

ETSI TS 133 203 V14.0.0 (2017-04)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Access security for IP-based services
(3GPP TS 33.203 version 14.0.0 Release 14)**



Reference

RTS/TSGS-0333203ve00

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

<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.

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.....	9
1 Scope	10
2 References	10
3 Definitions, symbols and abbreviations	13
3.1 Definitions	13
3.2 Symbols.....	13
3.3 Abbreviations	13
4 Overview of the security architecture.....	14
5 Security features	17
5.1 Secure access to IMS.....	17
5.1.1 Authentication of the subscriber and the network.....	17
5.1.2 Re-Authentication of the subscriber	17
5.1.3 Confidentiality protection	17
5.1.4 Integrity protection	18
5.2 Network topology hiding.....	18
5.3 SIP Privacy handling in IMS Networks	18
5.4 SIP Privacy handling when interworking with non-IMS Networks	19
6 Security mechanisms	19
6.1 Authentication and key agreement	19
6.1.0 General.....	19
6.1.1 Authentication of an IM-subscriber	19
6.1.2 Authentication failures.....	22
6.1.2.1 User authentication failure	22
6.1.2.2 Network authentication failure.....	22
6.1.2.3 Incomplete authentication	23
6.1.3 Synchronization failure.....	23
6.1.4 Network Initiated authentications.....	24
6.1.5 Integrity protection indicator	25
6.2 Confidentiality mechanisms	25
6.3 Integrity mechanisms	26
6.4 Hiding mechanisms	26
6.5 CSCF interoperating with proxy located in a non-IMS network.....	26
7 Security association set-up procedure	27
7.0 General	27
7.1 Security association parameters	27
7.2 Set-up of security associations (successful case).....	30
7.3 Error cases in the set-up of security associations	33
7.3.1 Error cases related to IMS AKA	33
7.3.1.0 General	33
7.3.1.1 User authentication failure	33
7.3.1.2 Network authentication failure.....	33
7.3.1.3 Synchronisation failure	33
7.3.1.4 Incomplete authentication	33
7.3.2 Error cases related to the Security-Set-up.....	33
7.3.2.1 Proposal unacceptable to P-CSCF.....	33
7.3.2.2 Proposal unacceptable to UE.....	33
7.3.2.3 Failed consistency check of Security-Set-up lines at the P-CSCF	34
7.4 Authenticated re-registration	34
7.4.0 General.....	34

7.4.1	Void	34
7.4.1a	Management of security associations in the UE	34
7.4.2	Void	35
7.4.2a	Management of security associations in the P-CSCF	35
7.5	Rules for security association handling when the UE changes IP address	36
8	ISIM	36
8.0	General	36
8.1	Requirements on the ISIM application	37
8.2	Sharing security functions and data with the USIM	37
9	IMC	38
Annex A:	Void	39
Annex B:	Void	40
Annex C:	Void	41
Annex D:	Void	42
Annex E:	Void	43
Annex F:	Void	44
Annex G (informative):	Management of sequence numbers	45
Annex H (normative):	The use of "Security Mechanism Agreement for SIP Sessions" [21] for security mode set-up	46
Annex I (normative):	Key expansion functions for IPsec ESP	48
Annex J (informative):	Recommendations to protect the IMS from UEs bypassing the P-CSCF	49
Annex K:	Void	50
Annex L (Normative):	Application to fixed broadband access	51
L.1	Introduction	51
L.2	Application of clause 4	51
Annex M (normative):	Enhancements to the access security for IP based services to enable NAT traversal for signaling messages	53
M.0	General	53
M.1	Scope	53
M.2	References	53
M.3	Definitions, symbols and abbreviations	53
M.4	Overview of the security architecture	53
M.5	Security features	53
M.6	Security mechanisms	54
M.6.1	Authentication and key agreement	54
M.6.2	Confidentiality mechanisms	54
M.6.3	Integrity mechanisms	54
M.6.4	Hiding mechanisms	54
M.6.5	CSCF interoperating with proxy located in a non-IMS network	55
M.7	Security association set-up procedure	55
M.7.0	General	55

