ETSI TS 133 401 V12.15.0 (2015-10)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP System Architecture Evolution (SAE);
Security architecture
(3GPP TS 33.401 version 12.15.0 Release 12)

Reference

RTS/TSGS-0333401vcf0

Keywords

GSM,LTE,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
http://portal.etsi.org/tb/status/status.asp

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 2015.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM 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 (http://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
1 Scope 9
2 References 9
3 Definitions, symbols and abbreviations 10
3.1 Definitions 10
3.2 Symbols 12
3.3 Abbreviations 12
3.4 Conventions 13
4 Overview of Security Architecture 14
5 Security Features 14
5.1 User-to-Network security 14
5.1.0 General 14
5.1.1 User identity and device confidentiality 15
5.1.2 Entity authentication 15
5.1.3 User data and signalling data confidentiality 15
5.1.3.1 Ciphering requirements 15
5.1.3.2 Algorithm Identifier Values 15
5.1.4 User data and signalling data integrity 16
5.1.4.1 Integrity requirements 16
5.1.4.2 Algorithm Identifier Values 16
5.2 Security visibility and configurability 17
5.3 Security requirements on eNodeB 17
5.3.1 General 17
5.3.2 Requirements for eNB setup and configuration 17
5.3.3 Requirements for key management inside eNB 18
5.3.4 Requirements for handling User plane data for the eNB 18
5.3.4a Requirements for handling Control plane data for the eNB 18
5.3.5 Requirements for secure environment of the eNB 18
5.4 Void 19
6 Security Procedures between UE and EPC Network Elements 19
6.0 General 19
6.1 Authentication and key agreement 19
6.1.1 AKA procedure 19
6.1.2 Distribution of authentication data from HSS to serving network 20
6.1.3 User identification by a permanent identity 21
6.1.4 Distribution of IMSI and authentication data within one serving network domain 22
6.1.5 Distribution of IMSI and authentication data between different serving network domains 23
6.1.6 Distribution of IMSI and UMTS authentication vectors between MMEs or between MME and SGSN 23
6.2 EPS key hierarchy 23
6.3 EPS key identification 26
6.4 Handling of EPS security contexts 27
6.5 Handling of NAS COUNTs 27
7 Security Procedures between UE and EPS Access Network Elements 29
7.0 General 29
7.1 Mechanism for user identity confidentiality 29
7.2 Handling of user-related keys in E-UTRAN 29
7.2.1 E-UTRAN key setting during AKA 29
7.2.2 E-UTRAN key identification 29

7.2.3 E-UTRAN key lifetimes 29
7.2.4 Security mode command procedure and algorithm negotiation 30
7.2.4.1 Requirements for algorithm selection 30
7.2.4.2 Procedures for AS algorithm selection 30
7.2.4.2.1 Initial AS security context establishment 30
7.2.4.2.2 X2-handover 31
7.2.4.2.3 S1-handover 31
7.2.4.2.4 Intra-eNB handover 31
7.2.4.3 Procedures for NAS algorithm selection 31
7.2.4.3.1 Initial NAS security context establishment 31
7.2.4.3.2 MME change 31
7.2.4.4 NAS security mode command procedure 32
7.2.4.5 AS security mode command procedure 33
7.2.4a Algorithm negotiation for unauthenticated UEs in LSM 34
7.2.5 Key handling at state transitions to and away from EMM-DEREGISTERED 34
7.2.5.1 Transition to EMM-DEREGISTERED 34
7.2.5.2 Transition away from EMM-DEREGISTERED 35
7.2.5.2.1 General 35
7.2.5.2.2 With existing native EPS NAS security context 36
7.2.5.2.3 With run of EPS AKA 36
7.2.6 Key handling in ECM-IDLE to ECM-CONNECTED and ECM-CONNECTED to ECM-IDLE transitions 37
7.2.6.1 ECM-IDLE to ECM-CONNECTED transition 37
7.2.6.2 Establishment of keys for cryptographically protected radio bearers 37
7.2.6.3 ECM-CONNECTED to ECM-IDLE transition 37
7.2.7 Key handling for the TAU procedure when registered in E-UTRAN 38
7.2.8 Key handling in handover 38
7.2.8.1 General 38
7.2.8.1.1 Access stratum 38
7.2.8.1.2 Non access stratum 39
7.2.8.2 Void 39
7.2.8.3 Key derivations for context modification procedure 39
7.2.8.4 Key derivations during handovers 40
7.2.8.4.1 Intra-eNB Handover 40
7.2.8.4.2 X2-handover 40
7.2.8.4.3 S1-Handover 40
7.2.8.4.4 UE handling 41
7.2.9 Key-change-on-the fly 41
7.2.9.1 General 41
7.2.9.2 K_{eNB} re-keying 41
7.2.9.3 KeNB refresh 42
7.2.9.4 NAS key re-keying 42
7.2.10 Rules on Concurrent Running of Security Procedures 43
7.3 UP security mechanisms 43
7.3.1 UP confidentiality mechanisms 43
7.3.2 UP integrity mechanisms 44
7.4 RRC security mechanisms 44
7.4.1 RRC integrity mechanisms 44
7.4.2 RRC confidentiality mechanisms 44
7.4.3 K_{eNB}* and Token Preparation for the RRCConnectionRe-establishment Procedure 45
7.5 Signalling procedure for periodic local authentication 46
8 Security mechanisms for non-access stratum signalling 46
8.0 General 46
8.1 NAS integrity mechanisms 46
8.1.1 NAS input parameters and mechanism 47
8.1.2 NAS integrity activation 47
8.2 NAS confidentiality mechanisms 47
9 Security interworking between E-UTRAN and UTRAN 48
9.1 RAU and TAU procedures 48
9.1.1 RAU procedures in UTRAN 48

