International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Q

Supplement 73

(03/2021)

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

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

ITU-T Q-series Recommendations – Supplement 73

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.

Supplement 73 to ITU-T Q-series Recommendations

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

Summary

There are two alternative types of mechanisms and technology platforms available to address the issues related to counterfeit, illegal and stolen mobile devices in a country. There are inherent pros and cons to each approach. Supplement 73 to ITU-T Q-series Recommendations provides a detailed and comprehensive understanding of the underlying matters that should be clearly recognized, understood and addressed in order to have a successful system implementation.

Over the last few years many governments and countries have realized the importance and necessity of implementing technical solutions to combat the issues associated with the influx of counterfeit mobile devices, the illegal importation of mobile phones and mobile theft.

Given the complexities and the impact associated with the system implementation due to the requirements to handle these enormous issues, it is no wonder that governments are inundated with many difficult questions that are challenging to answer. Governments are generally not equipped with the technical expertise, especially in countries where the above-mentioned problems are most prevalent.

For the governments with the prime responsibility of developing the regulatory framework required for ensuring a smooth system deployment without causing any inconveniences to consumers, operators or importers, this creates a dependency on vendors and solution providers who offer technical solutions to address the above-mentioned issues.

There are two types of mechanisms that are available and can be deployed, permissive mechanisms and restrictive mechanisms. However, it is rather difficult for governments to find accurate and balanced information that covers all aspects for a complex deployment as well as the impact on various elements including the government, device manufacturers, local assembly, operators, importers, and most importantly the consumers.

This has resulted in a need to provide comprehensive information to governments so that they fully understand all relevant aspects and issues of system implementation and its impact on all stakeholders in the country. Equipped only with this knowledge, governments could determine and decide the best course of action and the right technical solution that suits their countries' needs and caters to local dynamics of the society.

This Supplement provides detailed information on the two mechanisms and highlights the strengths and weaknesses of each approach. Additionally, it provides guidelines to ensure a successful system implementation with a broad range of comprehensive measures to be adopted to combat the said issues.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q Suppl. 73	2021-03-26	11	11.1002/1000/14608

Keywords

Blocked-list, CEIR, counterfeit, EIR, illegal, IMEI, mobile devices, permissive systems, permissive, permitted-list, restrictive systems, restrictive, stolen, system implementation.

---

* 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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 73 to ITU-T Q-series Recommendations

Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices

1 Scope

This Supplement provides guidelines for permissive versus restrictive system deployments that should be considered when deciding what approach to employ in order to address the issues of counterfeit, illegal and stolen mobile devices.

2 References

[ITU-T Q.5050] Recommendation ITU-T Q.5050 (2019), *Framework for solutions to combat counterfeit ICT devices*.

[ITU-T Q.5051] Recommendation ITU-T Q.5051 (2020), *Framework for combating the use of stolen mobile devices*.

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

[ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *ITU-T X.1120-X.1139 series, Supplement on security aspects of smartphones*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloned identifier [ITU-T Q.5051]: Is a valid device identifier properly assigned by the responsible management entity to one device but is being used by other different devices.

3.1.2 equipment identity register (EIR) [b-3GPP TS 22.016]: An EIR is a network element in the core of mobile networks that is used to terminate an access attempt or ongoing call when performing IMEI Check procedure depending on the status of the IMEI in one of its registers; blocked-list, permitted-list, or tracked-list.

3.1.3 invalid identifier [ITU-T Q.5051]: Is a unique identifier that does not comply with the format defined in the technical standards or that is not included in the device identifier reference database distributed by responsible management entity.

3.1.4 mobile device [ITU-T X-Sup.19]: An electronic device used for making phone calls and sending text messages across a wide geographic area through radio access to public mobile networks, while allowing the user to be mobile, or a smartphone.

3.1.5 radio access technology (RAT type) [b-3GPP TS 29.060]: 3GPP RAT type indicates which radio Access Technology is currently serving the User Equipment.

