

ETSI TS 133 180 V15.12.0 (2022-09)



LTE; Security of the Mission Critical (MC) service (3GPP TS 33.180 version 15.12.0 Release 15)

[ETSI TS 133 180 V15.12.0 \(2022-09\)](https://standards.iteh.ai/catalog/standards/sist/37ea1312-05b0-4836-9e7f-4d1a7828f92a/etsi-ts-133-180-v15-12-0-2022-09)

<https://standards.iteh.ai/catalog/standards/sist/37ea1312-05b0-4836-9e7f-4d1a7828f92a/etsi-ts-133-180-v15-12-0-2022-09>



ReferenceRTS/TSGS-0333180vfc0

KeywordsLTE, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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://standards-portal.etsi.org/People/CommitteeSupportStaff.aspx> 4836-9e7f-

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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.

© ETSI 2022.

All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	12
1 Scope	13
2 References	13
3 Definitions and abbreviations.....	15
3.1 Definitions	15
3.2 Abbreviations	16
4 Overview of Mission Critical Security.....	17
4.1 General	17
4.2 Signalling plane security architecture.....	17
4.3 MC system security architecture	18
4.3.1 General.....	18
4.3.2 User authentication and authorisation.....	18
4.3.3 Identity keying of users and services	19
4.3.4 Protection of application plane signalling.....	20
4.3.4.1 Application plane signalling security	20
4.3.4.2 Security enforcement at the network edge	21
4.3.5 Media security	23
4.3.5.1 General	23
4.3.5.2 Media security for group communications.....	23
4.3.5.3 Media security for private calls.....	24
5 Common mission critical security framework	26
5.1 User authentication and authorization	26
5.1.1 General.....	26
5.1.2 User authentication	27
5.1.2.1 Identity management functional model.....	27
5.1.2.2 User authentication framework	28
5.1.2.3 OpenID Connect (OIDC)	29
5.1.2.3.1 General	29
5.1.2.3.2 User authentication example using username/password.....	30
5.1.3 MCX user service authorisation.....	30
5.1.3.1 General	30
5.1.3.2 MCX user service authorization with MCX Server	33
5.1.3.2.1 General	33
5.1.3.2.2 Using SIP REGISTER.....	33
5.1.3.2.3 Using SIP PUBLISH	34
5.1.4 Inter-domain MC user service authorization	34
5.1.4.1 General	34
5.1.4.2 Inter-domain identity management functional model	34
5.1.5 MC user migration service authentication and authorisation.....	36
5.2 Key management common elements.....	38
5.2.1 Overview of key management	38
5.2.2 Common key distribution	38
5.2.3 Key distribution with end-point diversity	40
5.2.4 Key distribution with associated parameters	42
5.2.5 Key distribution with SAKKE-to-self payload.....	43
5.2.6 Key distribution with identity hiding	44
5.2.7 Key distribution across multiple security domains	45
5.2.7.1 General	45
5.2.7.2 Identification of External Security Domains	45
5.2.7.3 Using multiple security domains.....	46

