

ETSI TS 143 020 V15.3.0 (2024-04)



Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions (3GPP TS 43.020 version 15.3.0 Release 15)

Document Preview

[ETSI TS 143 020 V15.3.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/f788caaf-1c81-49b4-a6b9-d1f1a6bddef5/etsi-ts-143-020-v15-3-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/f788caaf-1c81-49b4-a6b9-d1f1a6bddef5/etsi-ts-143-020-v15-3-0-2024-04>



ReferenceRTS/TSGS-0343020v30

KeywordsGSM

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<https://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables. (2024-04)

The cross reference between 3GPP and ETSI identities can be found under <https://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	8
0 Scope	9
0.1 References	9
0.2 Abbreviations	10
1 General	10
2 Subscriber identity confidentiality	11
2.1 Generality	11
2.2 Identifying method	11
2.3 Procedures	12
2.3.1 Location updating in the same MSC area	12
2.3.2 Location updating in a new MSCs area, within the same VLR area.....	12
2.3.3 Location updating in a new VLR; old VLR reachable	13
2.3.4 Location Updating in a new VLR; old VLR not reachable.....	14
2.3.5 Reallocation of a new TMSI	15
2.3.6 Local TMSI unknown	16
2.3.7 Location updating in a new VLR in case of a loss of information.....	17
2.3.8 Unsuccessful TMSI allocation.....	17
2.3.9 Combined location area updating with the routing area updating.....	18
3 Subscriber identity authentication	19
3.1 Generality	19
3.2 The authentication procedure	19
3.3 Subscriber Authentication Key management	20
3.3.1 General authentication procedure	20
3.3.2 Authentication at location updating in a new VLR, using TMSI.....	21
3.3.3 Authentication at location updating in a new VLR, using IMSI.....	22
3.3.4 Authentication at location updating in a new VLR, using TMSI, TMSI unknown in "old" VLR	23
3.3.5 Authentication at location updating in a new VLR, using TMSI, old VLR not reachable	24
3.3.6 Authentication with IMSI if authentication with TMSI fails	24
3.3.7 Re-use of security related information in failure situations	24
4 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections	25
4.1 Generality	25
4.2 The ciphering method.....	25
4.3 Key setting.....	26
4.4 Ciphering key sequence number	27
4.5 Starting of the ciphering and deciphering processes	27
4.6 Synchronization.....	27
4.7 Handover	27
4.8 Negotiation of A5 algorithm	28
4.9 Support of A5 Algorithms in MS	28
4.10 Support of A5 Algorithms in the BSS	29
5 Synthetic summary	30
Annex A (informative): Security issues related to signalling schemes and key management	31
A.1 Introduction	31
A.2 Short description of the schemes.....	31
A.3 List of abbreviations.....	32

