

ETSI TS 133 102 V14.1.0 (2017-03)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
3G security;
Security architecture
(3GPP TS 33.102 version 14.1.0 Release 14)**



Reference

RTS/TSGS-0333102ve10

Keywords

GSM,SECURITY,UMTS

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

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.
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

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.....	7
1 Scope	8
2 References	8
3 Definitions, symbols abbreviations and conventions	10
3.1 Definitions	10
3.2 Symbols.....	11
3.3 Abbreviations	11
3.4 Conventions.....	12
4 Overview of the security architecture.....	12
5 Security features	14
5.1 Network access security	14
5.1.1 User identity confidentiality	14
5.1.2 Entity authentication	14
5.1.3 Confidentiality	14
5.1.4 Data integrity	15
5.1.5 Mobile equipment identification.....	15
5.2 Network domain security	15
5.2.1 Void	15
5.2.2 Void	15
5.2.3 Void	15
5.2.4 Fraud information gathering system	16
5.3 User domain security	16
5.3.1 User-to-USIM authentication.....	16
5.3.2 USIM-Terminal Link.....	16
5.4 Application security	16
5.4.1 Secure messaging between the USIM and the network	16
5.4.2 Void	16
5.4.3 Void	16
5.4.4 Void	16
5.5 Security visibility and configurability	17
5.5.1 Visibility	17
5.5.2 Configurability.....	17
6 Network access security mechanisms	17
6.1 Identification by temporary identities.....	17
6.1.1 General.....	17
6.1.2 TMSI reallocation procedure	18
6.1.3 Unacknowledged allocation of a temporary identity	18
6.1.4 Location update	18
6.2 Identification by a permanent identity.....	19
6.3 Authentication and key agreement	19
6.3.1 General.....	19
6.3.2 Distribution of authentication data from HE to SN	21
6.3.3 Authentication and key agreement.....	23
6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain.....	26
6.3.5 Re-synchronisation procedure	27
6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR	28
6.3.6.1 Authentication re-attempt.....	28
6.3.7 Length of authentication parameters.....	29
6.4 Local authentication and connection establishment	29

6.4.1	Cipher key and integrity key setting	29
6.4.2	Ciphering and integrity mode negotiation	29
6.4.3	Cipher key and integrity key lifetime	30
6.4.4	Cipher key and integrity key identification.....	30
6.4.5	Security mode set-up procedure.....	31
6.4.6	Signalling procedures in the case of an unsuccessful integrity check.....	34
6.4.7	Signalling procedure for periodic local authentication	34
6.4.8	Initialisation of synchronisation for ciphering and integrity protection.....	34
6.4.9	Emergency call handling	35
6.4.9.1	Security procedures applied	35
6.4.9.2	Security procedures not applied	35
6.5	Access link data integrity	36
6.5.1	General.....	36
6.5.2	Layer of integrity protection	36
6.5.3	Data integrity protection method	36
6.5.4	Input parameters to the integrity algorithm.....	37
6.5.4.1	COUNT-I.....	37
6.5.4.2	IK	37
6.5.4.3	FRESH	37
6.5.4.4	DIRECTION	38
6.5.4.5	MESSAGE	38
6.5.5	Integrity key selection.....	38
6.5.6	UIA identification	38
6.6	Access link data confidentiality.....	39
6.6.1	General.....	39
6.6.2	Layer of ciphering.....	39
6.6.3	Ciphering method	39
6.6.4	Input parameters to the cipher algorithm	40
6.6.4.1	COUNT-C.....	40
6.6.4.2	CK	40
6.6.4.3	BEARER.....	41
6.6.4.4	DIRECTION	41
6.6.4.5	LENGTH.....	41
6.6.5	Cipher key selection.....	41
6.6.6	UEA identification.....	42
6.7	Void.....	42
6.8	Interoperation and handover between UMTS and GSM	42
6.8.1	Authentication and key agreement of UMTS subscribers	42
6.8.1.1	General	42
6.8.1.2	R99+ HLR/AuC	43
6.8.1.3	R99+ VLR/SGSN	44
6.8.1.4	R99+ ME.....	45
6.8.1.5	USIM.....	45
6.8.2	Authentication and key agreement for GSM subscribers.....	46
6.8.2.1	General	46
6.8.2.2	R99+ HLR/AuC	47
6.8.2.3	VLR/SGSN	47
6.8.2.4	R99+ ME.....	48
6.8.3	Distribution and use of authentication data between VLRs/SGSNs	48
6.8.4	Intersystem handover for CS Services – from UTRAN to GSM BSS.....	49
6.8.4.1	UMTS security context	49
6.8.4.2	GSM security context.....	50
6.8.5	Intersystem handover for CS Services – from GSM BSS to UTRAN.....	50
6.8.5.1	UMTS security context	50
6.8.5.2	GSM security context.....	51
6.8.6	Intersystem change for PS Services – from UTRAN to GSM BSS	51
6.8.6.1	UMTS security context	51
6.8.6.2	GSM security context.....	52
6.8.7	Intersystem change for PS services – from GSM BSS to UTRAN.....	52
6.8.7.1	UMTS security context	52
6.8.7.2	GSM security context.....	52
6.8.8	PS handover from Iu to Gb mode	53