5.2.8	KMS Redirect Responses (KRRs)	46
5.2.8.1	Overview of KMS Redirect Response procedure (KRR)	46
5.2.8.1.1	General	46
5.2.8.1.2	KMSs and KMS URIs	47
5.2.8.2	Use of KRRs	47
5.2.8.2.1	Content of KRRs	47
5.2.8.2.2	KRR creation procedure by a receiver	47
5.2.8.2.3	KRR creation procedure by a MCX server or signalling proxy	48
5.2.8.2.4	Processing a KRR at a MCX server or signalling proxy	48
5.2.8.2.5	KMS Selection at the initiator	49
5.2.8.3	Security procedures for KMS Redirection Response	50
5.2.8.4	Security Procedures for reporting external security domain use	52
5.2.8.5	Policy around use of external security domains	52
5.3	User key management	52
5.3.1	Key Management Server (KMS)	52
5.3.1.1	General	52
5.3.1.2	Home KMS	53
5.3.1.3	Migration KMS	53
5.3.1.4	External KMS	54
5.3.2	Functional model for key management	54
5.3.3	Security procedures for key management	55
5.3.4	Provisioned key material to support end-to-end communication security	56
5.3.5	KMS Certificate	57
5.3.6	KMS provisioned Key Set	57
5.4	Key management from MC client to MC server (CSK upload)	58
5.5	Key management between MCX servers (SPK)	58
5.6	Key management for one-to-one (private) communications (PCK)	58
5.7	Key management for group communications (GMK)	59
5.7.1	General	59
5.7.2	Security procedures for GMK provisioning	59
5.7.3	Group member GMK management	60
5.8	Key management from MC server to MC client (Key download)	61
5.8.1	General	61
5.8.2	'Key download' procedure	61
5.9	Key management during MBMS bearer announcement	62
5.10	Void	62
5.10.1	Void	62
5.10.2	Void	62
5.10.3	Void	62
5.10.3.1	Void	62
5.10.3.2	Void	62
5.10.3.3	Void	62
5.10.3.4	Void	62
5.10.3.5	Void	62
5.10.4	Void	62
5.10.4.1	Void	62
5.10.4.2	Void	62
5.11	UE key storage and key persistence	62
5.11.1	Key storage	62
5.11.2	Key persistence	63
6	Supporting security mechanisms	63
6.1	HTTP	63
6.1.1	Authentication for HTTP-1 interface	63
6.1.2	HTTP-1 interface security	64
6.1.3	HTTP-3 interface security	64
6.2	SIP	64
6.2.1	Authentication for SIP core access	64
6.2.2	SIP-1 interface security	64
6.3	Network domain security	64
6.3.1	LTE access authentication and security	64
6.3.2	Inter/Intra domain interface security	64

7	MCPTT and MCVideo.....	65
7.1	General	65
7.2	Private communications	65
7.2.1	Key management	65
7.2.2	Security procedures (on-network).....	65
7.2.3	Security procedures (off-network).....	67
7.2.4	First-to-answer security and key management.....	68
7.2.4.1	Overview	68
7.2.4.2	First-to-answer request and response	69
7.2.4.3	First-to-answer call setup with security.....	69
7.2.4.4	First-to-answer media protection	71
7.2.5	Ambient listening call	71
7.2.6	Ambient viewing call.....	71
7.2.7	Private video pull	72
7.2.7.1	One-to-one video pull	72
7.2.7.2	One-from-server video pull	72
7.2.8	Private video push.....	73
7.2.8.1	One-to-one video push	73
7.2.8.2	One-to-server video push	74
7.2.8.3	Remotely initiated video push.....	74
7.3	Group communications	76
7.3.1	General.....	76
7.3.2	Group creation security procedure	76
7.3.3	Dynamic group keying.....	76
7.3.3.1	General	76
7.3.3.2	Group regrouping security procedure (within a single MC domain)	77
7.3.3.3	Group regrouping security procedure (involving multiple MC domains).....	77
7.3.4	Broadcast group call	78
7.3.5	Group-broadcast group call.....	78
7.3.6	Emergency group call	79
7.3.7	Imminent peril group call	79
7.3.8	Emergency Alert.....	79
7.3.9	Remotely initiated video push to group	80
7.3.10	Multi-talker configured MCPTT group	81
7.4	Key derivation for media.....	82
7.4.1	Derivation of SRTP master keys for private call	82
7.4.2	Derivation of SRTP master keys for group media	82
7.5	Media protection profile	83
7.5.1	General.....	83
7.5.2	Security procedures for media stream protection.....	84
8	MCDData	86
8.1	Overview	86
8.2	Key Management	87
8.3	One-to-one communications	88
8.4	Group communications	88
8.5	MCDData payload protection	89
8.5.1	General.....	89
8.5.2	Prerequisites.....	89
8.5.2.1	Prerequisites for protected payloads.....	89
8.5.2.2	Prerequisites for authenticated payloads	89
8.5.3	Key derivation for protected payloads.....	89
8.5.4	Payload protection	90
8.5.4.1	Format of protected payloads.....	90
8.5.4.2	Encryption of protected payloads.....	90
8.5.5	Payload authentication	91
9	Signalling protection	91
9.1	General	91
9.2	Key distribution for signalling protection	92
9.2.1	Client-Server Key (CSK).....	92
9.2.1.1	General	92

