

ETSI TS 143 020 V13.5.0 (2017-04)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Security related network functions
(3GPP TS 43.020 version 13.5.0 Release 13)**



Reference

RTS/TSGS-0343020vd50

Keywords

GSM,SECURITY

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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/ETSI/DeliverableStatus.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>

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.

© European Telecommunications Standards Institute 2017.

All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://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
Foreword.....	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	11
2.3.1 Location updating in the same MSC area	11
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	28
5 Synthetic summary	29
Annex A (informative): Security issues related to signalling schemes and key management	30
A.1 Introduction	30
A.2 Short description of the schemes.....	30
A.3 List of abbreviations.....	31

Annex B (informative):	Security information to be stored in the entities of the GSM system.....	45
B.1	Introduction	45
B.2	Entities and security information	45
B.2.1	Home Location Register (HLR)	45
B.2.2	Visitor Location Register (VLR).....	45
B.2.3	Mobile services Switching Centre (MSC)/Base Station System (BSS)	45
B.2.4	Mobile Station (MS).....	46
B.2.5	Authentication Centre (AuC)	46
Annex C (normative):	External specifications of security related algorithms.....	47
C.0	Scope	47
C.1	Specifications for Algorithm A5	47
C.1.1	Purpose	47
C.1.2	Implementation indications	47
C.1.3	External specifications of Algorithm A5	49
C.1.3.1	A5 algorithms with 64-bit keys.....	49
C.1.3.2	A5 algorithms with 128-bit keys.....	49
C.1.4	Internal specification of Algorithm A5	49
C.1.5	Definition of NPBB for different modulations.....	49
C.2	Algorithm A3	49
C.2.1	Purpose	49
C.2.2	Implementation and operational requirements	50
C.3	Algorithm A8	50
C.3.1	Purpose	50
C.3.2	Implementation and operational requirements	50
Annex D (normative):	Security related network functions for General Packet Radio Service	51
D.1	General	51
D.2	Subscriber identity confidentiality	51
D.2.1	Generality	51
D.2.2	Identifying method	52
D.2.3	Procedures	52
D.2.3.1	Routing area updating in the same SGSN area	52
D.2.3.2	Routing area updating in a new SGSN; old SGSN reachable.....	53
D.2.3.3	Routing area updating in a new SGSN; old SGSN not reachable.....	54
D.2.3.4	Reallocation of a TLLI	54
D.2.3.5	Local TLLI unknown.....	55
D.2.3.6	Routing area updating in a new SGSN in case of a loss of information	56
D.2.3.7	Unsuccessful TLLI allocation.....	56
D.3	Subscriber identity authentication	57
D.3.1	Generality	57
D.3.2	The authentication procedure	57
D.3.3	Subscriber Authentication Key management	57
D.3.3.1	General authentication procedure	57
D.3.3.2	Authentication at routing area updating in a new SGSN, using TLLI	58
D.3.3.3	Authentication at routing area updating in a new SGSN, using IMSI	59
D.3.3.4	Authentication at routing area updating in a new SGSN, using TLLI, TLLI unknown in 'old' SGSN	60
D.3.3.5	Authentication at routing area updating in a new SGSN, using TLLI, old SGSN not reachable.....	61
D.3.3.6	Authentication with IMSI if authentication with TLLI fails.....	61
D.3.3.7	Re-use of security related information in failure situations	61
D.4	Confidentiality of user information and signalling between MS and SGSN	62
D.4.1	Generality	62
D.4.2	The ciphering method.....	62
D.4.3	Key setting.....	62
D.4.4	Ciphering key sequence number	63
D.4.5	Starting of the ciphering and deciphering processes	63

D.4.6	Synchronisation	64
D.4.7	Inter SGSN routing area update	64
D.4.8	Negotiation of GPRS-A5 algorithm	64
D.4.9	Support of GPRS-A5 Algorithms in MS	65
D.5	Synthetic summary	66
D.6	Security of the GPRS backbone	66