3.1.6 smartphone [ITU-T X-Sup.19]: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

3.1.7 unique identifier [ITU-T Q.5050]: An identifier associated with a single device that aims to uniquely identify it.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 central equipment identity register (CEIR): The central equipment identity register (CEIR) maintains information on the eligibility of mobile devices to control access to the mobile networks. The CEIR interconnects with multiple equipment identity registers (EIRs) so that a common set of data is maintained and available to participating operators.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CEIR	Central Equipment Identity Register
DIRBS	Device Identification, Registration and Blocking System
EIR	Equipment Identity Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MNO	Mobile Network Operator
OEM	Original Equipment Manufacturer
RAT	Radio Access Technology
SIM	Subscriber Identity Module

5 Conventions

This Supplement applies the following verbal forms for the expression of provisions:

The keyword "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Supplement is to be claimed.

The keyword "should" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keyword "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Supplement.

6 System implementation modes

There are two types of systems available for implementation, referred to as permissive and restrictive. These modes fundamentally differ in how they allow or block network access to devices that are not considered 'compliant' as per the country regulations set by the government and/or the country regulator. Generally, devices that are not type-approved or certified by the regulator for use in a country, lack unique and valid device identifiers (IMEIs), reported lost or stolen and non-duty/tax-paid are considered 'non-compliant' and their access to the mobile networks is to be denied subject to such regulations in the country. A central equipment identity register (CEIR) is deployed as part of system implementation and in conjunction with a mobile operator's local EIR to identify compliant and/or non-compliant devices for granting or restricting network access to mobile devices.

6.1 Permissive versus restrictive modes

Figure 1 explains the two modes at a high level.

Figure 1 – Permissive and restrictive modes

6.1.1 Permissive mode

In permissive mode, equipment identity registers (EIRs) allow all devices on the network unless they are explicitly blocked.

In a permissive system, a device continues to receive mobile service from the operator until it is identified and categorized as an unauthorized device based on the defined rules and regulations set by the in-country authority. If the device's IMEI number does not appear on the blocked-list, it continues to get network service from its service provider. If it appears on the blocked-list, the device is blocked from registering on the network, except for emergency calls. In some cases, the legal enforcement authority responsible for stolen and lost mobile devices provides the blocked-list to the mobile operators. Other categories of devices in the blocked-list generally include IMEIs identified to be non-compliant as determined by the regulatory policy (e.g., devices programmed with all-zero IMEIs, etc.) post data analytics.

A permissive system should maintain the following lists:

- Blocked-list that contains IMEIs not allowed on the network.
- Tracked-list that contains IMEIs scheduled to be blocked unless their status is rectified (e.g., lost/stolen devices, suspected duplicate IMEI or non-payment of taxes and duties). A notification could be sent to alert the subscriber of the status of the device.
- Blocked-override-list (exceptions) that contains IMEI-IMSI or IMEI-MSISDN pairs to avoid blocking.

A permissive system synchronizes blocked, notification, and blocked-override-list (exceptions) list updates to operator EIRs. Operator EIRs use blocked-lists and blocked-override-list (exceptions) lists to grant or deny mobile access to the network.

Figure 2 depicts a conceptual call flow for allowing or rejecting device access in a permissive mode, where a country decides to take a central control that relies on a database with input of information from mobile operators and a feedback with the categorization of each IMEI accordingly with national regulation/rules.

Table 1 describes permissive mode system impact.