Annex B (informative):	Security information to be stored in the entities of the GSM system.....	46
B.1	Introduction	46
B.2	Entities and security information	46
B.2.1	Home Location Register (HLR)	46
B.2.2	Visitor Location Register (VLR).....	46
B.2.3	Mobile services Switching Centre (MSC)/Base Station System (BSS)	46
B.2.4	Mobile Station (MS).....	47
B.2.5	Authentication Centre (AuC)	47
Annex C (normative):	External specifications of security related algorithms.....	48
C.0	Scope	48
C.1	Specifications for Algorithm A5	48
C.1.1	Purpose	48
C.1.2	Implementation indications	48
C.1.3	External specifications of Algorithm A5	50
C.1.3.1	A5 algorithms with 64-bit keys.....	50
C.1.3.2	A5 algorithms with 128-bit keys.....	50
C.1.4	Internal specification of Algorithm A5	50
C.1.5	Definition of NPBB for different modulations.....	50
C.2	Algorithm A3	50
C.2.1	Purpose	50
C.2.2	Implementation and operational requirements	51
C.3	Algorithm A8	51
C.3.1	Purpose	51
C.3.2	Implementation and operational requirements	51
Annex D (normative):	Security related network functions for General Packet Radio Service	52
D.1	General	52
D.2	Subscriber identity confidentiality	52
D.2.1	Generality	52
D.2.2	Identifying method	53
D.2.3	Procedures	53
D.2.3.1	Routing area updating in the same SGSN area	53
D.2.3.2	Routing area updating in a new SGSN; old SGSN reachable.....	54
D.2.3.3	Routing area updating in a new SGSN; old SGSN not reachable.....	55
D.2.3.4	Reallocation of a TLLI	55
D.2.3.5	Local TLLI unknown.....	56
D.2.3.6	Routing area updating in a new SGSN in case of a loss of information	57
D.2.3.7	Unsuccessful TLLI allocation.....	57
D.3	Subscriber identity authentication	58
D.3.1	Generality	58
D.3.2	The authentication procedure	58
D.3.3	Subscriber Authentication Key management	58
D.3.3.1	General authentication procedure	58
D.3.3.2	Authentication at routing area updating in a new SGSN, using TLLI	59
D.3.3.3	Authentication at routing area updating in a new SGSN, using IMSI	60
D.3.3.4	Authentication at routing area updating in a new SGSN, using TLLI, TLLI unknown in 'old' SGSN	61
D.3.3.5	Authentication at routing area updating in a new SGSN, using TLLI, old SGSN not reachable.....	62
D.3.3.6	Authentication with IMSI if authentication with TLLI fails.....	62
D.3.3.7	Re-use of security related information in failure situations	62
D.4	Confidentiality of user information and signalling between MS and SGSN	63
D.4.1	Generality	63
D.4.2	The ciphering method.....	63
D.4.3	Key setting.....	63
D.4.4	Ciphering key sequence number	64
D.4.5	Starting of the ciphering and deciphering processes	64

D.4.6	Synchronisation	65
D.4.7	Inter SGSN routing area update	65
D.4.8	Negotiation of GPRS-A5 algorithm	66
D.4.9	Support of GPRS-A5 Algorithms in MS	66
D.5	Synthetic summary	67
D.6	Security of the GPRS backbone	67

Annex E (normative): GSM Cordless Telephony System (CTS), (Phase 1); Security related network functions; Stage 2.....68

E.1	Introduction	68
E.1.1	Scope	68
E.1.2	References	68
E.1.3	Definitions and Abbreviations	68
E.1.3.1	Definitions	68
E.1.3.2	Abbreviations	69
E.2	General	70
E.3	CTS local security system	71
E.3.1	Mobile Subscriber identity confidentiality	71
E.3.1.1	Identifying method	71
E.3.1.2	Procedures	71
E.3.1.2.1	CTSMSI assignment	71
E.3.1.2.2	CTSMSI update	72
E.3.1.2.3	CTS local identification	72
E.3.2	Identity authentication	72
E.3.2.1	The mutual authentication procedure	72
E.3.2.1.1	Authentication failure	73
E.3.2.2	Authentication Key management	73
E.3.3	Confidentiality of user information and signalling between CTS-MS and CTS-FP	74
E.3.3.1	The ciphering method	74
E.3.3.2	Key setting	74
E.3.3.3	Starting of the ciphering and deciphering processes	75
E.3.3.4	Synchronisation	76
E.3.4	Structured procedures with CTS local security relevance	76
E.3.4.1	Local Part of the Enrolment of a CTS-MS onto a CTS-FP	76
E.3.4.1.1	Local part of the enrolment procedure	76
E.3.4.2	General Access procedure	79
E.3.4.2.1	Attachment	79
E.3.4.2.2	CTS local security data update	80
E.3.4.3	De-enrolment of a CTS-MS	80
E.3.4.3.1	De-enrolment initiated by the CTS-FP	80
E.3.4.3.2	De-enrolment initiated by a CTS-MS	80
E.4	CTS supervising security system	81
E.4.1	Supervision data and supervision data protection	81
E.4.1.1	Structure of supervision data	81
E.4.1.2	Supervision data protection	81
E.4.1.3	Key management	82
E.4.2	CTS subscriber identity	82
E.4.3	Identity authentication with the CTS operator and the PLMN	82
E.4.3.1	Authentication of the CTS-FP	82
E.4.3.2	Authentication of the CTS-MS	83
E.4.4	Secure operation control	84
E.4.4.1	GSM layer 3 signalling	84
E.4.4.2	CTS application signalling via the Fixed Network	84
E.4.4.3	CTS operation control procedures	85
E.4.4.3.1	Initialisation of a CTS-FP	85
E.4.4.3.2	De-initialisation of a CTS-FP	85
E.4.4.3.3	Enrolment	86
E.4.4.3.3.1	Enrolment conducted via the CTS fixed network interface	86

