International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5053

(01/2021)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Combating counterfeiting and stolen ICT devices

Mobile device access list audit interface

Recommendation ITU-T Q.5053

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	**Q.5050–Q.5069**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.5053

Mobile device access list audit interface

Summary

Recommendation ITU-T Q.5053 defines the methodologies and interfaces between mobile device access list audit system (MDALAS) and mobile network operators' equipment identity register (EIR) to audit and reconcile whether the mobile network operators (MNOs) are complying with the defined mobile device access list requirements. This Recommendation proposes different types of methodologies and interfaces to check and reconcile the mobile device access list used by the MNOs to comply with the regulations for the mobile device access list audit system (MDALAS).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5053	2021-01-13	11	11.1002/1000/14587

Keywords

Access list, audit, blacklist, mobile device, whitelist.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.5053

Mobile device access list audit interface

1 Scope

In some countries, international mobile equipment identities (IMEIs) to be blacklisted, thus blocking access to the mobile network, or to be allowed (whitelisted) by the mobile network operators (MNOs), may be provided by a telecom authority or law enforcement agency (LEA) via mobile device identifier database (MDID). The mobile device access list as defined by the regulators under the country's governing laws and regulations are either directly provided to the MNOs by the authorities or only the access to these lists is provided to the MNOs instead of providing the actual lists.

There is no established mechanism to check and verify if the IMEI lists contained within each MNO's equipment identity register (EIR) contain all of the data provided by the various other IMEI sources and are therefore in compliance with locally mandated and/or agreed policies. Thus, there is a requirement to develop a common approach for audits and/or reconciliations of blacklist data to be undertaken.

This Recommendation suggests mechanisms to carry out such audits or reconciliations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.5052] Recommendation ITU-T Q.5052 (2020), *Addressing mobile devices with a duplicate unique identifier*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 mobile device identifier database (MDID) [ITU-T Q.5052]: A database containing aggregated information about mobile device unique identifiers.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 mobile device access list audit system (MDALAS): A system that authorised entities may use to audit, reconcile or verify accuracy of blocked or allowed international mobile equipment identity (IMEI) lists in individual mobile network operator (MNO) equipment identity registers (EIRs).

3.2.2 blacklist override (BLO): The list of subscribers that have blacklisted mobile devices (blocked international mobile equipment identities (IMEIs)), but who are still allowed to access mobile networks and services.

NOTE – A blacklist override comprises a combination of the international mobile equipment identity (IMEI) and the international mobile subscriber identity (IMSI).

4 Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

AMF Access and Mobility Management Function

BLO Blacklist Override

EIR Equipment Identity Register

GMSC Gateway MSC

GPRS General Packet Radio Service

HTTPS Hyper Text Transfer Protocol Secure

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

IWF Interworking Function

LEA Law Enforcement Agency

LTE Long-Term Evolution

MDALAS Mobile Device Access List Audit System

MDID Mobile Device Identifier Database

ME Mobile Equipment

MME Mobility Management Entity

MNO Mobile Network Operator

MSC Mobile Switching Centre

NIBAS Non-Intrusive Blacklist Audit System

SGSN Serving GPRS Support Node

SIM Subscriber Identification Module

5 Conventions

None.

6 Reference model

This Recommendation describes the possible mechanisms to confirm on the status of international mobile equipment identities (IMEIs).

6.1 Method 1 – Get IMEI status for mobile device

In this method the mobile device access list audit system (MDALAS) will query the MNO's equipment identity register (EIR) through standard 3GPP signalling messages.[1] As MNOs receive external messages through their gateway node only, so the MDALAS needs to send the message through this gateway depending on the network technology used by the MNO. This allows the MDALAS to check the status of a blacklisted, grey-listed or whitelisted international mobile

[1] All the relevant 3GPP standards for the current technologies are listed in the bibliography.

equipment identity (IMEI), based on an implementation scheme on an MNO's EIR through online interfaces and to validate if the IMEI list has been implemented correctly. Figure 1 shows the interface between the MDALAS and the MNO.

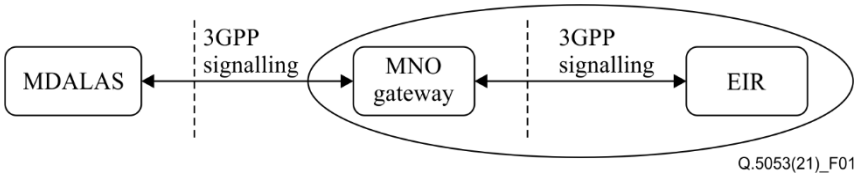

Figure 1 – Interface between MDALAS and MNO

6.1.1 Message exchange

– The MDALAS sends a CheckIMEI/ME_IdentityCheck/N5g-eir_EquipmentIdentityCheck request message to the gateway. The gateway forwards the request to the MNO's EIR.