9.1.2 TAU procedures in E-UTRAN 49
9.2 Handover 50
9.2.1 From E-UTRAN to UTRAN 50
9.2.2 From UTRAN to E-UTRAN 51
9.2.2.1 Procedure 51
9.2.2.2 Derivation of NAS keys and K_{eNB} during Handover from UTRAN to E-UTRAN 56
9.3 Recommendations on AKA at IRAT-mobility to E-UTRAN 56
9.4 Attach procedures 56
9.4.1 Attach in UTRAN 56

10 Security interworking between E-UTRAN and GERAN 57
10.1 General 57
10.2 RAU and TAU procedures 57
10.2.1 RAU procedures in GERAN 57
10.2.2 TAU procedures in E-UTRAN 58
10.3 Handover 58
10.3.1 From E-UTRAN to GERAN 58
10.3.2 From GERAN to E-UTRAN 58
10.3.2.1 Procedures 58
10.4 Recommendations on AKA at IRAT-mobility to E-UTRAN 58
10.5 Attach procedures 58
10.5.1 Attach in GERAN 58

11 Network Domain Control Plane protection 58

12 Backhaul link user plane protection 59

13 Management plane protection over the S1 interface 59

14 SRVCC between E-UTRAN and Circuit Switched UTRAN/GERAN 60
14.1 From E-UTRAN to Circuit Switched UTRAN/GERAN 60
14.2 Emergency call in SRVCC from E-UTRAN to circuit switched UTRAN/GERAN 61
14.3 SRVCC from circuit switched UTRAN/GERAN to E-UTRAN 62
14.3.1 Procedure 62

15 Security Aspects of IMS Emergency Session Handling 65
15.1 General 65
15.2 Security procedures and their applicability 66
15.2.1 Authenticated IMS Emergency Sessions 66
15.2.1.1 General 66
15.2.1.2 UE and MME share a current security context 66
15.2.2 Unauthenticated IMS Emergency Sessions 67
15.2.2.1 General 67
15.2.2.2 UE and MME share no security context 68
15.2.3 Void 69
15.2.4 Key generation procedures for unauthenticated IMS Emergency Sessions 69
15.2.4.1 General 69
15.2.4.2 Handover 69

Annex A (normative): Key derivation functions 70

A.1 KDF interface and input parameter construction 70
A.1.1 General 70
A.1.2 FC value allocations 70