9.2.1.2	Creation of the CSK	92
9.2.1.3	Initial 'CSK Upload' Procedure	92
9.2.1.4	CSK update via 'key download'	93
9.2.2	Multicast Signalling Key (MuSiK)	93
9.2.3	Signalling Protection Key (SPK)	94
9.3	Application signalling security (XML protection)	95
9.3.1	General	95
9.3.2	Protected content	95
9.3.3	Key agreement	96
9.3.4	Confidentiality protection using XML encryption (xmlesc)	96
9.3.4.1	General	96
9.3.4.2	XML content encryption	96
9.3.4.3	XML URI attribute encryption	97
9.3.5	Integrity protection using XML signature (xmlesig)	98
9.4	RTCP signalling protection (SRTCP)	99
9.4.1	General	99
9.4.2	Unicast RTCP protection between client and server	100
9.4.3	Multicast RTCP protection between client and server	100
9.4.4	Offline floor and transmission control protection	100
9.4.5	RTCP protection between servers	100
9.4.6	Key derivation for SRTCP	100
9.4.7	Security procedures for transmission of RTCP content	101
9.4.8	RTCP protection profile	102
9.5	MCDATA signalling protection	103
9.5.1	Key distribution for signalling protection	103
9.5.2	Protection of MCDATA application signalling payloads (XML)	103
9.5.3	Protection of MCDATA signalling payloads	103
9.6	Message origin authentication and authorisation	103
9.6.1	General	103
9.6.2	Origin authentication and authorisation in the MC System	104
9.6.2.1	Types of signalling	104
9.6.2.2	Privileged Signalling	105
9.6.2.3	Signalling between network entities across domains	105
9.6.2.4	Signalling between the GMS and the GMC	105
9.6.2.5	Signalling between the MC domain and a migrated user	106
9.6.2.6	Off-network signalling	106
9.6.3	Authorised Identities	106
9.6.3.1	Format of an Authorised Identity	106
9.6.3.2	Obtaining an Authorised Identity	107
9.6.4	Element for Authenticating Requests (EARs)	107
9.6.4.1	Overview	107
9.6.4.2	The EAR information element	107
9.6.4.3	EAR authorisation	107
9.6.5	Security procedures for origin authentication	108
9.6.5.1	General	108
9.6.5.2	SIP signalling	108
9.6.5.2.1	General	108
9.6.5.2.2	Group affiliation and deaffiliation signalling	108
9.6.5.3	Off-network signalling	109
9.6.5.4	Processing a received EAR	109
10	Logging, Audit and Discreet Monitoring	109
10.1	Logging and audit of service metadata	109
10.1.1	Overview	109
10.1.2	User events	110
10.1.2.1	Types of events	110
10.1.2.2	Location of recording function	110
10.1.2.3	Security content within user event logs	110
10.1.2.4	Protection of user event logs	111
10.2	Audit and Discreet Monitoring of user content	111
10.2.1	Overview	111
10.2.2	Collection of user media	111