– The MNO's EIR receives the message and returns a response message to the MNO gateway. The gateway forwards the response to the MDALAS. Figure 2 shows message flow between the MDALAS and the MNO.

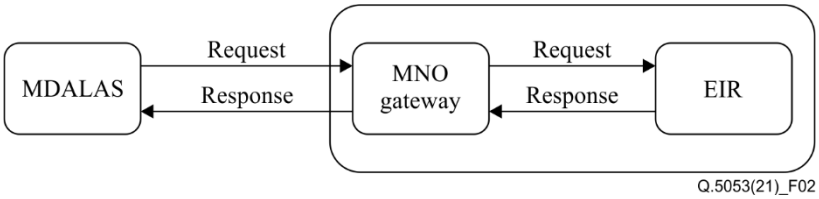

Figure 2 – Message flow between MDALAS and MNO

6.1.2 Detailed behaviour of MDALAS

Depending on the network architecture, the MDALAS shall use the CheckIMEI/ME_IdentityCheck/N5g-eir_EquipmentIdentityCheck message to get the IMEI status of a mobile device from the MNO's EIR. While receiving the response message from the MNO's EIR, the MDALAS shall check the IMEI status received on the status of the queried IMEI. Depending upon the result, the MDALAS takes following action:

– Received IMEI status from MNO EIR to be matched with the expected status as available with the MDALAS and reconciliation report to be prepared accordingly.

6.1.3 Detailed behaviour of EIR

When receiving the CheckIMEI/ME_IdentityCheck/N5g-eir_EquipmentIdentityCheck request message, the MNO's EIR shall check whether the mobile device is known. The EIR shall identify the mobile device based on the first 14 digits of the IMEI. The EIR shall return the IMEI status as White/Grey/Black in the response message.

6.1.4 Practical considerations

While this method offers certain advantages, such as avoiding the need to develop any proprietary interface or standardize any new message/protocol thus alleviating the need for any EIR upgrade or configuration changes itself, it may require an upgrade or configuration changes to the other network nodes, as explained below.

More importantly, the ability to channel messages to the MNO's EIR over the signalling network will only be possible if the MNO policies and network configurations allow receipt and processing of these messages from entities such as the MDALAS. This may not be possible depending on the signalling security policies and measures that have been deployed by the MNO and that have been mandated by local regulation.

As MNOs normally do not allow connection to their EIR from any external source, connection from a MDALAS needs to be through the gateway node. For example, a 2G/3G network could be connected through a gateway MSC (GMSC) or interworking function (IWF), a GRPS network through a serving GPRS support node (SGSN), a long-term evolution (LTE) network through a mobility management entity (MME), or a 5G network through an access and mobility management function (AMF). The MNO needs to allow the particular node MDALAS to connect to their network for performing an audit.

6.2 Method 2 – Get IMEI status through HTTP

In the online interface of Method 1 as presented in clause 6.1, the MDALAS can get the confirmation of listed international mobile equipment identity (IMEI) numbers only. IMEI/IMSI pairs or BLO subscribers can not be confirmed with this method. In this methodology, the MDALAS will need to get the IMEI status from the MNO's EIR using the HTTPS interface. Figure 3 shows the interface between MDALAS and EIR.

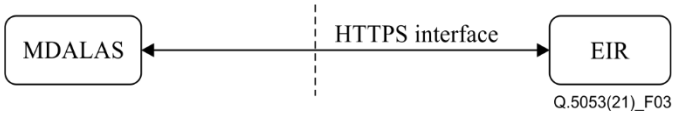

Figure 3 – Interface between MDALAS and EIR

6.2.1 Message exchange

The MDALAS sends a GetImeiStatusReq message to the EIR. The MNO's EIR receives the message and sends a response in GetImeiStatusResp message to the MDALAS. The MDALAS and EIR message flow diagram is shown in Figure 4.

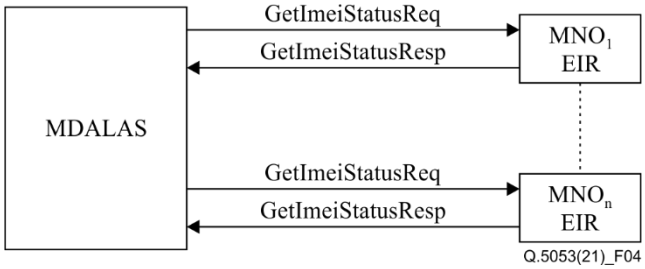

Figure 4 – GetImeiStatusReq message flow

Annexes A.1 and A.2 indicate the structure of the messages flow between the MDALAS and MNO EIR application server.