M.7.1	Security association parameters	55
M.7.2	Set-up of security associations (successful case).....	59
M.7.3	Error cases in the set-up of security associations	64
M.7.3.1	Error cases related to IMS AKA	64
M.7.3.2	Error cases related to the Security-Set-up.....	64
M.7.3.2.1	Proposal unacceptable to P-CSCF.....	64
M.7.3.2.2	Proposal unacceptable to UE.....	64
M.7.3.2.3	Failed consistency check of Security-Set-up lines at the P-CSCF	64
M.7.3.2.4	Missing NAT traversal capabilities in the presence of a NAT	64
M.7.4	Authenticated re-registration	64
M.7.4.0	General.....	64
M.7.4.1	Void	65
M.7.4.1a	Management of security associations in the UE	65
M.7.4.2	Void	65
M.7.4.2a	Management of security associations in the P-CSCF	65
M.7.5	Rules for security association handling when the UE changes IP address	66
M.8	ISIM	67
M.9	IMC	67
Annex N (normative): Enhancements to the access security to enable SIP Digest.....		68
N.1	SIP Digest.....	68
N.2	Authentication	68
N.2.1	Authentication Requirements	68
N.2.1.1	Authentication Requirements for Registrations	68
N.2.1.2	Authentication Requirements for Non-registration Messages	71
N.2.2	Authentication failures	73
N.2.2.1	User Authentication failure.....	73
N.2.2.2	Network authentication failure	73
N.2.2.3	Incomplete Authentication.....	73
N.2.3	SIP Digest synchronization failure.....	73
N.2.4	Network Initiated authentications.....	74
N.2.5	Support for dynamic password change.....	74
Annex O (normative): Enhancements to the access security to enable TLS.....		76
O.1	TLS.....	76
O.1.1	TLS Access Security	76
O.1.2	Confidentiality protection.....	76
O.1.3	Integrity protection	76
O.1.4	TLS integrity protection indicator	77
O.2	TLS Session set-up procedure.....	77
O.2.1	TLS Profile for TLS based access security.....	77
O.2.2	TLS session set-up during registration	78
O.2.3	TLS session set-up prior to Initial registration	79
O.3	Error cases in the set-up of TLS sessions.....	79
O.3.1	Error cases related to TLS	79
O.3.1.0	General.....	79
O.3.1.1	User authentication failure.....	79
O.3.1.2	Network authentication failure	80
O.3.1.3	Synchronisation failure	80
O.3.1.4	Incomplete authentication.....	80
O.3.2	Error cases related to the Security-Set-Up	80
O.4	Management of TLS sessions.....	80
O.4.1	Management of TLS sessions at the UE.....	80
O.4.2	Management of TLS sessions at the P-CSCF.....	80
O.4.3	Authenticated re-registration	80
O.5	TLS Certificate Profile and Validation.....	81

O.5.1	TLS Certificate	81
O.5.2	Certificate validation	81
O.5.3	Certificate Revocation	82
Annex P (normative): Co-existence of authentication schemes IMS AKA, GPRS-IMS-Bundled Authentication, NASS-IMS-bundled authentication, SIP Digest and Trusted Node Authentication83		
P.1	Scope of this Annex	83
P.2	Requirements on co-existence of authentication schemes	83
P.3	P-CSCF procedure selection	83
P.4	Determination of requested authentication scheme in S-CSCF	85
P.4.1	Stepwise approach	85
P.4.2	Mechanisms for performing steps 1 to 3 in P.4.1	86
P.5	Co-existence of PANI-aware and other P-CSCFs	87
P.6	Considerations on the Cx interface	87
Annex Q (informative): Usage of the authentication mechanisms for non-registration messages in Annexes N and O.....88		
Q.1	General	88
Q.2	Assertion of identities by the P-CSCF.....	88
Q.3	Strengths and boundary conditions for the use of authentication mechanisms for non-registration messages.....	89
Annex R (normative): NASS-IMS-bundled authentication91		
R.1	Overview	91
R.2	Use Cases and Limitations	91
R.3	Detailed description.....	91
Annex S (Normative): Application to 3GPP2 Access94		
S.1	Introduction	94
S.2	Application of clause 4.....	94
S.3	Application of clauses 5 through 9.....	95
S.4	3GPP2 AKA Credentials.....	96
S.4.1	Realisations of 3GPP2 AKA Credentials	96
S.5	Network Domain Security for IMS	96
S.5.1	General	96
S.5.2	Inter-domain Domain Security	96
S.5.3	Intra-domain Domain Security	97
S.5.4	Profiles of Network Domain Security Methods	97
S.5.4.1	General.....	97
S.5.4.2	Support of IPsec ESP.....	97
S.5.4.2.1	General	97
S.5.4.2.2	Support of ESP authentication and encryption.....	97
S.5.4.3	Support of TLS	98
Annex T (normative): GPRS-IMS-Bundled Authentication (GIBA) for Gm interface99		
T.1	Introduction	99
T.2	Requirements.....	99
T.3	Threat Scenarios.....	100