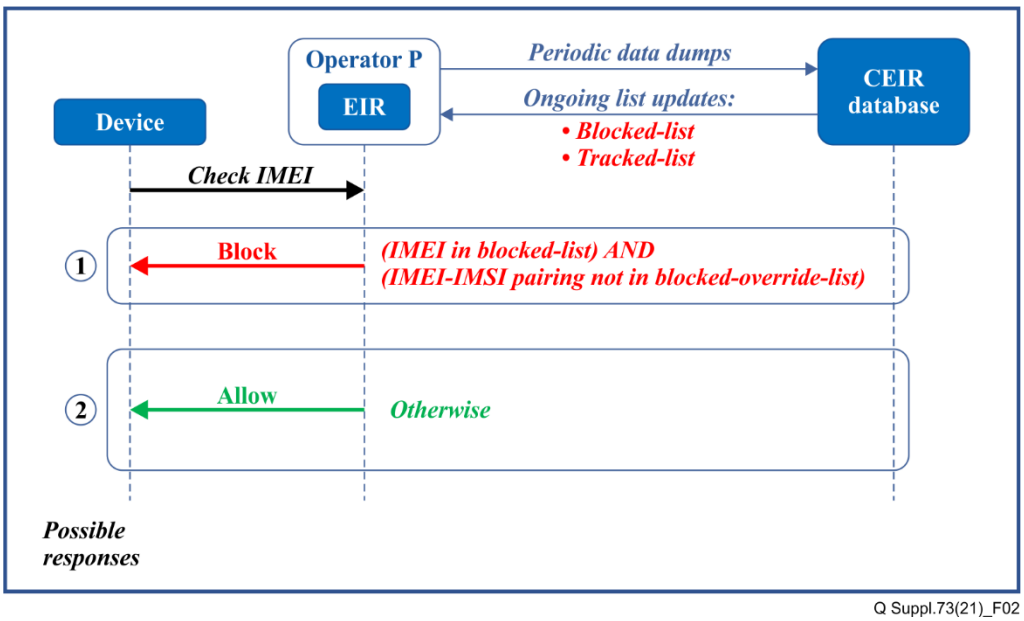

Figure 2 – Permissive mode data synchronization

Table 1 – Permissive mode system impact

Impact	Considerations	Permissive mode with exceptions
Data	**Data requirements**	Generally, the systems utilize IMEI-IMSI pairing or triplets (IMEI/IMSI/MSISDN) from the operators' network for analysis.
	Data processing	Offline (time delayed) processing.
	Processing methodology	Allows all devices initially (unless already blocked) until identified non-compliant in post-analysis and blocked.
EIR-CEIR integration	**Integration**	The system provides blocked-list and tracked-list for monitoring and notification purposes to the MNOs with no integration and interoperability requirements with their EIRs.
	Status update	Does not require real-time status updates.
	Capacity (storage, processing)	Lower requirements for processing capacity and storage. Only blocked-list Blocked-Override-list (exceptions) need to be supported.
Pairing	**IMEI-IMSI pairing**	IMEI-IMSI pairing not required for each device/customer.
	IMEI-IMSI pairing	Pairing is only required for a smaller set of IMEIs that are in the blocked-list and/or Blocked-Override-list (exceptions) list (e.g., to provide amnesty to existing devices or control IMEI duplication).

Table 1 – Permissive mode system impact

Impact	Considerations	Permissive mode with exceptions
Device Registration	**Registration**	Devices usable even if unregistered. Allows time for customers to register. Devices are blocked if not registered within the allowed time.
	Notification	Customers could be notified upon detection of unregistered devices.
Non-compliance detection	**Audit**	Process automation and various violation detection mechanisms (e.g., blocked-list violations) exist to ensure compliance to regulations.
Duplicate IMEI management	**Detection**	Detection granularity based on methodology used. All duplications can be detected subject to data availability for analysis[1].
	Duplicate handling	Devices with duplicate IMEI receive service initially. Duplicates are identified during analysis once new data dumps are received.

6.1.2 Restrictive mode

In restrictive mode, EIRs block all devices from the network unless they are explicitly allowed.

A restrictive system typically uses triplets (IMEI/IMSI/MSISDN) or IMEI/IMSI pairs for all networks in a country.

In a restrictive system, the IMEI number of the device is compared to the permitted-list before it is allowed to access the network. The device is allowed only if it is in the permitted-list. In certain implementations, the device is allowed restricted access for device registration purposes only by maintaining a tracked-list. The operators' EIRs are provisioned with permitted, and tracked-list as required, or connect to the central database (CEIR) for real-time synchronization.