6.2.2 Detailed behaviour of MDALAS

The MDALAS shall use the GetImeiStatusReq message to get the IMEI status of mobile equipment from the MNO's EIR. When receiving the GetImeiStatusResp response message from the MNO's EIR, the MDALAS shall check the IMEI status. Depending upon the result, the MDALAS takes the following action:

– Received IMEI status from MNO EIR to be matched with the expected status as available with MDALAS and reconciliation report to be prepared accordingly.

6.2.3 Detailed behaviour of EIR

When receiving the GetImeiStatusReq request message, the MNO's EIR shall check whether the mobile device is known. The EIR shall identify the mobile device based on the first 14 digits of the IMEI. The EIR shall return the IMEI status as White/Grey/Black in the GetImeiStatusResp

response. If the mobile device is blacklisted and BLO list exists within the EIR for that IMEI, then the EIR shall send the BLO list corresponding to that IMEI.

6.2.4 Practical considerations

The EIR interface on HTTP messages is available for 5G only. Proprietary interfaces and APIs/messages will need to be standardized by the standardization bodies among all EIRs and MDALAS for the all other technologies.

6.3 Method 3 – Get Complete List of IMEIs

In the two methodologies, presented in clauses 6.1 and 6.2, an IMEI lists audit has been proposed for an individual mobile device. But to perform actual reconciliation, the MDALAS needs to know if there are some extra mobile devices in any MNO's EIR. In this methodology, the MDALAS will get the IMEI list for the provided status (White/Grey/Black) from the MNO's EIR using an HTTPS interface. Figure 5 shows the interface between the MDALAS and EIR.

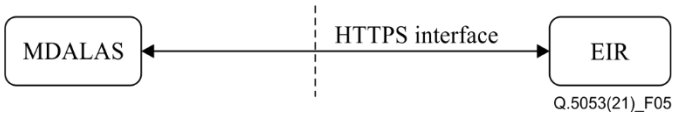

Figure 5 – Interface between the MDALAS and EIR

6.3.1 Message exchange

– The MDALAS sends a GetIMEIListReq message to the EIR.

– The MNO's EIR receives the message and sends a response in GetIMEIListResp message to the MDALAS.

The MDALAS and EIR message flow diagram is shown in Figure 6.

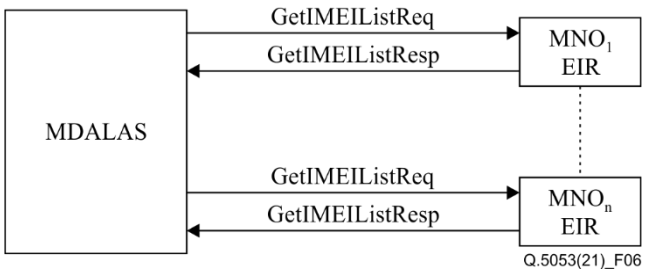

Figure 6 – Get IMEIlist message flow

Annexes A.3 and A.4 indicate the structure of the messages flow between the MDALAS and MNO EIR application server.

6.3.2 Detailed behaviour of MDALAS

The MDALAS shall use the GetIMEIListReq message to get the complete list of IMEIs from the MNO's EIR. When receiving the GetIMEIListResp response message from the MNO's EIR, the MDALAS shall match the list with its own IMEIlist. Depending upon the result, the MDALAS takes the following actions:

– The MDALAS shall generate additional IMEI list reports if the response message contains additional IMEIs for the provided status.

– The MDALAS shall generate a missing IMEI list report if the response message contains missing IMEIs for the provided status.

In instances where additional IMEIs are identified in the IMEI access lists provided by the MNOs that were not part of the list provided by the authorities, the MDALAS audit system will generate a separate report to highlight those IMEIs.

6.3.3 Detailed behaviour of EIR

When receiving the GetIMEIListReq request message, the MNO's EIR shall check its database for the complete list of IMEIs for requested IMEI status. The EIR shall return the complete list of IMEIs of requested status in a GetIMEIListResp response message. If the requested IMEI status is black, then in addition to the blacklist the MNO EIR will send the BLO list corresponding to the blacklisted IMEIs.

6.3.4 Practical considerations

EIR interfaces on HTTP messages are available for 5G only. Proprietary interfaces and APIs/messages will need to be standardized by the standardization bodies among all EIRs and MDALAS.

