

ETSI TS 133 180 V15.4.0 (2019-05)



LTE;
Security of the mission critical service
(3GPP TS 33.180 version 15.4.0 Release 15)

Standard Preview
(standards.it-ebooks.info)
Full standard: <https://standards.iteh.ai/catalog/standards/sis/1797185-013c-4da2-96ab-8d2c60aa245b/etsi-ts-133-180-v15-4-0-2019-05>



Reference

RTS/TSGS-0333180vf40

Keywords

LTE, 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 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://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.

© ETSI 2019.

All rights reserved.

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.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

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.

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.....	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	17
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.....	19
4.3.4.1 Application plane signalling security	19
4.3.4.2 Security enforcement at the network edge	20
4.3.5 Media security	22
4.3.5.1 General	22
4.3.5.2 Media security for group communications.....	22
4.3.5.3 Media security for private calls.....	23
5 Common mission critical security framework	25
5.1 User authentication and authorization	25
5.1.1 General.....	25
5.1.2 User authentication	26
5.1.2.1 Identity management functional model.....	26
5.1.2.2 User authentication framework	27
5.1.2.3 OpenID Connect (OIDC)	28
5.1.2.3.1 General	28
5.1.2.3.2 User authentication example using username/password.....	29
5.1.3 MCX user service authorisation.....	29
5.1.3.1 General	29
5.1.3.2 MCX user service authorization with MCX Server	32
5.1.3.2.1 General	32
5.1.3.2.2 Using SIP REGISTER.....	32
5.1.3.2.3 Using SIP PUBLISH	33
5.1.4 Inter-domain MC user service authorization	33
5.1.4.1 General	33
5.1.4.2 Inter-domain identity management functional model	33
5.1.5 MC user migration service authentication and authorisation.....	35
5.2 Key management common elements.....	37
5.2.1 Overview of key management	37
5.2.2 Common key distribution	37
5.2.3 Key distribution with end-point diversity	39
5.2.4 Key distribution with associated parameters	41
5.2.5 Key distribution with SAKKE-to-self payload.....	42
5.2.6 Key distribution with identity hiding	43
5.2.7 Key distribution across multiple security domains	44
5.2.7.1 General	44
5.2.7.2 Identification of External Security Domains.....	44
5.2.7.3 Using multiple security domains.....	45

5.2.8	KMS Redirect Responses (KRRs).....	45
5.2.8.1	Overview of KMS Redirect Response procedure (KRR).....	45
5.2.8.1.1	General	45
5.2.8.1.2	KMSs and KMS URIs.....	46
5.2.8.2	Use of KRRs	46
5.2.8.2.1	Content of KRRs	46
5.2.8.2.2	KRR creation procedure by a receiver.....	46
5.2.8.2.3	KRR creation procedure by a MCX server or signalling proxy	47
5.2.8.2.4	Processing a KRR at a MCX server or signalling proxy	47
5.2.8.2.5	KMS Selection at the initiator	48
5.2.8.3	Security procedures for KMS Redirection Response	49
5.2.8.4	Security Procedures for reporting external security domain use	51
5.2.8.5	Policy around use of external security domains	51
5.3	User key management	51
5.3.1	Key Management Server (KMS)	51
5.3.1.1	General.....	51
5.3.1.2	Home KMS	52
5.3.1.3	Migration KMS	52
5.3.1.4	External KMS	53
5.3.2	Functional model for key management.....	53
5.3.3	Security procedures for key management	54
5.3.4	Provisioned key material to support end-to-end communication security	55
5.3.5	KMS Certificate	56
5.3.6	KMS provisioned Key Set	56
5.4	Key management from MC client to MC server (CSK upload)	57
5.5	Key management between MCX servers (SPK)	57
5.6	Key management for one-to-one (private) communications (PCK).....	57
5.7	Key management for group communications (GMK)	58
5.7.1	General.....	58
5.7.2	Security procedures for GMK provisioning	58
5.7.3	Group member GMK management	59
5.8	Key management from MC server to MC client (Key download)	60
5.8.1	General.....	60
5.8.2	'Key download' procedure	60
5.9	Key management during MBMS bearer announcement	61
5.10	Void.....	61
5.10.1	Void	61
5.10.2	Void	61
5.10.3	Void	61
5.10.3.1	Void.....	61
5.10.3.2	Void.....	61
5.10.3.3	Void.....	61
5.10.3.4	Void.....	61
5.10.3.5	Void.....	61
5.10.4	Void	61
5.10.4.1	Void.....	61
5.10.4.2	Void.....	61
5.11	UE key storage and key persistence	61
5.11.1	Key storage	61
5.11.2	Key persistence	62
6	Supporting security mechanisms.....	62
6.1	HTTP.....	62
6.1.1	Authentication for HTTP-1 interface.....	62
6.1.2	HTTP-1 interface security	63
6.1.3	HTTP-3 interface security	63
6.2	SIP	63
6.2.1	Authentication for SIP core access	63
6.2.2	SIP-1 interface security.....	63
6.3	Network domain security	63
6.3.1	LTE access authentication and security	63
6.3.2	Inter/Intra domain interface security.....	63