10.2.3	Storing of user media	111
10.2.4	Decryption of user media	111
11	Interconnection, interworking and migration security	112
11.1	Interconnection	112
11.1.1	Overview	112
11.1.2	Security procedures for interconnection	113
11.1.2.1	General	113
11.1.2.2	GMK transfer between MC systems	113
11.2	Interworking	114
11.2.1	General	114
11.2.2	Transport of non-3GPP interworking security data (InterSD)	114
Annex A (normative):	Security requirements	116
A.1	Introduction	116
A.2	Configuration & service access	116
A.3	Group key management	116
A.4	On-network operation	116
A.5	Ambient listening	117
A.6	Data communication between MCX network entities	117
A.7	Key stream re-use	117
A.8	Late entry to group communication	117
A.9	Private call confidentiality	117
A.10	Off-network operation	118
A.11	Privacy of MCX service identities	118
A.12	User authentication and authorization	118
A.13	Inter-domain	119
A.14	MCDData	120
A.15	Multimedia Broadcast/Multicast Service	120
Annex B (normative):	OpenID connect profile for MCX	121
B.1	General	121
B.2	MCX tokens	121
B.2.1	ID token	121
B.2.1.1	General	121
B.2.1.2	Standard claims	121
B.2.1.3	MCX claims	121
B.2.2	Access token	122
B.2.2.1	Introduction	122
B.2.2.2	Standard claims	122
B.2.2.3	MCX claims	122
B.3	MCX client registration	122
B.4	Obtaining tokens	123
B.4.1	General	123
B.4.2	Native MCX client	123
B.4.2.1	General	123
B.4.2.2	Authentication request	123
B.4.2.3	Authentication response	125
B.4.2.4	Access token request	125
B.4.2.5	Access token response	126
B.5	Refreshing an access token	126
B.5.1	General	126
B.5.2	Access token request	127
B.5.3	Access token response	127
B.6	MCX client registration with partner IdM service	128
B.7	Obtaining an access token from a partner domain	128
B.7.1	Overview	128
B.7.2	Token Exchange Request	129

B.7.3	Token Exchange Response	130
B.7.4	Token Request	130
B.7.5	Token Response	132
B.8	Security tokens	132
B.9	Access tokens for partner services	133
B.10	Using the token to access MCX resource servers	133
B.11	Token validation	133
B.11.1	ID token validation	133
B.11.2	Access token validation	133
B.11.3	Security token validation	133
B.12	Token revocation	133
B.12	IdMS interface security	133
Annex C (informative): OpenID connect detailed flow		135
C.1	Detailed flow for MC user authentication and registration using OpenID Connect	135
C.2	Detailed flow for inter-domain MC user service authorization using OpenID Connect token exchange	136
Annex D (Normative): KMS provisioning messages		139
D.1	General aspects	139
D.2	KMS requests	139
D.2.1	General	139
D.2.2	KMS request security	139
D.2.3	KMS Initialize request	140
D.2.4	KMS KeyProvision request	140
D.2.5	KMS CertCache request	141
D.2.6	KMS Cert request	141
D.2.7	KMS Lookup request	141
D.2.8	KMS Redirect Upload	141
D.3	KMS responses	142
D.3.1	General	142
D.3.2	KMS certificates	142
D.3.2.1	Description	142
D.3.2.2	Fields	143
D.3.2.3	User IDs	143
D.3.3	User Key Provision	143
D.3.3.1	Description	143
D.3.3.2	Fields	144
D.3.4	Example KMS response XML	144
D.3.4.1	Example KMSInit XML	144
D.3.4.2	Example KMSKeyProv XML	145
D.3.4.3	Example KMSCertCache XML	147
D.3.5	KMS response XML schema	149
D.3.5.1	Base XML schema	149
D.3.5.2	Security extension to KMS response XML schema	152
D.4	KMS Redirect Response (KRR)	152
D.4.1	General	152
D.4.2	KRR XML signature profile	152
D.4.3	Example XML	153
D.4.4	Example XML schema	154
Annex E (normative): MIKEY message formats for media security		156
E.1	General aspects	156
E.1.1	Introduction	156