E.4.4.3.4	Supervising security in the CTS-FP/CTS-SN access procedure	87
E.4.4.3.4.1	Update of operation data.....	87
E.4.5	Equipment checking	88
E.4.6	FP-SIM card checking.....	88
E.5	Other CTS security features	89
E.5.1	Secure storage of sensitive data and software in the CTS-MS	89
E.5.1.1	Inside CTS-ME	89
E.5.2	Secure storage of sensitive data and software in CTS-FP	89
E.5.3	CTS-FP reprogramming protection	89
E.6	FP Integrity.....	89
E.6.1	Threats.....	90
E.6.1.1	Changing of FP software	90
E.6.1.2	Changing of IFPEI.....	91
E.6.1.3	Changing of IFPSI and operator and subscription related keys (K_{iFP} , K_{OP})	91
E.6.1.4	Changing of timers and timer limits	91
E.6.1.5	Changing of radio usage parameters.....	91
E.6.2	Protection and storage mechanisms.....	91
E.6.2.1	Static or semi static values.....	91
E.6.2.2	Timers.....	91
E.6.2.3	Physical protection.....	91
E.7	Type approval issues	91
E.8	Security information to be stored in the entities of the CTS	92
E.8.1	Entities and security information.....	92
E.8.1.1	CTS-HLR.....	92
E.8.1.2	CTS-SN	92
E.8.1.3	CTS-AuC.....	92
E.8.1.4	CTS Fixed Part Equipment (CTS-FPE).....	93
E.8.1.5	Fixed Part SIM card (FP-SIM)	93
E.8.1.6	CTS Mobile Equipment (CTS-ME).....	93
E.8.1.7	Mobile Station SIM card (MS-SIM).....	93
E.9	External specification of security related algorithms	94
E.9.1	Algorithm B1.....	94
E.9.1.1	Purpose	94
E.9.1.2	Implementation and operational requirements.....	95
E.9.2	Algorithm B2.....	95
E.9.2.1	Purpose	95
E.9.2.2	Implementation and operational requirements.....	95
E.9.3	Algorithms B3 and B4.....	96
E.9.3.1	Purpose	96
E.9.3.2	Implementation and operational requirements.....	96
E.9.4	Algorithms B5 and B6.....	96
E.9.4.1	Purpose	96
E.9.4.2	Implementation and operational requirements.....	96
E.10	Coding of the FPAC and CTS-PIN	97
E.11	(informative annex): Guidelines for generation of random numbers.....	97
Annex F (normative):	Ciphering of Voice Group Call Service (VGCS) and Voice Broadcast Service (VBS).....	98
F.1	Introduction	98
F.1.1	Scope	98
F.1.2	References	98
F.1.3	Definitions and Abbreviations.....	99
F.1.3.1	Definitions	99
F.1.3.2	Abbreviations.....	99
F.2	Security Requirements	99