7	MCPTT and MCVideo.....	64
7.1	General	64
7.2	Private communications	64
7.2.1	Key management	64
7.2.2	Security procedures (on-network).....	64
7.2.3	Security procedures (off-network).....	66
7.2.4	First-to-answer security and key management.....	67
7.2.4.1	Overview	67
7.2.4.2	First-to-answer request and response	68
7.2.4.3	First-to-answer call setup with security.....	68
7.2.4.4	First-to-answer media protection	70
7.2.5	Ambient listening call	70
7.2.6	Ambient viewing call.....	70
7.2.7	Private video pull	71
7.2.7.1	One-to-one video pull	71
7.2.7.2	One-from-server video pull.....	71
7.2.8	Private video push.....	72
7.2.8.1	One-to-one video push	72
7.2.8.2	One-to-server video push	73
7.2.8.3	Remotely initiated video push.....	73
7.3	Group communications	75
7.3.1	General.....	75
7.3.2	Group creation security procedure.....	75
7.3.3	Dynamic group keying.....	75
7.3.3.1	General	75
7.3.3.2	Group regrouping security procedure (within a single MC domain)	76
7.3.3.3	Group regrouping security procedure (involving multiple MC domains).....	76
7.3.4	Broadcast group call	77
7.3.5	Group-broadcast group call.....	77
7.3.6	Emergency group call	78
7.3.7	Imminent peril group call	78
7.3.8	Emergency Alert.....	79
7.3.9	Remotely initiated video push to group	79
7.3.10	Multi-talker configured MCPTT group	80
7.4	Key derivation for media.....	81
7.4.1	Derivation of SRTP master keys for private call	81
7.4.2	Derivation of SRTP master keys for group media	81
7.5	Media protection profile	82
7.5.1	General.....	82
7.5.2	Security procedures for media stream protection.....	83
8	MCDData	85
8.1	Overview	85
8.2	Key Management	86
8.3	One-to-one communications	87
8.4	Group communications	87
8.5	MCDData payload protection	88
8.5.1	General.....	88
8.5.2	Prerequisites.....	88
8.5.2.1	Prerequisites for protected payloads.....	88
8.5.2.2	Prerequisites for authenticated payloads	88
8.5.3	Key derivation for protected payloads	88
8.5.4	Payload protection	89
8.5.4.1	Format of protected payloads	89
8.5.4.2	Encryption of protected payloads.....	89
8.5.5	Payload authentication	90
9	Signalling protection	90
9.1	General	90
9.2	Key distribution for signalling protection	91
9.2.1	Client-Server Key (CSK).....	91
9.2.1.1	General	91