T.3.0	General	100
T.3.1	Impersonation on IMS level using the identity of an innocent user	100
T.3.2	IP spoofing	100
T.3.3	Combined threat scenario	100
T.4	GIBA Security Mechanism	101
T.5	Restrictions imposed by GIBA.....	101
T.6	Protection against IP address spoofing in GGSN.....	102
T.7	Interworking cases.....	102
T.8	Message Flows	105
T.8.1	Successful registration.....	105
T.8.2	Unsuccessful registration	106
T.8.3	Successful registration for a selected interworking case	108
Annex U (normative): Trusted Node Authentication (TNA)		111
U.1	Overview	111
U.2	Use case and detailed description.....	111
Annex V (informative): NAT deployment considerations for GIBA		114
Annex W (normative): Tunnelling of IMS Services over Restrictive Access Networks		115
W.1	Overview	115
W.2	Service and Media Reachability for Users over Restrictive Firewalls – Tunneled Firewall Traversal for IMS traffic	115
W.2.0	General	115
W.2.1	Firewall detection procedure	116
W.3	Service and Media Reachability for Users over Restrictive Firewalls – Extensions to STUN/TURN/ICE	117
W.3.1	Introduction	118
W.3.1.1	General.....	118
W.3.1.2	Firewall traversal for IMS control plane using SIP over TLS/TCP	118
W.3.1.3	Firewall traversal for IMS media plane using ICE and TURN	118
W.3.2	Reference model.....	119
W.3.3	Required functions of the UE.....	119
W.3.4	Required functions of the P-CSCF.....	120
W.3.5	Required functions of the TURN server.....	120
W.3.6	Required functions of the IMS-ALG and IMS-AGW	120
Annex X (Normative): Security for WebRTC IMS Client access to IMS		121
X.1	Introduction	121
X.2	Authentication of WebRTC IMS Client with IMS subscription re-using existing IMS authentication mechanisms.....	121
X.2.0	General	121
X.2.1	General requirements	121
X.2.2	Solution 1.1: Use of SIP Digest credentials.....	121
X.2.2.1	General.....	121
X.2.2.2	Requirements	122
X.2.2.3	Procedures.....	122
X.2.3	Solution 1.2: Use of IMS AKA	123
X.2.3.1	General.....	123
X.2.3.2	Requirements	124
X.2.3.3	Procedures.....	124
X.3	Authentication of WebRTC IMS Client with IMS subscription using web credentials.....	125
X.3.0	General	125
X.3.1	General requirements	126

X.3.2	Solution 2.1	126
X.3.2.1	General.....	126
X.3.2.2	Requirements	126
X.3.2.3	Procedures.....	127
X.4	Assignment of IMS identities to WebRTC IMS Client from pool of IMS subscriptions held by WWSF.....	131
X.4.0	General	131
X.4.1	General requirements	131
X.4.2	Solution 3.1	132
X.4.2.1	General.....	132
X.4.2.2	Requirements	132
X.4.2.3	Procedures.....	132
X.5	TURN credential provisioning and authentication (informative).....	136
X.5.1	Introduction	136
X.5.2	Solution 1: TURN credential provisioning and authentication using eP-CSCF	137
X.5.2.1	Overview	137
X.5.2.2	Procedures.....	137
X.5.3	Solution 2: TURN credential provisioning and authentication using OAuth Access token	138
X.5.3.1	Overview	138
X.5.3.2	Procedures.....	139
Annex Y (informative): Change history		142
History		147

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 scope for this technical specification is to specify the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system.

Since the scope also encompasses the use of these security features and mechanisms for secure access to IMS in the context of fixed broadband networks and 3GPP2 networks, Annex L and Annex S specify how the material in the main body and other normative Annexes of this document apply to the fixed broadband networks and 3GPP2 networks respectively.

The IMS supports IP Multimedia applications such as video, audio and multimedia conferences. SIP, Session Initiation Protocol, was chosen as the signalling protocol for creating and terminating Multimedia sessions, cf. RFC 3261 [6]. This specification only deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

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 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [2] Void.
- [3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".
- [4] Void.
- [5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".
- [6] IETF RFC 3261 "SIP: Session Initiation Protocol".
- [7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".
- [8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".
- [9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".
- [10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".
- [11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".
- [12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".
- [13]-[16] Void.