F.3	Storage of the Master Group Keys and overview of flows	100
F.3.1	Distribution of ciphering data during establishment of a voice/broadcast group call.....	100
F.3.2	Signalling information required for the voice group call uplink access in the anchor MSC (normal case, subsequent talker on dedicated channel)	103
F.3.3	Signalling information required to transfer the originator or subsequent talker from a dedicated channel to a group call channel.....	105
F.4	Key derivation	105
F.4.1	Key derivation within the USIM / GCR	106
F.4.2	Key derivation within the ME/BSS	107
F.4.3	Encryption algorithm selection.....	108
F.4.4	Algorithm requirements	108
F.4.4.1	A8_V	108
F.4.4.2	KMF.....	108
F.5	Encryption of voice group calls.....	109
F.6	Specification of the Key Modification Function (KMF).....	109
Annex G (informative): Generation of VSTK_RAND		110
Annex H (normative): Access security related functions for enhanced General Packet Radio Service (GPRS) in relation to Cellular Internet of Things (CIoT)		111
H.1	Introduction	111
H.1.1	General	111
H.1.2	Considerations on bidding down attacks	111
H.2	Authentication and key agreement	111
H.3	Ciphering and integrity mode negotiation.....	111
H.4	Protection of GMM messages	117
H.5	Algorithms for ciphering and integrity protection.....	117
H.5.0	General	117
H.5.1	Null ciphering algorithm	118
H.5.2	Ciphering algorithm	118
H.5.2.1	Inputs and outputs.....	118
H.5.2.1.1	General	118
H.5.2.1.2	CONSTANT-F.....	119
H.5.2.2	GEA5	119
H.5.3	Integrity algorithm.....	119
H.5.3.1	Inputs and outputs.....	119
H.5.3.1.1	General	119
H.5.3.1.2	INPUT-I.....	119
H.5.3.1.3	CONSTANT-F.....	120
H.5.3.2	GIA4	120
H.5.3.3	GIA5	120
H.6	Derivation of Kc128 and Ki128	120
H.7	Integrity protection of user plane	121
H.8	Definition of MAC-GMM in GMM Authentication and Ciphering Request and GMM Authentication and Ciphering Response messages	121
H.8.1	Inputs and outputs	121
H.9	Protected negotiation of IOV values	122
H.9.1	Protected IOV container	122
H.9.2	LLC XID procedure with protected IOV container.....	123
Annex I (informative): Change history		124
History		125

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 143 020 V15.3.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/f788caaf-1c81-49b4-a6b9-d1f1a6bddef5/etsi-ts-143-020-v15-3-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/f788caaf-1c81-49b4-a6b9-d1f1a6bddef5/etsi-ts-143-020-v15-3-0-2024-04>

0 Scope

This Technical Specification specifies the network functions needed to provide the security related service and functions specified in 3GPP TS 42.009.

This specification does not address the cryptological algorithms that are needed to provide different security related features. This topic is addressed in annex C. Wherever a cryptological algorithm or mechanism is needed, this is signalled with a reference to annex C. The references refers only to functionalities, and some algorithms may be identical or use common hardware.

0.1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 41.061: "GPRS ciphering algorithm requirements".
- [3] Void
- [4] 3GPP TS 42.009: " Security aspects".
- [5] 3GPP TS 42.017: " Subscriber Identity Modules (SIM) Functional characteristics".
- [6] 3GPP TS 42.056: " GSM Cordless Telephone System (CTS) Phase 1; Service Description; Stage 1".
- [7] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service description; Stage 1".
- [8] 3GPP TS 23.003: "Numbering, addressing and identification".
- [9] GSM 03.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS), Phase 1; CTS Architecture Description; Stage 2".
- [10] 3GPP TS 23.060: " Service description; Stage 2".
- [11] 3GPP TS 24.008: "Mobile radio interface layer 3 specification".
- [12] Void
- [13] 3GPP TS 45.001: "Physical layer on the radio path; General description".
- [14] 3GPP TS 45.002: "Multiplexing and multiple access on the radio path".
- [15] 3GPP TS 45.003: "Channel coding".
- [16] 3GPP TS 29.002: " Mobile Application Part (MAP) specification".
- [17] 3GPP TS 51.011: " Specification of the Subscriber Identity Module- Mobile Equipment (SIM-ME) interface".
- [18] 3GPP TS 33.102: "Technical Specification Group Services and System Aspects; 3G Security; Security architecture ".

- [19] 3GPP TS 24.301: "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".
- [20] 3GPP TS 44.064: "Technical Specification Group Core Network and Terminals; Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) layer specification".
- [21] 3GPP TS 55.226: " Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/4 encryption algorithms for GSM and ECSD, and the GEA4 encryption algorithm for GPRS".
- [22] 3GPP TS 33.220: " Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".
- [23] Void
- [24] 3GPP TS 33.102: " 3G security; Security architecture".
- [25] 3GPP TS 55.251: "Specification of the GEA5 encryption and GIA5 integrity algorithms for GPRS; GEA5 and GIA5 algorithm specification".
- [26] 3GPP TS 55.241: "Specification of the GIA4 integrity algorithm for GPRS; GIA4 specification".

0.2 Abbreviations

Abbreviations used in this specification are listed in 3GPP TS 21.905.

Specific abbreviations used in annex A are listed in clause A.3.

Specific CTS related abbreviations used in annex E are listed in clause E.1.3.