9.2.1.2	Creation of the CSK	91
9.2.1.3	Initial 'CSK Upload' Procedure	91
9.2.1.4	CSK update via 'key download'	92
9.2.2	Multicast Signalling Key (MuSiK)	92
9.2.3	Signalling Protection Key (SPK)	93
9.3	Application signalling security (XML protection)	94
9.3.1	General	94
9.3.2	Protected content	94
9.3.3	Key agreement	95
9.3.4	Confidentiality protection using XML encryption (xmlenc)	95
9.3.4.1	General	95
9.3.4.2	XML content encryption	95
9.3.4.3	XML URI attribute encryption	96
9.3.5	Integrity protection using XML signature (xmlsig)	97
9.4	RTCP signalling protection (SRTCP)	98
9.4.1	General	98
9.4.2	Unicast RTCP protection between client and server	99
9.4.3	Multicast RTCP protection between client and server	99
9.4.4	Offline floor and transmission control protection	99
9.4.5	RTCP protection between servers	99
9.4.6	Key derivation for SRTCP	99
9.4.7	Security procedures for transmission of RTCP content	100
9.4.8	RTCP protection profile	101
9.5	MCDATA signalling protection	102
9.5.1	Key distribution for signalling protection	102
9.5.2	Protection of MCDATA application signalling payloads (XML)	102
9.5.3	Protection of MCDATA signalling payloads	102
9.6	Message origin authentication and authorisation	102
9.6.1	General	102
9.6.2	Origin authentication and authorisation in the MC System	103
9.6.2.1	Types of signalling	103
9.6.2.2	Privileged Signalling	104
9.6.2.3	Signalling between network entities across domains	104
9.6.2.4	Signalling between the GMS and the GMC	104
9.6.2.5	Signalling between the MC domain and a migrated user	105
9.6.2.6	Off-network signalling	105
9.6.3	Authorised Identities	105
9.6.3.1	Format of an Authorised Identity	105
9.6.3.2	Obtaining an Authorised Identity	106
9.6.4	Element for Authenticating Requests (EARs)	106
9.6.4.1	Overview	106
9.6.4.2	The EAR information element	106
9.6.4.3	EAR authorisation	106
9.6.5	Security procedures for origin authentication	107
9.6.5.1	General	107
9.6.5.2	SIP signalling	107
9.6.5.2.1	General	107
9.6.5.2.2	Group affiliation and deaffiliation signalling	107
9.6.5.3	Off-network signalling	108
9.6.5.4	Processing a received EAR	108
10	Logging, Audit and Discreet Monitoring	108
10.1	Logging and audit of service metadata	108
10.1.1	Overview	108
10.1.2	User events	109
10.1.2.1	Types of events	109
10.1.2.2	Location of recording function	109
10.1.2.3	Security content within user event logs	109
10.1.2.4	Protection of user event logs	110
10.2	Audit and Discreet Monitoring of user content	110
10.2.1	Overview	110
10.2.2	Collection of user media	110

10.2.3	Storing of user media	110
10.2.4	Decryption of user media	110
11	Interconnection, interworking and migration security	111
11.1	Interconnection	111
11.1.1	Overview	111
11.1.2	Security procedures for interconnection	112
11.1.2.1	General	112
11.1.2.2	GMK transfer between MC systems	112
11.2	Interworking	113
11.2.1	General	113
11.2.2	Transport of non-3GPP interworking security data (InterSD)	113
Annex A (normative): Security requirements		115
A.1	Introduction	115
A.2	Configuration & service access	115
A.3	Group key management	115
A.4	On-network operation	115
A.5	Ambient listening	116
A.6	Data communication between MCX network entities	116
A.7	Key stream re-use	116
A.8	Late entry to group communication	116
A.9	Private call confidentiality	116
A.10	Off-network operation	117
A.11	Privacy of MCX service identities	117
A.12	User authentication and authorization	117
A.13	Inter-domain	118
A.14	MCDATA	119
A.15	Multimedia Broadcast/Multicast Service	119
Annex B (normative): OpenID connect profile for MCX		120
B.1	General	120
B.2	MCX tokens	120
B.2.1	ID token	120
B.2.1.1	General	120
B.2.1.2	Standard claims	120
B.2.1.3	MCX claims	120
B.2.2	Access token	121
B.2.2.1	Introduction	121
B.2.2.2	Standard claims	121
B.2.2.3	MCX claims	121
B.3	MCX client registration	121
B.4	Obtaining tokens	122
B.4.1	General	122
B.4.2	Native MCX client	122
B.4.2.1	General	122
B.4.2.2	Authentication request	122
B.4.2.3	Authentication response	124
B.4.2.4	Access token request	124
B.4.2.5	Access token response	125
B.5	Refreshing an access token	125
B.5.1	General	125
B.5.2	Access token request	126
B.5.3	Access token response	126
B.6	MCX client registration with partner IdM service	127
B.7	Obtaining an access token from a partner domain	127
B.7.1	Overview	127
B.7.2	Token Exchange Request	128