The authorities will need to ensure standard operating procedures between the authorized entities and the MNOs are in place to avoid any disruption in the verification and audit process.

6.4 Method 4 – Non-intrusive blacklist audit system (NIBAS)

This clause provides an alternate methodology specific to blacklist implementations to verify whether the provided blacklists have been properly provisioned into the MNOs EIRs and are in effect as per the regulatory mandate barring non-compliant devices from accessing the mobile network without any need to directly connect to the MNO's network (MSC/GMSC) or their EIRs on the dedicated link.

This approach is notably useful in countries where connectivity of an external system (such as MDALAS) to the MNOs' network nodes may not be possible. This proposed mechanism ensures continued regulatory compliance and conformity to the regulations by the MNOs.

This non-intrusive approach provides a mechanism that ensures MNO's comply to the regulatory mandate while providing the following benefits:

– Eliminates the need to define a new standard/protocol for messaging
– Eradicates the burden on EIR vendors to support any new interfaces and messaging for blacklist auditing
– Eradicates the burden on network infrastructure vendors to upgrade their network nodes
– Eliminates the need for interoperability testing between equipment of multiple EIR and network infrastructure vendors
– Alleviates the need to connect to MNO's EIR relieving any concerns of external components connecting to a live network
– Not prone to any inaccuracies or inconsistencies in an MNO's system as this approach does not directly rely on any information from the MNO's EIR

This methodology shall not use a regular mobile device but instead it shall utilize a specialized audit equipment/system available only to the authorised entity/regulator responsible for the IMEI audit purposes, that allows for verification of blacklisted IMEIs.

This process will allow the regulators or authorities to verify blacklisted IMEIs one-by-one by performing an automated network procedure for blacklisted IMEIs on all mobile networks using respective mobile operators' subscriber identification modules (SIM). Successful access to the given networks will indicate the blacklisted IMEIs were not blocked on a given MNO's network.

The sample procedure along with sample flow diagram (see Figure 7) is described below:

1. Originate a mobile call with a local SIM from an MNO on whose network the blacklisted IMEIs are being verified/audited using a blacklisted IMEI on the apparatus.
2. Generate a report if the call is successful indicating a violation by the MNO (MNO is not blocking the blacklisted IMEI on its network). Add that IMEI to a "Violation-List" with the network-IMEI information.
3. Repeat the above steps for the selected sample blacklisted IMEI.
4. Repeat the above procedure using SIMs from all other operators one at a time.

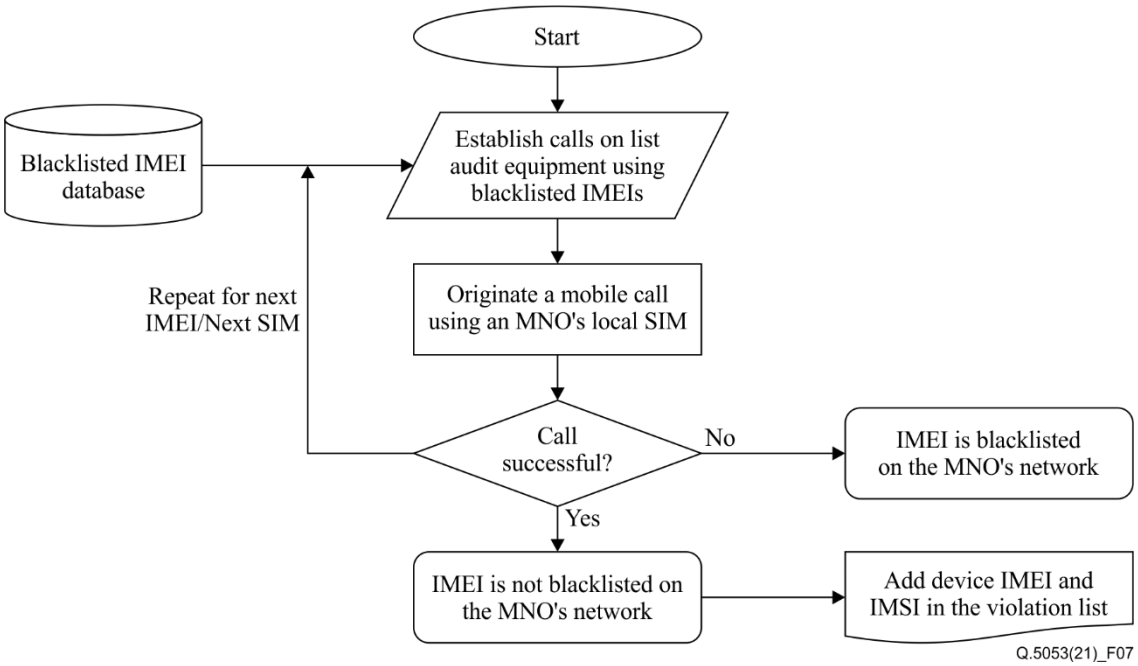

Figure 7 – NIBAS workflow

6.4.1 Practical considerations

It should be noted that most country regulations normally do not allow any IMEI tampering or reprogramming. This process requires special provisions in the regulations for the government and government authorized entities to utilize a specialized audit equipment/system. The availability of such equipment/system is usually restricted to government's verification/audit use only.

