ETSI TS 143 020 V14.3.0 (2017-08)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions (3GPP TS 43.020 version 14.3.0 Release 14)

A GLOBAL INITIATIVE

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Reference

RTS/TSGS-0343020ve30

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/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/CommiteeSupportStaff.aspx

Copyright Notification

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 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 65
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 (Ki_{FP}, 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....92

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....93
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)....94
E.8.1.7 Mobile Station SIM card (MS-SIM)....94

E.9 External specification of security related algorithms....94
E.9.1 Algorithm B1....95
E.9.1.1 Purpose....95
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)....99

F.1 Introduction....99
F.1.1 Scope....99
F.1.2 References....99
F.1.3 Definitions and Abbreviations....100
F.1.3.1 Definitions....100
F.1.3.2 Abbreviations....100

F.2 Security Requirements....100

F.3 Storage of the Master Group Keys and overview of flows 101
F.3.1 Distribution of ciphering data during establishment of a voice/broadcast group call....................101
F.3.2 Signalling information required for the voice group call uplink access in the anchor MSC (normal case, subsequent talker on dedicated channel) 104
F.3.3 Signalling information required to transfer the originator or subsequent talker from a dedicated channel to a group call channel....................106

F.4 Key derivation....................106
F.4.1 Key derivation within the USIM / GCR....................107
F.4.2 Key derivation within the ME/BSS....................108
F.4.3 Encryption algorithm selection....................109
F.4.4 Algorithm requirements 109
F.4.4.1 A8_V 109
F.4.4.2 KMF....................109

F.5 Encryption of voice group calls....................110

F.6 Specification of the Key Modification Function (KMF)....................110

Annex G (informative): Generation of VSTK_RAND 111

Annex H (normative): Access security related functions for enhanced General Packet Radio Service (GPRS) in relation to Cellular Internet of Things (CIoT)..........112

H.1 Introduction 112
H.1.1 General 112
H.1.2 Considerations on bidding down attacks 112

H.2 Authentication and key agreement....................112

H.3 Ciphering and integrity mode negotiation....................112

H.4 Protection of GMM messages 118

H.5 Algorithms for ciphering and integrity protection....................118
H.5.0 General 118
H.5.1 Null ciphering algorithm 119
H.5.2 Ciphering algorithm 119
H.5.2.1 Inputs and outputs....................119
H.5.2.1.1 General....................119
H.5.2.1.2 CONSTANT-F....................120
H.5.2.2 GEA5 120
H.5.3 Integrity algorithm....................120
H.5.3.1 Inputs and outputs....................120
H.5.3.1.1 General....................120
H.5.3.1.2 INPUT-I 120
H.5.3.1.3 CONSTANT-F....................121
H.5.3.2 GIA4 121
H.5.3.3 GIA5 121

H.6 Derivation of Kc128 and Ki128 121

H.7 Integrity protection of user plane 122

H.8 Definition of MAC-GMM in GMM Authentication and Ciphering Request and GMM Authentication and Ciphering Response messages 122
H.8.1 Inputs and outputs 122

H.9 Protected negotiation of IOV values 123
H.9.1 Protected IOV container....................123
H.9.2 LLC XID procedure with protected IOV container....................124

Annex I (informative): Change history 125

History 126

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 ".