B.7.3	Token Exchange Response.....	129
B.7.4	Token Request.....	129
B.7.5	Token Response	131
B.8	Security tokens	131
B.9	Access tokens for partner services	132
B.10	Using the token to access MCX resource servers	132
B.11	Token validation.....	132
B.11.1	ID token validation.....	132
B.11.2	Access token validation.....	132
B.11.3	Security token validation.....	132
B.12	Token revocation.....	132
B.12	IdMS interface security	132
Annex C (informative): OpenID connect detailed flow.....		134
C.1	Detailed flow for MC user authentication and registration using OpenID Connect	134
C.2	Detailed flow for inter-domain MC user service authorization using OpenID Connect token exchange.....	135
Annex D (Normative): KMS provisioning messages		138
D.1	General aspects.....	138
D.2	KMS requests	138
D.2.1	General	138
D.2.2	KMS request security	138
D.2.3	KMS Initialize request.....	139
D.2.4	KMS KeyProvision request.....	139
D.2.5	KMS CertCache request.....	140
D.2.6	KMS Cert request.....	140
D.2.7	KMS Lookup request	140
D.2.8	KMS Redirect Upload.....	140
D.3	KMS responses.....	141
D.3.1	General	141
D.3.2	KMS certificates.....	141
D.3.2.1	Description.....	141
D.3.2.2	Fields	142
D.3.2.3	User IDs	142
D.3.3	User Key Provision	142
D.3.3.1	Description.....	142
D.3.3.2	Fields	143
D.3.4	Example KMS response XML	143
D.3.4.1	Example KMSInit XML	143
D.3.4.2	Example KMSKeyProv XML.....	144
D.3.4.3	Example KMSCertCache XML.....	146
D.3.5	KMS response XML schema.....	148
D.3.5.1	Base XML schema.....	148
D.3.5.2	Security Extension to KMS response XML schema.....	150
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.....	152
D.4.4	Example XML schema.....	153
Annex E (normative): MIKEY message formats for media security		155
E.1	General aspects.....	155
E.1.1	Introduction	155

E.1.2	MIKEY common fields	155
E.1.3	Crypto Session Identifiers	156
E.2	MIKEY message structure for GMK distribution	156
E.2.1	General	156
E.2.2	Default SRTP security profile for GMK use	156
E.3	MIKEY message structure for PCK distribution.....	157
E.3.1	General.....	157
E.3.2	Default SRTP security profile for PCK.....	158
E.3.3	Providing a SRTP security profile for PCK use	158
E.4	MIKEY message structure for CSK and MuSiK distribution	158
E.4.1	General	158
E.4.2	Default SRTCP security profile for CSK and MuSiK.....	159
E.4.3	Providing a SRTCP security profile for CSK or MuSiK.....	159
E.5	MIKEY general extension payload to support 'SAKKE-to-self'	159
E.6	MIKEY general extension payload to encapsulate parameters associated with a key	160
E.6.1	General	160
E.6.2	Void.....	161
E.6.3	MC group IDs.....	161
E.6.4	Activation time	162
E.6.5	Text	162
E.6.6	Reserved.....	162
E.6.7	Void.....	162
E.6.8	Void.....	162
E.6.9	Status	162
E.6.10	Expiry time.....	162
E.6.11	Key Type.....	162
E.7	Hiding identities within MIKEY messages.....	163
Annex F (normative): Key derivation and hash functions.....		164
F.1	KDF interface and input parameter construction	164
F.1.1	General	164
F.1.2	FC value allocations	164
F.1.3	Calculation of the User Salt for GUK-ID generation	164
F.1.4	Calculation of keys for application data protection.....	164
F.1.5	Calculation of keys for MCDATA payload protection	165
F.2	Hash functions.....	165
F.2.1	Generation of MIKEY-SAKKE UID	165
F.2.1.1	Overview	165
F.2.1.2	Example UID	166
Annex G (normative): Key identifiers		168
Annex H (normative): Support for legacy multicast key (MKFC) and for MSCCK.....		169
H.1	General	169
H.2	MKFC Receipt	169
H.3	MSCCK Distribution.....	169
H.4	Use of multicast signalling keys (MKFC and MSCCK)	169
Annex I (normative): Signalling Proxies.....		170
I.1	Overview	170
I.2	Location of a signalling proxy.....	171
I.2.1	Overview	171
I.2.2	Deployment with an untrusted SIP Core.....	171
I.2.3	Deployment with a trusted SIP Core.....	172
I.3	Functions of a signalling proxy	173
I.3.1	Overview	173
I.3.2	Identifier modification (topology hiding)	173

