ETSI TS 133 180 V14.8.0 (2020-01)

TECHNICAL SPECIFICATION

LTE;
Security of the mission critical service
(3GPP TS 33.180 version 14.8.0 Release 14)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14-8-0-2020-01

Reference

RTS/TSGS-0333180ve80

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/31d5df9-4d5a-48dd-a4c5-a5ecae0b63/etsi-ts-133-180-v14.8.0-2020-01

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 2020.
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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/1dc5df9-4d5a-48cd-9465-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

Contents

Intellectual Property Rights 2

Legal Notice 2

Modal verbs terminology 2

Foreword 9

1 Scope 10

2 References 10

3 Definitions and abbreviations 12
3.1 Definitions 12
3.2 Abbreviations 13

4 Overview of Mission Critical Security 13
4.1 General 13
4.2 Signalling plane security architecture 14
4.3 MC system security architecture 14
4.3.1 General 14
4.3.2 User authentication and authorisation 15
4.3.3 Identity keying of users and services 16
4.3.4 Protection of application plane signalling 16
4.3.5 Media security 17
4.3.5.1 General 17
4.3.5.2 Media security for group communications 17
4.3.5.3 Media security for private calls 19

5 Common mission critical security framework 20
5.1 User authentication and authorization 20
5.1.1 General 20
5.1.2 User authentication 21
5.1.2.1 Identity management functional model 21
5.1.2.2 User authentication framework 22
5.1.2.3 OpenID Connect (OIDC) 23
5.1.2.3.1 General 23
5.1.2.3.2 User authentication example using username/password 24
5.1.3 MCX user service authorisation 24
5.1.3.1 General 24
5.1.3.2 MCX user service authorization with MCX Server 27
5.1.3.2.1 General 27
5.1.3.2.2 Using SIP REGISTER 27
5.1.3.2.3 Using SIP PUBLISH 28
5.1.4 Inter-domain MCX user service authorization 28
5.1.4.1 General 28
5.1.4.2 Inter-domain identity management functional model 28
5.2 Key management common elements 30
5.2.1 Overview of key management 30
5.2.2 Common key distribution 31
5.2.3 Key distribution with end-point diversity 32
5.2.4 Key distribution with associated parameters 35
5.2.5 Key distribution with SAKKE-to-self payload 36
5.2.6 Key distribution with identity hiding 37
5.2.7 Key distribution across multiple security domains 38
5.2.7.1 General 38
5.2.7.2 Identification of External Security Domains 38
5.2.7.3 Using multiple security domains 39
5.3 User key management 39
5.3.1 General 39
5.3.2 Functional model for key management 39

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df0-4d5a-48c9-94c5-ae5ecac60b63/etsi-ts-133-180-v14.8.0-2020-01

5.3.3 Security procedures for key management 40
5.3.4 Provisioned key material to support end-to-end communication security 42
5.3.5 KMS Certificate 42
5.3.6 KMS provisioned Key Set 42
5.4 Key management from MC client to MC server (CSK upload) 43
5.5 Key management between MCX servers (SPK) 43
5.6 Key management for one-to-one (private) communications (PCK) 43
5.7 Key management for group communications (GMK) 44
5.7.1 General 44
5.7.2 Security procedures for GMK provisioning 44
5.7.3 Group member GMK management 45
5.8 Key management from MC server to MC client (Key download) 46
5.8.1 General 46
5.8.2 ‘Key download' procedure 46
5.9 Key management during MBMS bearer announcement 47
5.10 UE key storage and key persistence 47
5.10.1 Key storage 47
5.10.2 Key persistence 47

6 Supporting security mechanisms 48
6.1 HTTP 48
6.1.1 Authentication for HTTP-1 interface 48
6.1.2 HTTP-1 interface security 48
6.2 SIP 48
6.2.1 Authentication for SIP core access 48
6.2.2 SIP-1 interface security 48
6.3 Network domain security 49
6.3.1 LTE access authentication and security 49
6.3.2 Inter/Intra domain interface security 49