The permitted-list contains the full IMEI numbers provided by the local manufacturers or Customs, received from commercial importers, distributors, original equipment manufacturers (OEMs) and individual as part of the device registration process. An operator claims a permitted IMEI by pairing it to an IMSI and notifying the CEIR. Countries may require users to provide information to tie IMEI-to-subscriber pairing performing an IMEI-IMSI pairing process. This verification could be done either in advance or as part of the IMEI-IMSI pairing as described in Figure 3.

Restrictive systems generally maintain the following information in their permitted-list:

- All IMEIs of legally imported and locally manufactured devices.
- All IMEI-IMSI or IMEI-MSISDN pairs (paired IMEI allowed to register on the mobile network only with IMSI or MSISDN with which it has a pair).
- All existing IMEIs on the country mobile networks before restrictions started (list of IMEIs that have been granted amnesty).

A blocked-list can also be maintained in the restrictive system and updated regularly by the authorized entity.

Table 2 describes restrictive mode system impact.

[1] Recommendation ITU-T Q.5052 "Addressing mobile devices with duplicate unique identifiers".

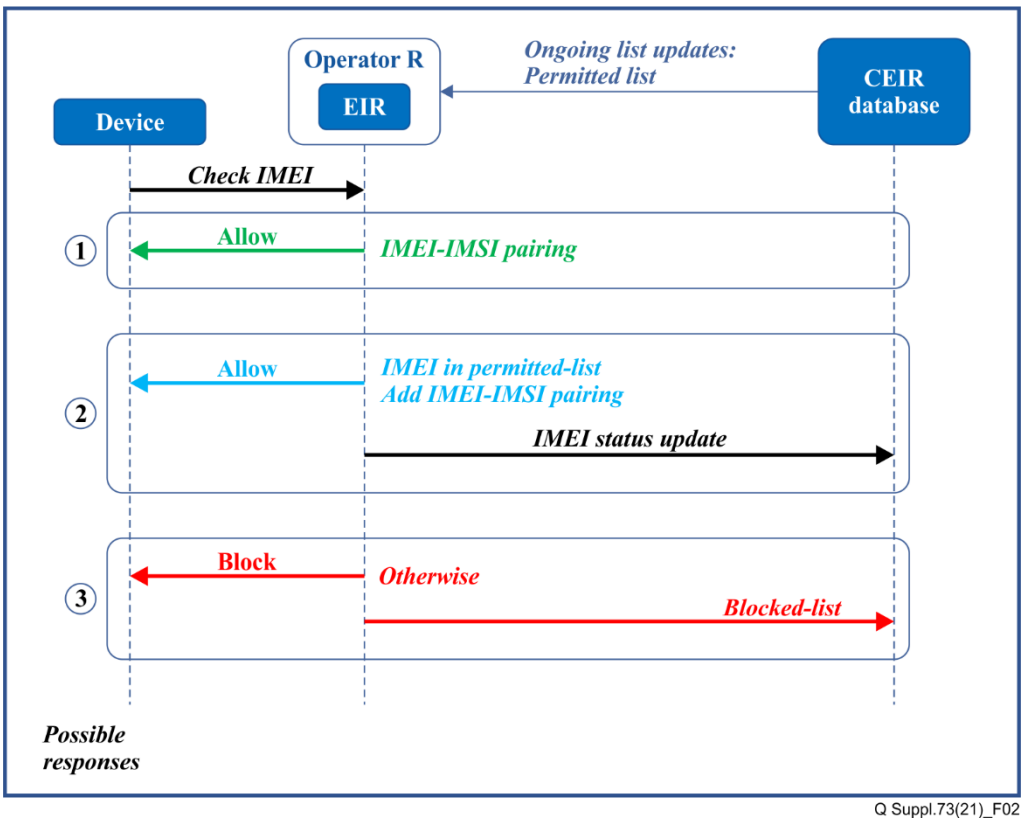

Figure 3 – Restrictive mode data synchronization

Table 2 – Restrictive mode system impact

Impact	Consideration	Restrictive mode (IMEI-IMSI / MSISDN)
Data	**Data requirements**	Access to the list of IMEIs registered (permitted-list) to form IMEI/IMSI pairing or triplets (IMEI/IMSI/MSISDN).
	Data processing	Online (real-time) processing to allow or deny call access.
	Processing accuracy	Susceptible to allowing fraudulent devices if a counterfeit device programmed with a permitted IMEI is paired with an IMSI before a genuine device thus rejecting genuine device access to the network.
	Device technology anomaly detection	Inability to detect technology mismatch in fraudulent devices programmed with GSMA allocated unique IMEIs. Offline processing is required in order to address this issue.
EIR	**Capacity (storage, processing)**	Larger processing capacity and storage requirements to cater to all allowed IMEIs or all allowed bindings of IMEIs in the entire country. impacting hardware and software requirements.

Table 2 – Restrictive mode system impact

Impact	Consideration	Restrictive mode (IMEI-IMSI / MSISDN)
	EIR-CEIR integration	No standardized EIR-CEIR interface available. Requires integration and interoperability testing with each vendor's EIR may result in additional cost, time, and resources.
Customer engagement	**Device verification before purchase**	Device compliance could be verified against the permitted-list during call setup (CEIR registration list); however, a fraudulent device could be mistaken for a compliant device resulting in a false positive.
	IMEI-IMSI pairing	IMEI-IMSI pairing burdens all subscribers requiring them to manage the pairing/unpairing process when changing SIMs or selling/purchasing an existing device.