Annex E (normative): GSM Cordless Telephony System (CTS), (Phase 1); Security related network functions; Stage 2.....67

E.1	Introduction	67
E.1.1	Scope	67
E.1.2	References	67
E.1.3	Definitions and Abbreviations	67
E.1.3.1	Definitions	67
E.1.3.2	Abbreviations	68
E.2	General	69
E.3	CTS local security system	70
E.3.1	Mobile Subscriber identity confidentiality	70
E.3.1.1	Identifying method	70
E.3.1.2	Procedures	70
E.3.1.2.1	CTSMSI assignment	70
E.3.1.2.2	CTSMSI update	71
E.3.1.2.3	CTS local identification	71
E.3.2	Identity authentication	71
E.3.2.1	The mutual authentication procedure	71
E.3.2.1.1	Authentication failure	72
E.3.2.2	Authentication Key management	72
E.3.3	Confidentiality of user information and signalling between CTS-MS and CTS-FP	73
E.3.3.1	The ciphering method	73
E.3.3.2	Key setting	73
E.3.3.3	Starting of the ciphering and deciphering processes	74
E.3.3.4	Synchronisation	75
E.3.4	Structured procedures with CTS local security relevance	75
E.3.4.1	Local Part of the Enrolment of a CTS-MS onto a CTS-FP	75
E.3.4.1.1	Local part of the enrolment procedure	75
E.3.4.2	General Access procedure	78
E.3.4.2.1	Attachment	78
E.3.4.2.2	CTS local security data update	79
E.3.4.3	De-enrolment of a CTS-MS	79
E.3.4.3.1	De-enrolment initiated by the CTS-FP	79
E.3.4.3.2	De-enrolment initiated by a CTS-MS	79
E.4	CTS supervising security system	80
E.4.1	Supervision data and supervision data protection	80
E.4.1.1	Structure of supervision data	80
E.4.1.2	Supervision data protection	80
E.4.1.3	Key management	81
E.4.2	CTS subscriber identity	81
E.4.3	Identity authentication with the CTS operator and the PLMN	81
E.4.3.1	Authentication of the CTS-FP	81
E.4.3.2	Authentication of the CTS-MS	82
E.4.4	Secure operation control	83
E.4.4.1	GSM layer 3 signalling	83
E.4.4.2	CTS application signalling via the Fixed Network	83
E.4.4.3	CTS operation control procedures	84
E.4.4.3.1	Initialisation of a CTS-FP	84
E.4.4.3.2	De-initialisation of a CTS-FP	84
E.4.4.3.3	Enrolment	85
E.4.4.3.3.1	Enrolment conducted via the CTS fixed network interface	85

