (HLR). Storage needs in both the standalone and combo case are defined by database size supported by the hardware.

EIR hardware consists of racks with each rack containing multiple computing cards/boards for backend processing. Each computing card can support a few million subscribers per card in a combo solution. For example, a combo HLR+EIR solution consists of a rack containing 28 compute cards, with each card capable of serving approximately five million subscribers. This deployed solution using multiple racks can support a capacity of 200 million subscribers.

Most vendors claim that there is not an upper bound on the capacity that can be supported. Capacity for some of the smaller EIR vendors can be limited to 100-150 million subscribers. The capacity on an existing EIR solution can be scaled by adding additional hardware or by licensing additional capacity on existing hardware. As the EIR is highly robust and scalable, operators start by deploying capacity that can meet current needs and scale over time, as subscribers are added to the network, and the size of blacklists and exceptions lists grow.

7.2 Performance

EIR performance can be defined in terms of transactions per second (tps), or the numbers of Check IMEI requests that the system can scale to handle in each period.

Some vendors define performance by the number of Check IMEI transactions or requests they can support per hour.

The number of Check IMEI requests on the EIR are dependent on signaling events, such as:

- On device registration or a call processing event (sending or receiving an SMS)
- Periodically on location area update (LAU) as the device moves

Operators control and manage the frequency of Check IMEI requests on the EIR. For example, when the device is moving around, the LAU can be a frequent event. Therefore, operators decide to enable the Check IMEI request every ‘N’ number of LAU events. Typically, the value of “N” is greater than 1. For example, if operator configures the value at 5, every 5th LAU event would trigger a Check IMEI request.

Another metric to consider is the *"Check IMEI peak hour load"* on the EIR. This can be correlated to the number of active subscribers on the network during peak hour. For example, if the load on the EIR is estimated to be "N" Check IMEI request(s) for every active subscriber during the peak hour, the number of active subscribers during the peak hour would determine the performance requirements that EIR must meet.

The performance is also a function of the capacity of the EIR, as additional capacity can be added to the EIR to handle proportional growth in Check IMEI requests.

7.3 Pricing

EIR pricing varies based on supported features and the business relationship between the operators and vendors and the competitive landscape of vendors share in the market. This section provides guidance on the parameters which drive the pricing costs of EIR.

Figure 7-1 EIR pricing parameters

EIR pricing is a function of different parameters:

- Installed hardware (capacity, standalone vs. combo, redundant system)
  - Capacity refers to the number of racks and compute cards per rack installed
  - Level of redundancy (active/active links, active/fallback links)
  - Standalone vs. combo solution refers to EIR deployment as a standalone node or a combo solution, i.e., EIR+HLR
- Licensed software capacity
  - In the combo solution, the licensing fee can be per-subscriber, based on the number of subscribers that are provisioned in the HLR+EIR or the operator can purchase bulk subscriber license that apply to both HLR and EIR entries
  - For standalone EIRs, the fee is based on the number of entries provisioned in the different lists
- EIR features
  - In the traditional EIR use case where the EIR must check if the IMEI exists on the blacklist or not, the vendor can charge based on the number of requests per second that the EIR must support

- The vendors may also charge nominal fees to unlock certain features on the EIR, i.e., IMEI-IMSI overriding and blocking non-standard features such as malformed IMEIs

- Performance requirements
  - Number of Check IMEI requests per second or in the peak hour

8 EIR and Core Network Questionnaire

Table 8-1 provides a list of questions that operators can answer to help regulators understand EIR and Core network implementations, costs, and vendor details. This questionnaire helps make better national policy statements to block fraudulent IMEIs.