Specific VCGS and VBS related abbreviations used in annex F are listed in clause F.1.3.

Throughout this specification, the abbreviation K_{C128} is used to indicate a 128-bit ciphering key as derived by UMTS AKA [18]. The abbreviation K_{C128} is only used where it matters that the ciphering key is 128 bits long; the abbreviation K_c is used in all other places.

1 General

The different security related services and functions that are listed in 3GPP TS 42.009 are grouped as follows:

- Subscriber identity confidentiality;
- Subscriber identity authentication;
- Signalling information element and connectionless user data confidentiality and data confidentiality for physical connections (ciphering).

It shall be possible to introduce new authentication and ciphering algorithms during the systems lifetime. The fixed network may support more than one authentication and ciphering algorithm.

The security procedures include mechanisms to enable recovery in event of signalling failures. These recovery procedures are designed to minimize the risk of a breach in the security of the system.

General on figures in this specification:

- In the figures below, signalling exchanges are referred to by functional names. The exact messages and message types are specified in 3GPP TS 24.008 and 3GPP TS 29.002.
- No assumptions are made for function splitting between MSC (Mobile Switching Centre), VLR (Visitor Location Register) and BSS (Base Station System). Signalling is described directly between MS and the local network (i.e. BSS, MSC and VLR denoted in the figures by BSS/MSC/VLR). The splitting in annex A is given only for illustrative purposes.

- Addressing fields are not given; all information relates to the signalling layer. The TMSI allows addressing schemes without IMSI, but the actual implementation is specified in the GSM 04-series.
- The term HPLMN in the figures below is used as a general term which should be understood as HLR (Home Location Register) or AuC (Authentication Centre).
- What is put in a box is not part of the described procedure but it is relevant to the understanding of the figure.

2 Subscriber identity confidentiality

2.1 Generality

The purpose of this function is to avoid the possibility for an intruder to identify which subscriber is using a given resource on the radio path (e.g. TCH (Traffic Channel) or signalling resources) by listening to the signalling exchanges on the radio path. This allows both a high level of confidentiality for user data and signalling and protection against the tracing of a user's location.

The provision of this function implies that the IMSI (International Mobile Subscriber Identity), or any information allowing a listener to derive the IMSI easily, should not normally be transmitted in clear text in any signalling message on the radio path.

Consequently, to obtain the required level of protection, it is necessary that:

- a protected identifying method is normally used instead of the IMSI on the radio path; and
- the IMSI is not normally used as addressing means on the radio path (see 3GPP TS 42.009);
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following subclause. The ciphering of communication over the radio path is specified in clause 4.

2.2 Identifying method

The means used to identify a mobile subscriber on the radio path consists of a TMSI (Temporary Mobile Subscriber Identity). This TMSI is a local number, having a meaning only in a given location area; the TMSI must be accompanied by the LAI (Location Area Identification) to avoid ambiguities. The maximum length and guidance for defining the format of a TMSI are specified in 3GPP TS 23.003.

The network (e.g. a VLR) manages suitable data bases to keep the relation between TMSIs and IMSIs. When a TMSI is received with an LAI that does not correspond to the current VLR, the IMSI of the MS must be requested from the VLR in charge of the indicated location area if its address is known; otherwise the IMSI is requested from the MS.

A new TMSI must be allocated at least in each location updating procedure. The allocation of a new TMSI corresponds implicitly for the MS to the de-allocation of the previous one. In the fixed part of the network, the cancellation of the record for an MS in a VLR implies the de-allocation of the corresponding TMSI.

To cope with some malfunctioning, e.g. arising from a software failure, the fixed part of the network can require the identification of the MS in clear. This procedure is a breach in the provision of the service, and should be used only when necessary.

When a new TMSI is allocated to an MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is the same as defined in clause 4.

The MS must store its current TMSI in a non volatile memory, together with the LAI, so that these data are not lost when the MS is switched off.

2.3 Procedures

This subclause presents the procedures, or elements of procedures, pertaining to the management of TMSIs.

2.3.1 Location updating in the same MSC area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on the same MSC. The part of this procedure relative to TMSI management is reduced to a TMSI re-allocation (from TMSIo with "o" for "old" to TMSIn with "n" for "new").