E.4.4.3.4	Supervising security in the CTS-FP/CTS-SN access procedure	86
E.4.4.3.4.1	Update of operation data.....	86
E.4.5	Equipment checking	87
E.4.6	FP-SIM card checking.....	87
E.5	Other CTS security features	88
E.5.1	Secure storage of sensitive data and software in the CTS-MS	88
E.5.1.1	Inside CTS-ME.....	88
E.5.2	Secure storage of sensitive data and software in CTS-FP	88
E.5.3	CTS-FP reprogramming protection.....	88
E.6	FP Integrity.....	88
E.6.1	Threats.....	89
E.6.1.1	Changing of FP software	89
E.6.1.2	Changing of IFPEI.....	90
E.6.1.3	Changing of IFPSI and operator and subscription related keys (K_{iFP} , K_{OP})	90
E.6.1.4	Changing of timers and timer limits	90
E.6.1.5	Changing of radio usage parameters.....	90
E.6.2	Protection and storage mechanisms.....	90
E.6.2.1	Static or semi static values.....	90
E.6.2.2	Timers.....	90
E.6.2.3	Physical protection.....	90
E.7	Type approval issues	90
E.8	Security information to be stored in the entities of the CTS	91
E.8.1	Entities and security information.....	91
E.8.1.1	CTS-HLR.....	91
E.8.1.2	CTS-SN	91
E.8.1.3	CTS-AuC.....	91
E.8.1.4	CTS Fixed Part Equipment (CTS-FPE).....	92
E.8.1.5	Fixed Part SIM card (FP-SIM)	92
E.8.1.6	CTS Mobile Equipment (CTS-ME).....	92
E.8.1.7	Mobile Station SIM card (MS-SIM).....	92
E.9	External specification of security related algorithms	93
E.9.1	Algorithm B1.....	93
E.9.1.1	Purpose	93
E.9.1.2	Implementation and operational requirements.....	94
E.9.2	Algorithm B2.....	94
E.9.2.1	Purpose	94
E.9.2.2	Implementation and operational requirements.....	94
E.9.3	Algorithms B3 and B4.....	95
E.9.3.1	Purpose	95
E.9.3.2	Implementation and operational requirements.....	95
E.9.4	Algorithms B5 and B6.....	95
E.9.4.1	Purpose	95
E.9.4.2	Implementation and operational requirements.....	95
E.10	Coding of the FPAC and CTS-PIN	96
E.11	(informative annex): Guidelines for generation of random numbers.....	96
Annex F (normative):	Ciphering of Voice Group Call Service (VGCS) and Voice Broadcast Service (VBS).....	97
F.1	Introduction	97
F.1.1	Scope.....	97
F.1.2	References	97
F.1.3	Definitions and Abbreviations.....	98
F.1.3.1	Definitions	98
F.1.3.2	Abbreviations.....	98
F.2	Security Requirements	98

F.3	Storage of the Master Group Keys and overview of flows	99
F.3.1	Distribution of ciphering data during establishment of a voice/broadcast group call.....	99
F.3.2	Signalling information required for the voice group call uplink access in the anchor MSC (normal case, subsequent talker on dedicated channel)	102
F.3.3	Signalling information required to transfer the originator or subsequent talker from a dedicated channel to a group call channel.....	104
F.4	Key derivation	104
F.4.1	Key derivation within the USIM / GCR	105
F.4.2	Key derivation within the ME/BSS	106
F.4.3	Encryption algorithm selection.....	107
F.4.4	Algorithm requirements	107
F.4.4.1	A8_V	107
F.4.4.2	KMF.....	107
F.5	Encryption of voice group calls.....	108
F.6	Specification of the Key Modification Function (KMF).....	108
Annex G (informative): Generation of VSTK_RANDOM		109
Annex H (normative): Access security related functions for enhanced General Packet Radio Service (GPRS) in relation to Cellular Internet of Things (CIoT)		110
H.1	Introduction	110
H.1.1	General	110
H.1.2	Considerations on bidding down attacks	110
H.2	Authentication and key agreement	110
H.3	Ciphering and integrity mode negotiation.....	110
H.4	Protection of GMM messages	116
H.5	Algorithms for ciphering and integrity protection.....	116
H.5.0	General	116
H.5.1	Null ciphering algorithm	117
H.5.2	Ciphering algorithm	117
H.5.2.1	Inputs and outputs.....	117
H.5.2.1.1	General	117
H.5.2.1.2	CONSTANT-F.....	118
H.5.2.2	GEA5	118
H.5.3	Integrity algorithm.....	118
H.5.3.1	Inputs and outputs.....	118
H.5.3.1.1	General	118
H.5.3.1.2	INPUT-I.....	118
H.5.3.1.3	CONSTANT-F.....	119
H.5.3.2	GIA4	119
H.5.3.3	GIA5	119
H.6	Derivation of Kc128 and Ki128	119
H.7	Integrity protection of user plane	120
H.8	Definition of MAC-GMM in GMM Authentication and Ciphering Request and GMM Authentication and Ciphering Response messages	120
H.8.1	Inputs and outputs	120
H.9	Protected negotiation of IOV values	121
H.9.1	Protected IOV container	121
H.9.2	LLC XID procedure with protected IOV container.....	122
Annex I (informative): Change history		123
History		124

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.

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 ".