	Registration	Devices do not get access to the network until registered in the CEIR's permitted-list, however, new devices can be allowed network access only for registration purposes.
	Notification	Notifications are generally not required as inability to access the network implicitly indicates the need for registration but in certain implementations customers could be notified upon detection of unregistered devices.
Non-compliance	**Audit**	No audit mechanism available for the authorities if operators allow non-permitted devices on their networks or add additional IMEIs in their local EIR's permitted-list.
Duplicate IMEI management	**Detection**	Duplicate IMEIs will not work on the same network; Some *Restrictive* implementation may not detect cross-network duplication
	Duplicate handling	Duplicates are denied service immediately; however, a genuine device could be blocked if a device with duplicated (non-compliant/illegal) IMEI is paired first.

6.1.2.1 Synchronization mode

In this mode, the CEIR database and the MNOs' local EIR databases are synchronized. The CEIR manages and distributes list updates to the operators so that MNOs' EIRs can directly respond to IMEI check on their respective networks using the IMEI information in their local databases. Each MNO manages its own pairing list and sends IMEI status updates to the CEIR when performing pairing and unpairing procedures. The CEIR performs IMEI association and/or disassociation with the respective MNOs and sends IMEI status updates to all connected MNOs.

This mode requires the same capacity capabilities of the MNOs EIRs as the CEIR, which could be potentially large depending on the database size in the country. The processing burden is distributed over the number of MNOs in the country as their local EIRs are responsible for querying the status of the device and pairing/un-pairing processing.

6.1.2.2 Authorization mode

In the authorization mode, the CEIR acts as the local EIR connected to each mobile network. All IMEI checks, including for new and unpaired IMEIs, are performed by querying the information in the CEIR. The CEIR maintains a local list of IMEIs or IMEI-IMSI pairs or triplets (MSISDN, IMSI, IMEIs). Availability of triplets data at the CEIR can be processed offline to aid in cross-network duplicate detection, SIM/IMSI change and mobile network operator (MNP).

As the CEIR is responsible to process device status, pairing and un-pairing requests from all MNOs, there is a higher degree of dependency and processing requirement in addition to ensuring it meets all capacity demands. Additionally, a single CEIR could be the single point of failure unless redundancy is supported.

6.1.2.3 Hybrid mode

In the hybrid mode, the CEIR provides centralized, real-time responses to IMEI checks from the MNOs. The MNOs EIRs query the CEIR for IMEIs that do not have any associated pairing on the network. Each MNO manages its own pairing list and sends IMEI status updates to the CEIR when performing pairing and unpairing procedures. The CEIR performs IMEI association and/or disassociation with the respective MNOs and sends IMEI status updates to all connected MNOs.