Table 8-1 EIR and Core network questionnaire

1. **EIR Architecture and Design**	
1.1	What is the architecture of EIR? a) Central EIR b) Individual Operator EIR
1.2	What is the deployed EIR solution? a) Standalone EIR b) HLR/EIR Combo Solution
1.3	What is the current Hardware capacity of EIR – Storage and Processing in terms of number of subscribers EIR can Support?
1.4	What is the current software License capacity of EIR Processing in terms of number of subscribers EIR can Support? Can more subscriber be added to existing HW via Software License change?
1.5	What is the maximum hardware capacity they can have in their EIR? This helps regulator understand if HW is designed to scale for a few years as Blacklist and Exceptions list grow
1.6	What is the maximum software licensing capacity their EIR can handle?
1.7	What is the unit of software licenses? Is it on per subscriber basis or a bulk license?
1.8	Does EIR vendor charge for licenses for each type of list EIR maintains or the single license covers all the lists?
1.9	Which Vendors is MNO using for EIR in their CORE Network?
1.10	What is the type of hardware used for EIR (Type of servers etc.)?
1.11	What is the level of redundancy in EIR MNO used (active/active, active/fallback)?
1.12	What is the price of their overall EIR Solution (optional)?
2. **CORE Network Infrastructure Vendor**	
2.1	Which Vendors is MNO using for MSCs in their CORE Network?
2.2	Which Vendors is MNO using for SGSNs and MME in their CORE Network?
2.3	Which Vendors is MNO using for IWF in their CORE Network?
2.4	Which Vendors is MNO using for billing system in their CORE Network?
2.5	If they have IWF in their network which vendors is MNO using in their CORE Network?
3. **EIR Functionalities**	
3.1	Does the check_IMEI message between MSC and EIR in their network contains IMSI?
3.2	Does the check_IMEI message between MSC and EIR in their network contains MSISDN?
3.3	Does the ECR message between MME and EIR in their network contains IMSI?
3.4	Does the ECR message between MME and EIR in their network contains MSISDN?

3.5	What's the performance of EIR in TPS (transactions per second) or Check IMEI or ECR messages per seconds?
3.6	How many lists MNO's EIR maintain (Blacklists, Exceptions List)?
3.7	Is IMEI override function is present in EIR?
3.8	What's the capacity of IMEI Override Table in EIR (How many IMSIs can be paired with single IMEI?)
3.9	Does IMEI override function works with IMSI or MSISDN or with both?
3.10	Does EIR's Blacklist accommodate Malformed IMEIs (NULL IMEIs, alpha numeric IMEIs, HEX IMEIS, special characters)?
3.11	Does EIR's Blacklist accommodate IMEIs less than 14 and greater than 16 digits?
4. **CORE Network Functionalities**	
4.1	Does MNO's MSCs & SGSNs/MMEs are configurable to allow or restrict Malformed IMEIs?
4.1.1	Do MSCs/SGSNs allow NULL IMEIs?
4.1.2	Do MSCs/SGSNs allow alpha-numeric IMEIs?
4.1.3	Do MSCs/SGSNs allow IMEIs less than 14 and greater than 16 digits?
4.1.4	Does MSC/SGSN perform any sort of masking on invalid IMEIs?
4.1.5	Do MSCs/SGSNs allow IMEIs with special characters?
4.2	Can MNO's billing system extract Radio Access Type along with date, IMEI, IMSI & MSISDN?
4.3	Can MNO provide HLR Data dumps?
4.4	Can MNO's billing system extract LAC and Cell IDs along with other parameters?
4.5	Does billing system extract all the parameters from CDRs and store them or does it store selected fields only?
4.6	In case of selected parameters, how long will MNO take to make available those rejected parameters?
4.7	Does the MNO billing system perform any type of masking/altering on invalid IMEIs especially NULL IMEIs?

9 Inter-Op Test Cases – Malformed and Invalid IMEIs

Table 9-1 lists tests that can be executed to observe how the network handles malformed and invalid IMEIs. This testing can be done after Operator Call data records analysis is complete.

In the test table below, we have listed examples of IMEIs that are either Malformed or Invalid and seen in the field in operator data dumps.

To execute the tests, a few test devices can be programmed with IMEI to trigger Check IMEI or ECR requests from the Core network (MSC, SGSN, MME). Ideally, Core network elements block malformed IMEIs and EIRs to block invalid IMEIs.

If the network does not block malformed IMEIs, logs can be collected at each network node for evidence collection, further analysis, and discussions between regulator, operator, and vendors to implement blocking.

If EIR does not block invalid IMEIs, the regulator can step in and work with Operators to ensure that invalid IMEIs are on blacklists and thus blocked by EIRs.

Table 9-1 Test case matrix

Type	Case description	IMEI in DUT
Malformed	**NULL IMEI**	
	Null IMEI	""
	IMEIs with hexa-decimal values	
	Multiple Hexa-Decimal IMEI [=14]	"DEABFCDE2ABFEC"
	Multiple Alpha-Numeric IMEI [=14]	"BA0A0000000000"
	Multiple Hexa-Decimal IMEI [=14]	"FFFFFFFFFFFFFF"
	Multiple Alpha-Numeric IME [=15]	"00D0D0D0D0D0D00"
	Multiple Alpha-Numeric IMEI [=15]	"355E87F00000000"
	Multiple Alpha-Numeric IMEI [=15]	"35295907A9CD4E0"
	Multiple Mix IMEI [=15]	"352502084170D00"
	IMEIs with alphabets other than hex digits	
	Multiple Alphabets IMEI [=14]	"PWIUYTRWQLKJHM"
	Multiple Alphabets IMEI [=15]	"MNVZLKvuGSQWRTY"
	IMEIs with special characters	
	Single Special-Character IMEI	"#" or "*" or any other character
	Multiple Mix IMEI [=15]	"35424208#*21340"
	Multiple Blank Spaces IMEI [=14]	" "
	Incorrect length - IMEIS < 14 and IMEIs > 16 tests	
	All Zeros IMEI [<14]	"00"
	Single Hexa-Decimal IMEI	"F"
	Multiple Hexa-Decimal IMEI [<14]	"BA0A"