E.1.2	MIKEY common fields	156
E.1.3	Crypto Session Identifiers	157
E.2	MIKEY message structure for GMK distribution	157
E.2.1	General	157
E.2.2	Default SRTP security profile for GMK use	157
E.3	MIKEY message structure for PCK distribution.....	158
E.3.1	General.....	158
E.3.2	Default SRTP security profile for PCK.....	159
E.3.3	Providing a SRTP security profile for PCK use	159
E.4	MIKEY message structure for CSK and MuSiK distribution	159
E.4.1	General	159
E.4.2	Default SRTCP security profile for CSK and MuSiK	160
E.4.3	Providing a SRTCP security profile for CSK or MuSiK.....	160
E.5	MIKEY general extension payload to support 'SAKKE-to-self'	160
E.6	MIKEY general extension payload to encapsulate parameters associated with a key	161
E.6.1	General	161
E.6.2	Void.....	162
E.6.3	MC group IDs.....	162
E.6.4	Activation time	163
E.6.5	Text	163
E.6.6	Reserved	163
E.6.7	Void.....	163
E.6.8	Void.....	163
E.6.9	Status	163
E.6.10	Expiry time.....	163
E.6.11	Key Type.....	163
E.7	Hiding identities within MIKEY messages.....	164
Annex F (normative):	Key derivation and hash functions.....	165
F.1	KDF interface and input parameter construction	165
F.1.1	General	165
F.1.2	FC value allocations	165
F.1.3	Calculation of the User Salt for GUK-ID generation	165
F.1.4	Calculation of keys for application data protection.....	165
F.1.5	Calculation of keys for MCDATA payload protection	166
F.2	Hash functions.....	166
F.2.1	Generation of MIKEY-SAKKE UID	166
F.2.1.1	Overview	166
F.2.1.2	Example UID	167
Annex G (normative):	Key identifiers	169
Annex H (normative):	Support for legacy multicast key (MKFC) and for MSCCK.....	170
H.1	General	170
H.2	MKFC Receipt	170
H.3	MSCCK Distribution.....	170
H.4	Use of multicast signalling keys (MKFC and MSCCK)	170
Annex I (normative):	Signalling Proxies.....	171
I.1	Overview	171
I.2	Location of a signalling proxy.....	172
I.2.1	Overview	172
I.2.2	Deployment with an untrusted SIP Core.....	172
I.2.3	Deployment with a trusted SIP Core.....	173
I.3	Functions of a signalling proxy	174
I.3.1	Overview	174
I.3.2	Identifier modification (topology hiding)	174

I.3.3	Resilience against signalling storm.....	174
I.3.4	Client connection to a CS Proxy	174
I.3.5	CSK key download from a CS Proxy	174
I.3.6	MuSiK and MSCCK key download from a CS Proxy.....	175
I.3.7	Signalling protection by the IS Proxy	175
I.3.8	Creation of KMS Redirect Responses (KRRs)	175
I.3.9	Policy enforcement	175

Annex J (normative): Authentication and authorisation formats176

J.1	Elements for Authenticating Requests	176
J.1.1	General	176
J.1.2	Format of an EAR	176
J.1.3	Format of an EAR ID	176
J.1.4	Format of an entity's Role ID	177
J.1.5	Format of an MC Entity ID	177
J.2	Request types and parameters	178
J.2.1	General	178
J.2.2	Request Information element	178
J.2.3	Request type	178
J.2.4	Request expiry	178
J.2.5	Request IDs	179
J.2.5.1	Format.....	179
J.2.5.2	Request ID values for privileged signalling.....	180
J.2.5.3	Request IDs for off-network signalling	180
J.3	Authorisation fields	181
J.3.1	General	181
J.3.2	Authorisation field names	181
J.3.3	Authorisation field values	182
J.3.3.1	General.....	182
J.3.3.2	Role authorisations	183
J.3.3.3	Authorisations for privileged signalling	183
J.3.3.4	Authorisations for off-network signalling.....	184
J.3.4	Example Authorised Identities	185
J.3.4.1	General.....	185
J.3.4.2	PTT User (on and off-network)	185
J.3.4.3	Dispatcher	185

Annex K (informative): Non-3GPP security mechanisms.....186

K.1	General	186
K.2	LMR E2EE	186
K.2.1	General	186
K.2.2	Interworking E2EE keys and key management.....	186
K.2.3	Interworking E2EE media for MCPTT	186
K.2.4	Interworking E2EE media for MCData.....	186

Annex L (normative): MC Security Gateway (SeGy).....188

L.1	General	188
L.2	Functional model for the MC Security Gateway (SeGy)	188
L.3	Functions of a MC Security Gateway (SeGy).....	189
L.3.1	Components of a MC Security Gateway (SeGy).....	189
L.3.2	Pseudo KMS.....	189
L.3.3	Pseudo GMS.....	189
L.3.4	Pseudo MCX Server or IS Proxy.....	190
L.3.5	Pseudo MC clients.....	190
L.4	Security procedures for the MC Security Gateway (SeGy)	190
L.4.1	General.....	190