This mode alleviates the need for large capacity and processing capability requirements at the MNOs EIRs as they only need to manage just the pairing information for their own network and the larger IMEI database is managed by the CEIR.

6.1.3 Roaming in permissive and restrictive modes

In some countries, the mobile networks generally do not perform IMEI checks (CHECK_IMEI) for inbound roamers thus allowing them to establish calls regardless of the status of the IMEI. In either mode (permissive or restrictive), roamers are not affected in any way.

If a country regulator decides to enforce a policy mandate for CHECK_IMEI procedures for inbound roamers, the request is forwarded to the roamer's home network and the device is managed according to the response.

6.1.4 Mobile number portability (MNP) handling in permissive and restrictive modes

In the case of MNP, the donor (current MNO) unpairs the IMEI and sends a disassociation request to the CEIR. The recipient (new MNO) pairs the IMEI after receiving the IMEI availability status from the CEIR and sends the association request to the CEIR. The CEIR associates the IMEI with the new network and sends the status update to all connected MNOs.

7 Considerations for system deployment

When deploying a technical solution, there are many aspects affecting stakeholders especially the users and operators that must be well understood and factored into a permissive versus a restrictive system decision. These include customer considerations, regulatory considerations, and technical considerations that are discussed in clauses 7.1 to 7.3.

7.1 Customer considerations

Customer interaction and engagement with the system should be one of the key criteria that the regulators and the governments must consider as mobile users are the largest group of stakeholders affected by the choice of system implementation.

7.1.1 Device status verification

In a permissive system implementation, the status of a device (registered, lost/stolen, and known duplicate, etc.) may be verified by inquiring the system through mechanisms such as an app, web, and SMS when available.

In a restrictive system, the user may attempt to access the network with their subscriber identity module (SIM). IMEIs that are not permitted will not be able to access the network with a new SIM.

7.1.2 Duplication before purchase

In a permissive system, if a duplicated IMEI is already being used in country and has been identified by the system, it would already be blocked and not be able to access the network.

In a restrictive system, if another device clones an IMEI and accesses the network before the legitimate device, it would be paired to another IMSI and the genuine device with that IMEI will not be able to access the network with a new IMSI.

7.1.3 Duplication after purchase

In a permissive system, while device verification can provide current status at the time of device purchase, the IMEI could later be subjected to duplication. If this happens, the system can identify duplication and the customer can be notified to contact an authorized entity and be given a grace period during which time the device will continue to work. The authorized entity would provide exception pairing(s) for the legitimate device and all other uses of the IMEI would be blocked.

In a restrictive system, once paired, a legitimate customer should not be subject to having their IMEI duplicated.

7.1.4 SIM swapping

In a permissive system, IMEI-IMSI pairing is usually not required and the users can swap their SIM cards as usual under normal circumstances.

In scenarios where pairing is required by the administration, the call is still allowed to establish. The system detects a new pair with the same IMEI by performing offline analysis process and the user is notified to register the new pair (IMEI-IMSI). If an IMEI has been duplicated and the customer has received an exception pairing, they will need to perform a pairing change procedure when swapping SIM cards.

In a restrictive system, since all IMEIs are paired to an IMSI, all customers must always perform a pairing change procedure when swapping SIM cards. Similarly, if customer purchases a device that was previously used with another SIM, they must ensure that it has been unpaired before it can be used with another SIM.

7.1.5 Device registration

Some countries use a device registration database containing the legal imported/acquired IMEI paired with the identification document of the owner, in a way to identify those devices that have accomplished a legal process of importation or acquisition locally or abroad; other countries use a device registration database containing the legal imported/acquired IMEIs without requiring the identification of the user/owner. This serves as a reference to MNOs in order to tackle irregular IMEIs, in which those that have not been legally imported/acquired need to be notified to the user of handset to be registered in the said database. Otherwise it will be blocked.