Type	Case description	IMEI in DUT
	Single Decimal IMEI	"8"
	Multiple Decimal IMEI [<14]	"35365308"
	Multiple Decimal IMEI [>16]	"567123098764107642"
Invalid	**IMEIs with same digits**	
	Multiple Alpha-Numeric IMEI [=15]	"000000004037A50"
	All Zeros IMEI [=14]	"00000000000000"
	All Ones IMEI [=14]	"11111111111111"
	All 2s IMEI [=14]	"22222222222222"
	All 3s IMEI [=14]	"33333333333333"
	All 4s IMEI [=14]	"44444444444444"
	All 5s IMEI [=14]	"55555555555555"
	All 6s IMEI [=14]	"66666666666666"
	All 7s IMEI [=14]	"77777777777777"
	All 8s IMEI [=14]	"88888888888888"
	All 9s IMEI [=14]	"99999999999999"
	IMEIs with decimal values	
	Multiple Decimal IMEI [=15]	"353653080000000"
	Multiple Decimal IMEI [=14]	"00000000123456"
	Multiple Decimal IMEI [=14]	"11223344556677"
	Multiple Decimal IMEI [=15]	"123456789012345"
	Multiple Decimal IMEI [=14]	"01010101010101"

Table 9-2 shows an example test report that can be generated for each test case.

Table 9-2 Test report example

#	IMEI seen at EIR	IMEI seen at MSC	IMEI seen at SGSN/ MME	Test MSISDN	EIR vendor	MSC vendor	SGSN/ MME vendor	Notes
1	Yes	Yes, Not Blocked	N/A	408-650-1234	Nokia	Huawei	Huawei	

10 IMEI Structure

IMEIs are unique to every handset and is defined in 3GPP TS 23.003

The IMEI in blacklist or exceptions list in EIR can have either a 14-digit IMEI or a 15-digit IMEI (with a computed Luhn digit). The check digit is not transmitted.

IMEI contains the following elements where each element must be encoded as **decimal digits only**:

- **TAC *(*8 digits)** consists of the reporting body identifier (AA), indicating the GSMA approved group that allocated TAC
  - For example: BABT allocates TACs in England and MSAI allocates TACs in India
- **Serial number (6 digits)** uniquely identifies the unit of a given device model
- **Check digit (1 bit)** helps guard against the possibility of incorrect entries in EIR equipment
  - Calculated according to the Luhn formula (see *Identification cards – Identification of issuers – Part 1: Numbering system* (ISO/IEC 7812-1))
  - Check digit is a function of first 14 digits in the IMEI (check digit not transmitted)

Table 10-1 IMEI – TAC, serial number, check digit

TAC								Serial number						Check digit
A	A	B	B	B	B	B	B	C	C	C	C	C	C	D
8 Digits								6 Digits						1 Digit

11 Blacklist and Exceptions List

Information about these lists is touched upon briefly in this section. For details on the definition and usage of these lists, please refer to the DIRBS Core User Guide located at: https://github.com/dirbs/DIRBS-Core/tree/master/Documentation

11.1 Blacklist

The blacklist contains IMEIs that must be blocked by the EIR.

During blacklist generation, regulators must ensure that the IMEI meets one of the blacklisting conditions when operator provided data is checked against GSMA TAC data base, stolen list data, or device registration data.

Some examples of specific conditions include:

- Invalid IMEI (not registered in GSMA TAC database)
- Duplicate IMEI (possible cloned device)
- Stolen IMEI (as reported to authorities)

The blacklist is generated on a nationwide basis and contains the IMEI, the date IMEI must be blocked, and a reason for blocking.

11.2 Exceptions list

The exceptions list contains IMEI to IMSI pairing information. Regulators provide exceptions list to operators. EIR grants exceptions to these IMEI/IMSI pairs from blocking even if the IMEI is on a blacklist. Exceptions lists are generated on a per-operator basis and contains IMEI and IMSI pair information.