7 MCPTT and MCVideo 49
7.1 General 49
7.2 Private communications 49
7.2.1 Key management 49
7.2.2 Security procedures (on-network) 49
7.2.3 Security procedures (off-network) 51
7.2.4 First-to-answer security and key management 52
7.2.4.1 Overview 52
7.2.4.2 First-to-answer request and response 53
7.2.4.3 First-to-answer call setup with security 53
7.2.4.4 First-to-answer media protection 55
7.2.5 Ambient listening call 55
7.2.6 Ambient viewing call 55
7.2.7 Private video pull 56
7.2.7.1 One-to-one video pull 56
7.2.7.2 One-from-server video pull 56
7.2.8 Private video push 57
7.2.8.1 One-to-one video push 57
7.2.8.2 One-to-server video push 57
7.2.8.3 Remotely initiated video push 58
7.3 Group communications 59
7.3.1 General 59
7.3.2 Group creation security procedure 60
7.3.3 Dynamic group keying 60
7.3.3.1 General 60
7.3.3.2 Group regrouping security procedure (within a single MC domain) 60
7.3.3.3 Group regrouping security procedure (involving multiple MC domains) 60
7.3.4 Broadcast group call 62
7.3.5 Group-broadcast group call 62
7.3.6 Emergency group call 62
7.3.7 Imminent peril group call 63
7.3.8 Emergency Alert 63

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-a5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

7.3.9 Remotely initiated video push to group ... 63
7.4 Key derivation for media ... 65
7.4.1 Derivation of SRTP master keys for private call ... 65
7.4.2 Derivation of SRTP master keys for group media ... 65
7.5 Media protection profile ... 66
7.5.1 General ... 66
7.5.2 Security procedures for media stream protection ... 67

8 MCData ... 69
8.1 Overview ... 69
8.2 Key Management ... 70
8.3 One-to-one communications ... 71
8.4 Group communications ... 71
8.5 MCData payload protection ... 72
8.5.1 General ... 72
8.5.2 Prequisites ... 72
8.5.2.1 Prequisites for protected payloads ... 72
8.5.2.2 Prequisites for authenticated payloads ... 72
8.5.3 Key derivation for protected payloads ... 72
8.5.4 Payload protection ... 73
8.5.4.1 Format of protected payloads ... 73
8.5.4.2 Encryption of protected payloads ... 73
8.5.5 Payload authentication ... 74

9 Signalling protection ... 74
9.1 General ... 74
9.2 Key distribution for signalling protection ... 75
9.2.1 Client-Server Key (CSK) ... 75
9.2.1.1 General ... 75
9.2.1.2 Creation of the CSK ... 75
9.2.1.3 Initial 'CSK Upload' Procedure ... 75
9.2.1.4 CSK update via 'key download' ... 76
9.2.2 Multicast Signalling Key (MuSiK) ... 76
9.2.3 Signalling Protection Key (SPK) ... 77
9.3 Application signalling security (XML protection) ... 78
9.3.1 General ... 78
9.3.2 Protected content ... 78
9.3.3 Key agreement ... 79
9.3.4 Confidentiality protection using XML encryption (xmlenc) ... 79
9.3.4.1 General ... 79
9.3.4.2 XML content encryption ... 79
9.3.4.3 XML URI attribute encryption ... 80
9.3.5 Integrity protection using XML signature (xmlsig) ... 81
9.4 RTCP signalling protection (SRTCP) ... 82
9.4.1 General ... 82
9.4.2 Unicast RTCP protection between client and server ... 82
9.4.3 Multicast RTCP protection between client and server ... 83
9.4.4 Offline floor and transmission control protection ... 83
9.4.5 RTCP protection between servers ... 83
9.4.6 Key derivation for SRTCP ... 83
9.4.7 Security procedures for transmission of RTCP content ... 84
9.4.8 RTCP protection profile ... 84
9.5 MCData signalling protection ... 85
9.5.1 Key distribution for signalling protection ... 85
9.5.2 Protection of MCData application signalling payloads (XML) ... 85
9.5.3 Protection of MCData signalling payloads ... 85