The authorities are encouraged to ensure that standard operating procedures between the authorized entities and the MNOs are in place to avoid any disruption in the verification and audit process.

The authorities can decide the appropriate sample size and periodicity to perform this audit procedure to ensure the process is not overburdened.

Annex A

Message structure

(This annex forms an integral part of this Recommendations.)

A.1 GetImeiStatusReq request message

This message will be sent by the MDALAS to the MNO EIR to get the status of the IMEI. It will have the content described in the Table A.1.

A.1.1 Message elements

Table A.1 - GetImeiStatusReq request message content

Name	Type	Length	Required	Description
MessageHeader	MessageHeaderType		R	Will contain the information of MNO, Zone and Date.
IMEI	IMEIType	14-16	R	IMEI of the mobile device

A.2 GetImeiStatusResp response message

This message will be sent by the MNO EIR node to the MDALAS in response to the GetImeiStatusReq message. It will have the content described in Table A.2.

A.2.1 Message elements

Table A.2 - GetImeiStatusResp response message content

Name	Type	Length	Required/ Conditional	Description
MessageHeader	MessageHeaderType		R	Will contain the information of MNO, Zone and Date.
ImeiStatus	String	5	R	It can be WHITE/ GREY/ BLACK
BLO	BLOType		C	Complete BLO List corresponding if the requested IMEI status is black
BLO/RecordCount	RecordCountType		R	Will contain the BLO List Count if BLO exists.
BLO/Record	BLORecordType		C	Will contain the <IMEI, IMSI> Pair of the complete BLO List. It is mandatory if Record Count is available.

A.3 GetIMEIListReq request message

This message will be sent by the MDALAS to the EIR to get the complete list of IMEIs of a particular IMEI status. It will have the content described in Table A.3

A.3.1 Message elements

Table A.3 - GetIMEIListReq request message content

Name	Type	Length	Required	Description
MessageHeader	MessageHeaderType		R	Will contain the information of MNO, Zone and Date.
ImeiStatus	String	5	R	It can be WHITE/ GREY/ BLACK

A.4 GetIMEIListResp response message

This message will be sent by the EIR node to the MDALAS in response to the GetIMEIListReq message. It will have the content described in Table A.4.

A.4.1 Message elements

Table A.4 - GetIMEIListResp response message content

Name	Type	Length	Required/ Optional	Description
MessageHeader	MessageHeaderType		R	Will contain the information of MNO, Zone and Date.
ImeiStatus	String	5	R	It can be WHITE/ GREY/ BLACK
IMEIList	IMEIListType		R	Complete List corresponding to the requested IMEI
IMEIList/RecordCount	RecordCountType		R	Will contain total number of records of requested IMEI status if exists.
IMEIList/Record	BlackListRecordType		C	Will contain exact IMEI, IMSI (optional) of requested IMEI status if RecordCount exists
BLO	BLOType	5	C	It will contain BLO if BLO exists for any IMEI in case of requested IMEI status is black.
BLO/RecordCount	RecordCountType		R	Will contain the BLO List Count if BLO exists for the IMEI status as black
IMEIBloList/Record	BloListRecordType		C	Will contain the <IMEI, IMSI> Pair of the complete BLO List if BLO count exists for the IMEI status as black.

Bibliography

[b-3GPP TS 23.060] 3GPP TS 23.060 (ETSI TS 123.060) *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description*.

[b-3GPP TS 23.401] 3GPP TS 23.401 (ETSI TS 123.401) *LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*.

[b-3GPP TS 29.002] 3GPP TS 29.002 (ETSI TS 129.002) *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile Application Part (MAP) specification*.

[b-3GPP TS 29.272] 3GPP TS 29.272 (ETSI TS 129.272) *Universal Mobile Telecommunications System (UMTS); LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol*.

[b-3GPP TS 29.511] 3GPP TS 29.511 (ETSI TS 129.511) *5G System; Equipment Identity Register Services*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021