I.3.3	Resilience against signalling storm.....	173
I.3.4	Client connection to a CS Proxy.....	173
I.3.5	CSK key download from a CS Proxy.....	173
I.3.6	MuSiK and MSCCK key download from a CS Proxy.....	174
I.3.7	Signalling protection by the IS Proxy.....	174
I.3.8	Creation of KMS Redirect Responses (KRRs).....	174
I.3.9	Policy enforcement.....	174

Annex J (normative): Authentication and authorisation formats175

J.1	Elements for Authenticating Requests.....	175
J.1.1	General.....	175
J.1.2	Format of an EAR.....	175
J.1.3	Format of an EAR ID.....	175
J.1.4	Format of an entity's Role ID.....	176
J.1.5	Format of an MC Entity ID.....	176
J.2	Request types and parameters.....	177
J.2.1	General.....	177
J.2.2	Request Information element.....	177
J.2.3	Request type.....	177
J.2.4	Request expiry.....	177
J.2.5	Request IDs.....	178
J.2.5.1	Format.....	178
J.2.5.2	Request ID values for privileged signalling.....	179
J.2.5.3	Request IDs for off-network signalling.....	179
J.3	Authorisation fields.....	180
J.3.1	General.....	180
J.3.2	Authorisation field names.....	180
J.3.3	Authorisation field values.....	181
J.3.3.1	General.....	181
J.3.3.2	Role authorisations.....	182
J.3.3.3	Authorisations for privileged signalling.....	182
J.3.3.4	Authorisations for off-network signalling.....	183
J.3.4	Example Authorised Identities.....	184
J.3.4.1	General.....	184
J.3.4.2	PTT User (on and off-network).....	184
J.3.4.3	Dispatcher.....	184

Annex K (informative): Non-3GPP security mechanisms.....185

K.1	General.....	185
K.2	LMR E2EE.....	185
K.2.1	General.....	185
K.2.2	Interworking E2EE keys and key management.....	185
K.2.3	Interworking E2EE media for MCPTT.....	185
K.2.4	Interworking E2EE media for MCDATA.....	185

Annex L (normative): MC Security Gateway (SeGy).....187

L.1	General.....	187
L.2	Functional model for the MC Security Gateway (SeGy).....	187
L.3	Functions of a MC Security Gateway (SeGy).....	188
L.3.1	Components of a MC Security Gateway (SeGy).....	188
L.3.2	Pseudo KMS.....	188
L.3.3	Pseudo GMS.....	188
L.3.4	Pseudo MCX Server or IS Proxy.....	189
L.3.5	Pseudo MC clients.....	189
L.4	Security procedures for the MC Security Gateway (SeGy).....	189
L.4.1	General.....	189

L.4.2 Security procedures for private communication (initiated in the protected MC system)190

L.4.3 Security procedures for private communication (initiated in the unprotected MC system)191

L.4.4 Security procedures for group communications (group homed in the protected MC system)192

L.4.5 Security procedures for group communications (group homed in the unprotected MC system)194

L.5 Interworking using a MC Security Gateway195

L.5.1 General195

L.5.2 MC Security Gateway and the IWF195

Annex M (informative): Change history197

History200

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/41797185-013c-4da2-96ab-8d2c60aa245b/etsi-ts-133-180-v15.4.0-2019-05>

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.

PREVIEW
iTech STANDARD
(standards.itih.ai)
Full standard:
<https://standards.itih.ai/catalog/standards/sist/41797185-013c-4da2-96ab-8d2c60aa245b/etsi-ts-133-180-v15.4.0-2019-05>