In a permissive system, while the device verification system would identify that an IMEI is unregistered, the system will still allow that device to be temporarily used. Once detected, the customer would be notified to register their device and given a grace period for the devices to work. If the device is not registered during the grace period, it would be blocked.

In a restrictive system, non-registered IMEIs would not be permitted and not be able to access the network. A customer must register their device before it can be used.

7.2 Technical considerations

7.2.1 EIR impact

In a permissive system, the EIR stores blocked IMEIs and any paired IMEI-IMSI exceptions. Both lists represent a small subset of devices on the networks and in the market, resulting in modest EIR processing and storage capacity requirements.

Growth of these lists should be modest and continue to decrease over time as there is little financial incentive to introduce bad devices knowing that they will be blocked.

In a restrictive system, the EIR stores all permitted IMEIs available to be paired and all IMEI-IMSI pairs that can access the network. Representing all available devices and active subscriptions, these lists result in large EIR processing and storage capacity requirements.

Growth of these lists over time will continue unabated as new devices are registered in the market and used by subscribers.

7.3 Regulatory considerations

7.3.1 Data privacy

In a permissive system, the operators provide periodic IMEI-IMSI-MSISDN data dumps to support offline analysis. Blocked-list and exceptions list updates are shared with the operators by the CEIR.

In a restrictive system, the operators report triplets (IMEI-IMSI-MSISDN) or IMEI-IMSI pairs to CEIR when they are created. Permitted-list updates are shared with the operators by the CEIR.

7.3.2 Blocking

This clause highlights how the two systems, a permissive system, and a restrictive system, manage device blocking based on identified status of the device.

7.3.2.1 Device blocking in a permissive system

7.3.2.1.1 Blocked devices

All blocked IMEIs are blocked unless they have a corresponding exception IMEI-IMSI pairing.

7.3.2.1.2 Unregistered devices

Customers are notified and provided a grace period to register devices.

7.3.2.1.3 Duplication

Non-blocked IMEIs are subject to duplication. If affected, customers are notified after detection via data analysis and can receive exception pairings before the IMEI is blocked.

7.3.2.2 Device blocking in a restrictive system

7.3.2.2.1 Immediate blocking

All non-paired, non-permitted IMEIs are blocked.

7.3.2.2.2 Unregistered devices

Customers are immediately blocked from using devices not yet registered.

7.3.2.2.3 Duplication

Permitted IMEIs are subject to being paired with an illegitimate device. Once on the pairing list, an IMEI is not subject to duplication.

7.3.3 Oversight

In a permissive system, violations can be detected if the devices on the blocked-list are not being blocked by the operators and blocked-list violations report can be generated.

In a restrictive system, there is no clear audit mechanism available for the authorities if operators allow non-permitted devices on their networks or add additional IMEIs to the permitted-list in their local EIR.

8 Conclusion

In conclusion, both systems have their own merits and handle some aspects of the overall system implementation better than the other.

A country regulator/government looking to deploy a system should give due consideration to all aspects described in this document and should decide on the key reasons that merit selection of one type of system over the other.

Appendix I

DIRBS open-source platform

Device identification, registration and blocking system (DIRBS) is a server-based software platform intended to address counterfeit, illegal and stolen mobile devices in a country [b-DIRBS]. The DIRBS software platform is available as open source to assist governments, regulators, and others in their efforts to combat the improper use of counterfeit, illegal and stolen devices on mobile networks.

The DIRBS open-source platform supports both system configurations (permissive and restrictive) and can be configured, customized, and deployed as required. The platform is consistent with the International Telecommunication Union's ITU-T Q.5050 series.

Bibliography

[b-3GPP TS 22.016] 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI)* (Release 16).

[b-3GPP TS 29.060] 3rd Generation Partnership Project; *Technical Specifications: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface*.

[b-EICTA Doc: 04cc100] GSMA Doc Ref: *Security Principles Related to Handset Theft 3.0.0*.

[b-Tekelec EAGLE® 5] Feature Manual – *Equipment Identity Register*.

[b-DIRBS] DIRBS Open-Source Platform. www.github.com/dirbs

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