L.4.2	Security procedures for private communication (initiated in the protected MC system)	191
L.4.3	Security procedures for private communication (initiated in the unprotected MC system)	192
L.4.4	Security procedures for group communications (group homed in the protected MC system)	193
L.4.5	Security procedures for group communications (group homed in the unprotected MC system)	195
L.5	Interworking using a MC Security Gateway	196
L.5.1	General	196
L.5.2	MC Security Gateway and the IWF	196
Annex M (informative):	Change history	198
History		201

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 133 180 V15.12.0 (2022-09)

<https://standards.iteh.ai/catalog/standards/sist/37ea1312-05b0-4836-9e7f-4d1a7828f92a/etsi-ts-133-180-v15-12-0-2022-09>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 133 180 V15.12.0 (2022-09)

<https://standards.iteh.ai/catalog/standards/sist/37ea1312-05b0-4836-9e7f-4d1a7828f92a/etsi-ts-133-180-v15-12-0-2022-09>

1 Scope

The present document specifies the security architecture, procedures and information flows needed to protect the mission critical service (MCX). The architecture includes mechanisms to protect the Common Functional Architecture and security mechanisms for mission critical applications. This includes Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCDData). Additionally, security mechanisms relating to on-network use, off-network use, roaming, migration, interconnection, interworking and multiple security domains are described.

This specification complements the Common Functional Architecture defined in TS 23.280 [36], the functional architecture for MCPTT defined in 3GPP TS 23.379 [2], the functional architecture for MCVideo defined in 3GPP TS 23.281 [37] and the functional architecture for MCDData defined in 3GPP TS 23.282 [38].

The MC service can be used for public safety applications and also for general commercial applications e.g. utility companies and railways. As the security model is based on the public safety environment, some MC security features may not be applicable for commercial purposes.

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 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".
- [3] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT); Stage 1".
- [4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".
- [6] 3GPP TS 33.203: "3G security; Access security for IP-based services".
- [7] 3GPP TS 33.179 Release 13: "Security of Mission Critical Push To Talk (MCPTT) over LTE".
- [8] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".
- [9] IETF RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".
- [10] IETF RFC 6508: "Sakai-Kasahara Key Encryption (SAKKE)".
- [11] IETF RFC 6509: "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".
- [12] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".
- [13] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".
- [14] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- [15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

- [16] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".
- [17] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".
- [18] NIST FIPS 180-4: "Secure Hash Standard (SHS)".
- [19] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".
- [20] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".
- [21] OpenID Connect 1.0: "OpenID Connect Core 1.0 incorporating errata set 1", http://openid.net/specs/openid-connect-core-1_0.html.
- [22] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".
- [23] IETF RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".
- [24] IETF RFC 4771: "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)".
- [25] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".
- [26] IETF RFC 7714: "AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)".
- [27] W3C: "XML Encryption Syntax and Processing Version 1.1", <https://www.w3.org/TR/xmlenc-core1/>.
- [28] W3C: "XML Signature Syntax and Processing (Second Edition)", <http://www.w3.org/TR/xmldsig-core/>.
- [29] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".
- [30] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".
- [31] IETF RFC 6090: "Fundamental Elliptic Curve Cryptography Algorithms".
- [32] IETF RFC 7519: "JSON Web Token (JWT)".
- [33] IETF RFC 7662: "OAuth 2.0 Token Introspection".
- [34] IETF RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm".
- [35] IETF RFC 7515: "JSON Web Signature (JWS)".
- [36] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".
- [37] 3GPP TS 23.281: "Functional architecture and information flows for mission critical video; Stage 2".
- [38] 3GPP TS 23.282: "Functional model and information flows for Mission Critical Data".
- [39] 3GPP TS 23.002: "Network Architecture".
- [40] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".
- [41] IETF RFC 2392: "Content-ID and Message-ID Uniform Resource Locators".
- [42] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC".
- [43] IETF RFC 5116: "An Interface and Algorithms for Authenticated Encryption".