ETSI TS 133 180 V14.13.0 (2026-02)

TECHNICAL SPECIFICATION

LTE;
Security of the Mission Critical (MC) service
(3GPP TS 33.180 version 14.13.0 Release 14)

Reference
RTS/TSGS-0333180ved0

Keywords
5G,LTE

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

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 at 3GPP to ETSI numbering cross-referencing.

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

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the security architecture, 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".

[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".

[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.

3.2 Abbreviations

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

CMS	Configuration Management Server
CS	Crypto Session
CSB-ID	Crypto Session Bundle Identifier
CSC	Common Services Core
CSK	Client-Server Key
CSK-ID	Client-Server Key Identifier
GBA	Generic Bootstrapping Architecture
GMK	Group Master Key
GMK-ID	Group Master Key Identifier
GMS	Group Management Server
GUK-ID	Group User Key Identifier
IdM	Identity Management
IdMS	Identity Management Server
JSON	JavaScript Object Notation
JWS	JSON Web Signature
JWT	JSON Web Token
KDF	Key Derivation Function
KFC	Key For Control Signalling
KFC-ID	Key for Floor Control Identifier
KMS	Key Management Server
MBCP	Media Burst Control Protocol
MCData	Mission Critical Data
MCPTT	Mission Critical Push to Talk
MCVideo	Mission Critical Video
MCX	Mission Critical Services
MKFC	Multicast Key for Floor Control
MSCCK	MBMS subchannel control key
MSRP	Message Session Relay Protocol
MuSiK	Multicast Signalling Key
MKI	Master Key Identifier
NGMI	Next Generation Mobile Intelligence
NTP	Network Time Protocol
NTP-UTC	Network Time Protocol – Coordinated Universal Time
OIDC	OpenID Connect
PCK	Private Call Key
PCK-ID	Private Call Key Identifier
PKCE	Proof Key for Code Exchange
PSK	Pre-Shared Key
SEG	Security Gateway
SPK	Signalling Protection Key
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSRC	Synchronization Source
TBCP	Talk Burst Control Protocol
TGK	Traffic Generating Key
TrK	KMS Transport Key
UID	User Identifier for MIKEY-SAKKE (referred to as the 'Identifier' in RFC 6509 [11])
XPK	XML Protection Key

4 Overview of Mission Critical Security

4.1 General

The mission critical security architecture defined in this document is designed to meet the security requirements defined in Annex A. The security architecture provides signalling and application plane security mechanisms to protect metadata and communications used as part of the MC service. The following signalling plane security mechanisms are used by the MC service:

- Protection of the signalling plane used by the MC Service, defined in clause 6.1 and 6.2.
- Protection of inter/intra domain interfaces, defined in clause 6.3.

The following application plane security mechanisms are used by the MC service:

- Authentication and authorisation of users to the MC Service, defined in clause 5.1.
- Protection of sensitive application signalling within the MC Service, defined in clause 9.
- Security of RTCP (e.g. floor control, transmission control) within the MC Service, defined in clause 9.
- Security of data signalling within the MCData Service, defined in clause 8.
- End-to-end security of user media within the MC Service. Defined in clause 7 for MCPTT and MCVideo services and defined in clause 8 for the MCData service.

Security mechanisms in the signalling and application plane are independent of each other, but may both be required for a secure MC system.

4.2 Signalling plane security architecture

Within a MC system, signalling plane security protects the interfaces used by the MC application. Figure 4.2-1 provides an overview of these interfaces.

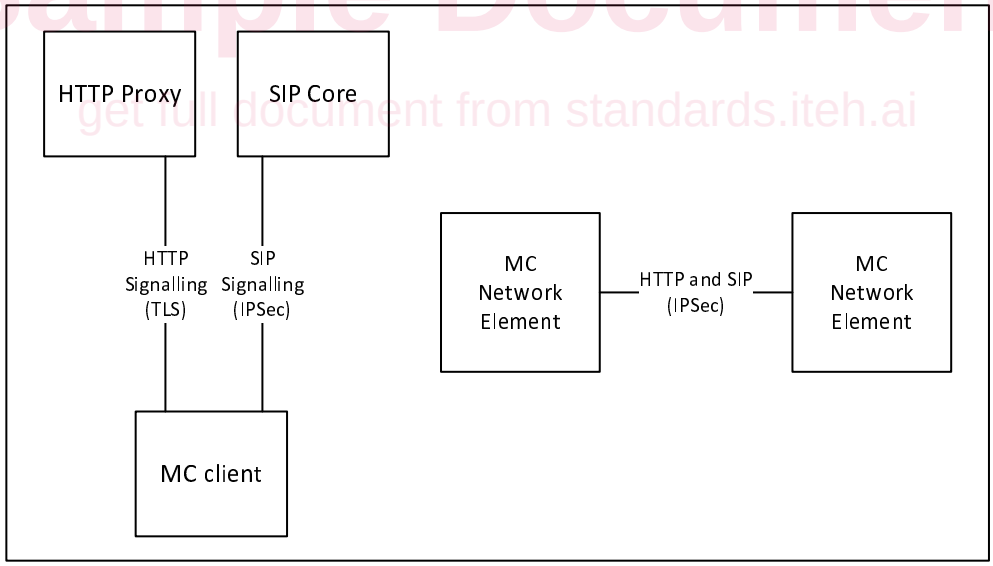

Figure 4.2-1: Signalling plane security architecture

Signalling from the MC client is passed over both HTTP and SIP. The signalling plane security mechanisms for client to server interfaces and between network elements are defined in clause 6.

4.3 MC system security architecture

4.3.1 General

The MC system security architecture provides protection both between MC clients, between the MC client and the MC domain, and also between MC domains. MC system security on the client is bound to the MC user associated with the