Annex A (normative): Security requirements ... 86
A.1 Introduction ... 86
A.2 Configuration & service access ... 86
A.3 Group key management ... 86
A.4 On-network operation ... 86
A.5 Ambient listening ... 87

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

A.6 Data communication between MCX network entities 87
A.7 Key stream re-use 87
A.8 Late entry to group communication 87
A.9 Private call confidentiality 87
A.10 Off-network operation 88
A.11 Privacy of MCX service identities 88
A.12 User authentication and authorization 88
A.13 Inter-domain 89
A.14 MCData 90
A.15 Multimedia Broadcast/Multicast Service 90

Annex B (normative): OpenID connect profile for MCX 91

B.1 General 91

B.2 MCX tokens 91
B.2.1 ID token 91
B.2.1.1 General 91
B.2.1.2 Standard claims 91
B.2.1.3 MCX claims 91
B.2.2 Access token 92
B.2.2.1 Introduction 92
B.2.2.2 Standard claims 92
B.2.2.3 MCX claims 92

B.3 MCX client registration 92

B.4 Obtaining tokens 93
B.4.1 General 93
B.4.2 Native MCX client 93
B.4.2.1 General 93
B.4.2.2 Authentication request 93
B.4.2.3 Authentication response 95
B.4.2.4 Access token request 95
B.4.2.5 Access token response 96

B.5 Refreshing an access token 96
B.5.1 General 96
B.5.2 Access token request 97
B.5.3 Access token response 97

B.6 MCX client registration with partner IdM service 98

B.7 Obtaining an access token from a partner domain 98
B.7.1 Overview 98
B.7.2 Token Exchange Request 99
B.7.3 Token Exchange Response 100
B.7.4 Token Request 100
B.7.5 Token Response 102

B.8 Security tokens 102

B.9 Access tokens for partner services 103

B.10 Using the token to access MCX resource servers 103

B.11 Token validation 103
B.11.1 ID token validation 103
B.11.2 Access token validation 103
B.11.3 Security token validation 103

B.12 Token revocation 103

B.13 IdMS interface security 103

Annex C (informative): OpenID connect detailed flow 105

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

C.1 Detailed flow for MC user authentication and registration using OpenID Connect 105
C.2 Detailed flow for inter-domain MC user service authorization using OpenID Connect token exchange 106

Annex D (Normative): KMS provisioning messages 109
D.1 General aspects 109
D.2 KMS requests 109
D.3 KMS responses 110
D.3.1 General 110
D.3.2 KMS certificates 110
D.3.2.1 Description 110
D.3.2.2 Fields 111
D.3.2.3 User IDs 111
D.3.3 User Key Provision 111
D.3.3.1 Description 111
D.3.3.2 Fields 112
D.3.4 Example KMS response XML 112
D.3.4.1 Example KMSInit XML 112
D.3.4.2 Example KMSKeyProv XML 113
D.3.4.3 Example KMSCertCache XML 115
D.3.5 KMS response XML schema 117
D.3.5.1 Base XML schema 117
D.3.5.2 Security Extension to KMS response XML schema 120

Annex E (normative): MIKEY message formats for media security 121
E.1 General aspects 121
E.1.1 Introduction 121
E.1.2 MIKEY common fields 121
E.1.3 Crypto Session Identifiers 121
E.2 MIKEY message structure for GMK distribution 122
E.2.1 General 122
E.2.2 Default SRTP security profile for GMK use 122
E.3 MIKEY message structure for PCK distribution 123
E.3.1 General 123
E.3.2 Default SRTP security profile for PCK 123
E.3.3 Providing a SRTP security profile for PCK use 124
E.4 MIKEY message structure for CSK and MuSiK distribution 124
E.4.1 General 124
E.4.2 Default SRTCP security profile for CSK and MuSiK 125
E.4.3 Providing a SRTCP security profile for CSK or MuSiK 125
E.5 MIKEY general extension payload to support 'SAKKE-to-self' 125
E.6 MIKEY general extension payload to encapsulate parameters associated with a key 126
E.6.1 General 126
E.6.2 Void 127
E.6.3 MC group IDs 127
E.6.4 Activation time 128
E.6.5 Text 128
E.6.6 Reserved 128
E.6.7 Void 128
E.6.8 Void 128
E.6.9 Status 128
E.6.10 Expiry time 128
E.6.11 Key Type 128
E.7 Hiding identities within MIKEY messages 129