A.2 K_{ASME} derivation function 70

A.3 K_{eNB} derivation function 70

A.4 NH derivation function 71

A.5 K_{eNB}* derivation function 71

A.6 Void 71

A.7 Algorithm key derivation functions 71

A.8 K_{ASME} to CK', IK' derivation at handover 72
A.9 NAS token derivation for inter-RAT mobility 72
A.10 K'$_{ASME}$ from CK, IK derivation during handover 73
A.11 K'$_{ASME}$ from CK, IK derivation during idle mode mobility 73
A.12 K_{ASME} to CK_{SRVCC}, IK_{SRVCC} derivation 73
A.13 K_{ASME} to CK', IK' derivation at idle mobility 74
A.14 (Void) 74
A.15 Derivation of S-K_{eNB} for dual connectivity 74
Annex B (normative): Algorithms for ciphering and integrity protection 75
B.0 Null ciphering and integrity protection algorithms 75
B.1 128-bit ciphering algorithm 75
B.1.1 Inputs and outputs 75
B.1.2 128-EEA1 76
B.1.3 128-EEA2 76
B.1.4 128-EEA3 76
B.2 128-Bit integrity algorithm 76
B.2.1 Inputs and outputs 76
B.2.2 128-EIA1 77
B.2.3 128-EIA2 77
B.2.4 128-EIA3 77
Annex C (informative): Algorithm test data 78
C.1 128-EEA2 78
C.1.1 Test Set 1 78
C.1.2 Test Set 2 79
C.1.3 Test Set 3 80
C.1.4 Test Set 4 80
C.1.5 Test Set 5 81
C.1.6 Test Set 6 82
C.2 128-EIA2 85
C.2.1 Test Set 1 86
C.2.2 Test Set 2 87
C.2.3 Test Set 3 88
C.2.4 Test Set 4 89
C.2.5 Test Set 5 90
C.2.6 Test Set 6 91
C.2.7 Test Set 7 92
C.2.8 Test Set 8 95
C.3 128-EEA1 107
C.4 128-EIA1 107
C.4.1 Test Set 1 107
C.4.2 Test Set 2 108
C.4.3 Test Set 3 108
C.4.4 Test Set 4 108
C.4.5 Test Set 5 108
C.4.6 Test Set 6 109
C.4.7 Test Set 7 109
Annex D (normative): Security for Relay Node Architectures 112
D.1 Introduction 112
D.2 Solution 112

D.2.1 General 112
D.2.2 Security Procedures 112
D.2.3 USIM Binding Aspects 115
D.2.4 Enrolment procedures for RNs 115
D.2.5 Secure management procedures for RNs 115
D.2.6 Certificate and subscription handling 116

D.3 Secure channel profiles 117
D.3.1 General 117
D.3.2 APDU secure channel profile 117
D.3.3 Key agreement based on certificate exchange 118
D.3.3.1 TLS profile 118
D.3.3.2 Common profile for RN and UICC certificate 118
D.3.3.3 RN certificate profile 118
D.3.3.4 UICC certificate profile 119
D.3.4 Key agreement for pre-shared key (psk) case 119
D.3.5 Identities used in key agreement 119

Annex E: Dual connectivity 120

E.1 Introduction 120

E.2 Dual connectivity offload architecture 121
E.2.1 Protection of the X2 reference point 121
E.2.2 Addition and modification of DRB in SeNB 121
E.2.3 Activation of encryption/decryption 121
E.2.4 Derivation of keys for the DRBs in the SeNB 123
E.2.4.1 SCG Counter maintenance 123
E.2.4.2 Security key derivation 123
E.2.4.3 Negotiation of security algorithms 124
E.2.5 S-K_{eNB} update 124
E.2.5.1 S-K_{eNB} update triggers 124
E.2.5.2 S-K_{eNB} update procedure 124
E.2.6 Handover procedures 124
E.2.7 Periodic local authentication procedure 124
E.2.8 Radio link failure recovery 124
E.2.9 Avoiding key stream reuse caused by DRB type change 125

Annex F (informative): Change history 126

History 131

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.

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the Evolved Packet System and the Evolved Packet Core, and the security procedures performed within the evolved Packet System (EPS) including the Evolved Packet Core (EPC) and the Evolved UTRAN (E-UTRAN).

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 33.102: "3G security; Security architecture".

[5] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[9] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[10] – [11] Void.

[12] 3GPP TS 36.323: "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification"

[13] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[14] 3GPP TS 35.215: "Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications"

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197) "

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] – [20] Void.

[21] 3GPP TS 36.331:"Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".