The MS sends TMSIo as an identifying field at the beginning of the location updating procedure.

The procedure is schematized in figure 2.1.

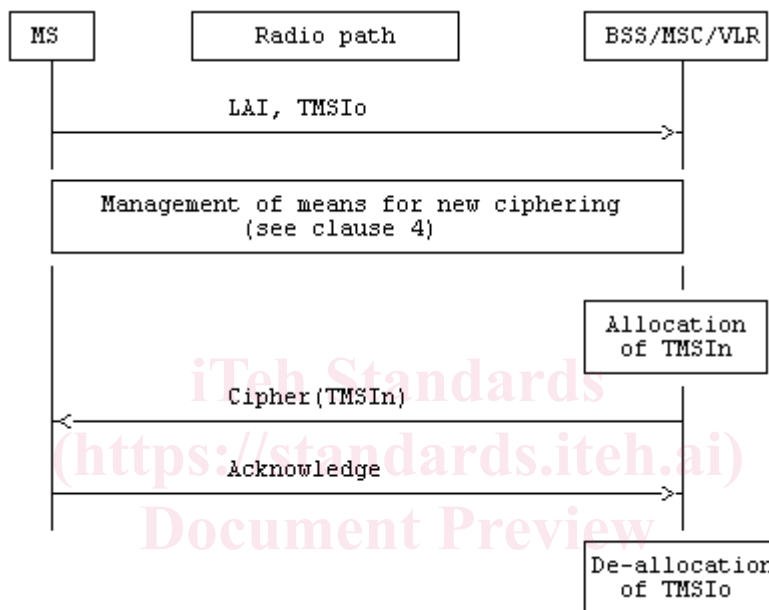


Figure 2.1: Location updating in the same MSC area

Signalling Functionalities:

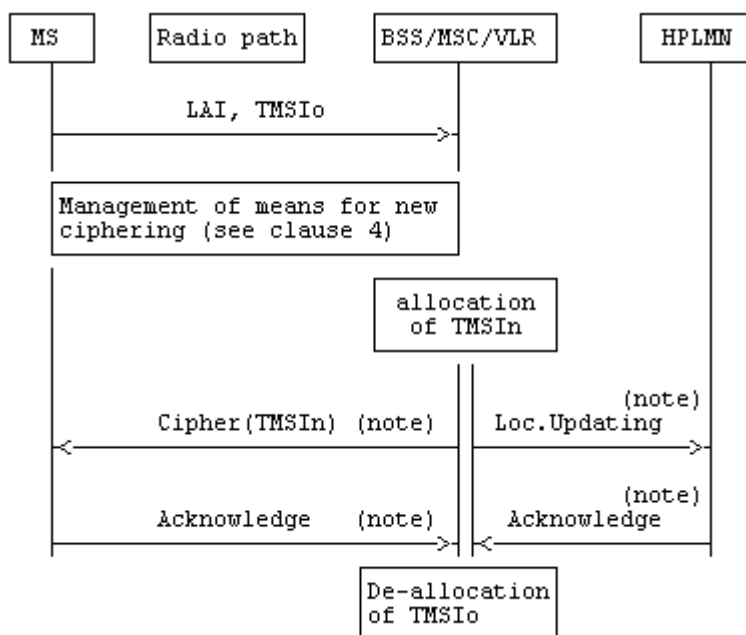
Management of means for new ciphering:

The MS and BSS/MSC/VLR agree on means for ciphering signalling information elements, in particular to transmit TMSIn.

2.3.2 Location updating in a new MSCs area, within the same VLR area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on different MSCs, but on the same VLR.

The procedure is schematized on figure 2.2.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.2: Location updating in a new MSCs area, within the same VLR area

Signalling functionalities:

Loc.Updating:

stands for Location Updating

The BSS/MSC/VLR indicates that the location of the MS must be updated.

2.3.3 Location updating in a new VLR; old VLR reachable

This procedure is part of the normal location updating procedure, using TMSI and LAI, when the original location area and the new location area depend on different VLRs.

The MS is still registered in VLR_o ("o" for old or original) and requests registration in VLR_n ("n" for new). LAI and TMSIo are sent by MS as identifying fields during the location updating procedure.

The procedure is schematized in figure 2.3.