6.8.8.1	UMTS security context	53
6.8.8.2	GSM security context.....	53
6.8.9	PS handover from Gb to Iu mode	54
6.8.9.1	UMTS security context	54
6.8.9.2	GSM security context.....	54
6.8.10	SRVCC – between HSPA and UTRAN/GERAN.....	54
6.8.10.1	SRVCC from HSPA to circuit switched UTRAN/GERAN	54
6.8.10.2	SRVCC from circuit switched GERAN to HSPA.....	56
6.8.11	Handling of the START value in intersystem mobility cases	58
7	Void.....	59
8	Application security mechanisms.....	59
8.1	Void.....	59
8.2	Void.....	59
8.3	Mobile IP security	59
Annex A:	Void	60
Annex B (normative):	Key derivation function.....	61
B.1	General	61
B.2	FC value allocations	61
B.3	Derivation of $CK'_{CS} IK'_{CS}$ from $CK_{PS} IK_{PS}$	61
B.4	Derivation of Kc' from Kc for HSPA to UTRAN/GERAN SRVCC handover.....	61
B.5	Derivation of Kc_{128}	61
B.6	Derivation of $CK'_{PS} IK'_{PS}$ from $CK_{CS} IK_{CS}$	62
B.7	Derivation of Kc' from Kc for UTRAN/GERAN to HSPA SRVCC handover	62
Annex C (informative):	Management of sequence numbers	63
C.1	Generation of sequence numbers in the Authentication Centre	63
C.1.1	Sequence number generation schemes	63
C.1.1.1	General scheme.....	63
C.1.1.2	Generation of sequence numbers which are not time-based	64
C.1.1.3	Time-based sequence number generation	64
C.1.2	Support for the array mechanism	64
C.2	Handling of sequence numbers in the USIM	64
C.2.1	Protection against wrap around of counter in the USIM	65
C.2.2	Verification of sequence number freshness in the USIM	65
C.2.3	Notes	65
C.3	Sequence number management profiles.....	66
C.3.1	Profile 1: management of sequence numbers which are partly time-based.....	66
C.3.2	Profile 2: management of sequence numbers which are not time-based	67
C.3.3	Profile 3: management of sequence numbers which are entirely time-based	67
C.3.4	Guidelines for the allocation of the index values in the array scheme	68
C.4	Guidelines for interoperability in a multi-vendor environment.....	68
Annex D:	Void	69
Annex E:	Void	70
Annex F (informative):	Example uses of the proprietary part of the AMF.....	71
F.1	Support multiple authentication algorithms and keys	71
F.2	Changing sequence number verification parameters.....	71
F.3	Setting threshold values to restrict the lifetime of cipher and integrity keys	71

Annex G (normative):	Support of algorithm change features.....	72
Annex H (normative):	Usage of the AMF	73
Annex I (normative):	Security requirements for RNCs in exposed locations	74
I.1	General	74
I.2	Requirements for RNCs in exposed locations.....	74
I.2.1	Requirements for setup and configuration.....	74
I.2.2	Requirements for key management inside RNCs in exposed locations	74
I.2.3	Requirements for handling user plane data	75
I.2.4	Requirements for handling control plane data.....	75
I.2.5	Requirements for secure environment.....	75
I.3	Security mechanisms for interfaces with RNCs in exposed locations	75
Annex J (informative):	Change history	77
History		79

Foreword

This Technical Specification (TS) has been produced by ETSI 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.

1 Scope

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (TS 21.133 [1]) and implement the security objectives and principles described in TS 33.120 [2]. A security mechanism is an element that is used to realise a security feature. All security features and security mechanisms taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e. intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the MS are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

GSM security functions are defined in the TS 43.020 [36].

2 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 21.133: "3G Security; Security Threats and Requirements".
- [2] 3GPP TS 33.120: "3G Security; Security Principles and Objectives".
- [3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications (Release 1999)".
- [4] 3GPP TS 23.121: "Architecture Requirements for Release 99".
- [5] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".
- [6] 3GPP TS 22.022: "Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".
- [7] 3GPP TS 23.048: "Security Mechanisms for the (U)SIM application toolkit; Stage 2".
- [8] 3GPP TS 43.020: "Security related network functions".
- [9] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".
- [11] 3GPP TS 35.201: "Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".
- [12] 3GPP TS 35.202: "Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".