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11de5df9-4d5a-48ed-94c8-ae5ecac60b63/etsi-ts-133-180-v14.8.0-2020-01

Annex F (normative): Key derivation and hash functions 130

F.1 KDF interface and input parameter construction 130
F.1.1 General 130
F.1.2 FC value allocations 130
F.1.3 Calculation of the User Salt for GUK-ID generation 130
F.1.4 Calculation of keys for application data protection 130
F.1.5 Calculation of keys for MCData payload protection 131

F.2 Hash functions 131
F.2.1 Generation of MIKEY-SAKKE UID 131
F.2.1.1 Overview 131
F.2.1.2 Example UID 132

Annex G (normative): Key identifiers 134

Annex H (normative): Support for legacy multicast key (MKFC) and for MSCCK 135
H.1 General 135
H.2 MKFC Receipt 135
H.3 MSCCK Distribution 135
H.4 Use of multicast signalling keys (MKFC and MSCCK) 135

Annex I (informative): Change history 136

History 137

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

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)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

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 (MCData). 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 MCData 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) over LTE; 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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-405a-48ed-94c3-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01

[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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11dc5df9-4dda-48ed-9465-ae5dae600663/etsi-ts-133-180-v14.8.0-2020-01

[45] IETF RFC 7521: “Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants”.

[46] IETF RFC 7523: “JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants”.

[47] 3GPP TS 22.280: " Mission Critical Services Common Requirements; Stage 1".

[48] Void.

[49] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification."

[50] 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification. "

[51] IETF RFC 3711 Errata ID 3712, https://www.rfc-editor.org/errata/eid3712.

[52] IANA: "Multimedia Internet KEYing (MIKEY) Payload Name Spaces", https://www.iana.org/assignments/mikey-payloads/mikey-payloads.xhtml.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Authorised Identity: An application identity given to an authorised user or network entity (e.g. MC Service ID) containing authorisation information.

External KMS: The KMS which is the root of trust for a specific External Security Domain.

External Security Domain: A security domain that the user is not a member of, but with which the user may communicate.

Floor: Floor(x) is the largest integer smaller than or equal to x.

Home KMS: The KMS that is the root of trust of the Home Security Domain.

Home Security Domain: The MCX user's primary security domain.

Identity Management Domain: The MC clients and MC functions that share an Identity Management Server (IdMS). To be specific, the MC clients request access tokens from the same primary IdMS, and the MC functions accept access tokens from this IdMS.

KMS Certificate: A certificate containing the security parameters for a security domain. This is required to support identity-based cryptography and differs from X.509 certificates used for traditional PKI. See Annex D.3.1 for details.

KMS URI: A unique identifier for a security domain, or equivalently, a logical KMS.

MCX: Mission critical services where “MCX” may be substituted with the term “MCPTT”, “MCVideo”, “MCData”, or any combination thereof.

Partner domain: A secondary MC domain which may support MC services for MC users who are home to a different MC domain. See also External Security Domain.

Primary domain: The “home” MC domain where MC users receive their primary identity management and MC services. See also Home Security Domain.

Security Domain: A security domain is a group of MCX users who share common security requirements and policies for their communications. From a technical perspective, users within a security domain share a KMS and KMS certificate. MCX users may be members of one or more security domains.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/11ec5e90-4d5a-48cd-94c5-ae5ecae60b63/etsi-ts-133-180-v14.8.0-2020-01