ETSI TS 133 179 V13.9.0 (2019-07)

TECHNICAL SPECIFICATION

LTE;
Security of Mission Critical Push To Talk (MCPTT) over LTE
(3GPP TS 33.179 version 13.9.0 Release 13)

Reference
RTS/TSGS-0333179vd90

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

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.

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 push to talk (MCPTT) service. The architecture includes mechanisms for authentication, protection of MCPTT signalling and protection of MCPTT media. Security for both MCPTT group calls and MCPTT private calls operating in on-network and off-network modes of operation is specified.

The functional architecture for MCPTT is defined in 3GPP TS 23.179 [2], the corresponding service requirements are defined in 3GPP TS 22.179 [3].

The MCPTT 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 security features may not be applicable to MCPTT 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 23.179: "Functional architecture and information flows to support mission critical communication services; 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] Void.

[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] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC".

[37] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[38] IETF RFC 2392: "Content-ID and Message-ID Uniform Resource Locators".

[39] 3GPP TS 24.380: " Mission Critical Push To Talk (MCPTT) media plane control; Protocol specification".

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

[41] 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].

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

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].

CSC	Common Services Core
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
KMS	Key Management Server
MBCP	Media Burst Control Protocol
MCPTT	Mission Critical Push to Talk
MKI	Master Key Identifier
MSCCK	MBMS subchannel control key
OIDC	OpenID Connect
PCK	Private Call Key
PCK-ID	Private Call Key Identifier
PSK	Pre-Shared Key
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSRC	Synchronization Source
TBCP	Talk Burst Control Protocol
TrK	KMS Transport Key
UID	User Identifier for MIKEY-SAKKE (referred to as the 'Identifier' in RFC 6509 [11])

4 Overview of MCPTT security

4.1 General

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

- Protection of the signalling plane used by the MCPTT Service, defined in clause 6.
- Protection of inter/intra domain interfaces, defined in clause 8.

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

- Authentication and authorisation of users to the MCPTT Service, defined in clause 5.
- Protection of sensitive application signalling within the MCPTT Service, defined in clause 9.

- Security of floor control within the MCPTT Service, defined in clause 7.
- End-to-end security of user media within the MCPTT Service, also defined in clause 7.

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

4.2 Signalling plane security architecture

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

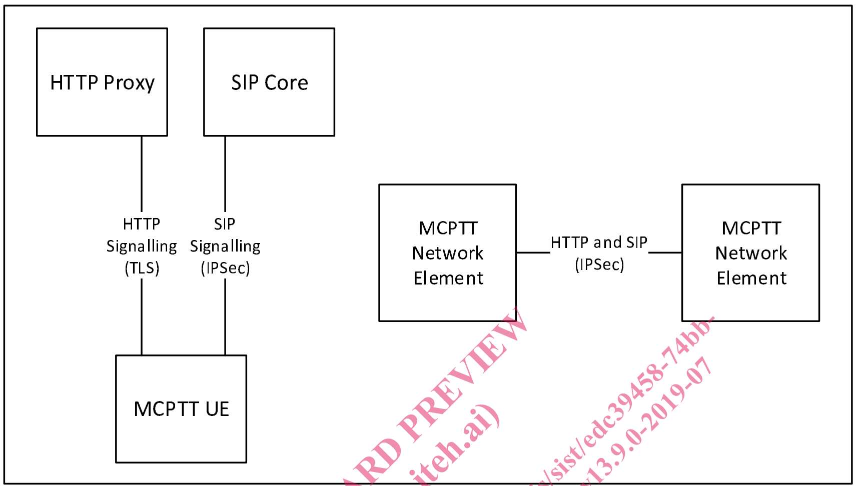

Figure 4.2-1: Signalling plane security architecture

MCPTT signalling from the UE is passed over both HTTP and SIP. The signalling plane security mechanisms for UE to Server interfaces are defined in clause 6. Additionally, MCPTT data is passed between MCPTT network elements, either inter or intra MCPTT domain. The security mechanism for protecting data between MCPTT network elements is defined in clause 8.

4.3 Application plane security architecture

4.3.1 General

Application plane security provides protection both between MCPTT clients, between the MCPTT client and the MCPTT domain, and also between MCPTT domains. Application plane security on the client is bound to the MCPTT user associated with the client and not to the MCPTT UE. Consequently, user authentication and authorisation to the MCPTT domain is required prior to access to the majority of MCPTT services.

Application plane signalling security allows protection of MCPTT-specific signalling from non-MCPTT entities (including the SIP core). Application plane signalling security is applied from the MCPTT client to the client's primary MCPTT domain. It may also be applied between MCPTT domains.

Media security allow protection of MCPTT media within the MCPTT system. It is applied end-to-end between MCPTT clients. It is a configuration option whether MCPTT network entities, including the MCPTT Server is able to access the content of MCPTT media.

Additionally, signalling plane protection is applied to all HTTP and SIP connections into the MCPTT domain. While signalling plane protection and signalling plane entities are not shown in this subclause, including the SIP core and HTTP proxy, it is assumed that signalling plane protection mechanisms are in use.

4.3.2 User authentication and authorisation

Prior to connecting to the MCPTT domain, the MCPTT user application requires a 'token' authorising its access to MCPTT services. To obtain authorisation token(s), the MCPTT user application authenticates the MCPTT user to an Identity Management Server which provides the authorisation token.

The authorisation token is provided to MCPTT network entities, such as the MCPTT Server, over an MCPTT signalling interface (either a HTTP interface or SIP interface). The MCPTT network entity will provide access to MCPTT services based upon the token provided.

The architecture for user authentication and authorisation is shown in Figure 4.3.2-1.

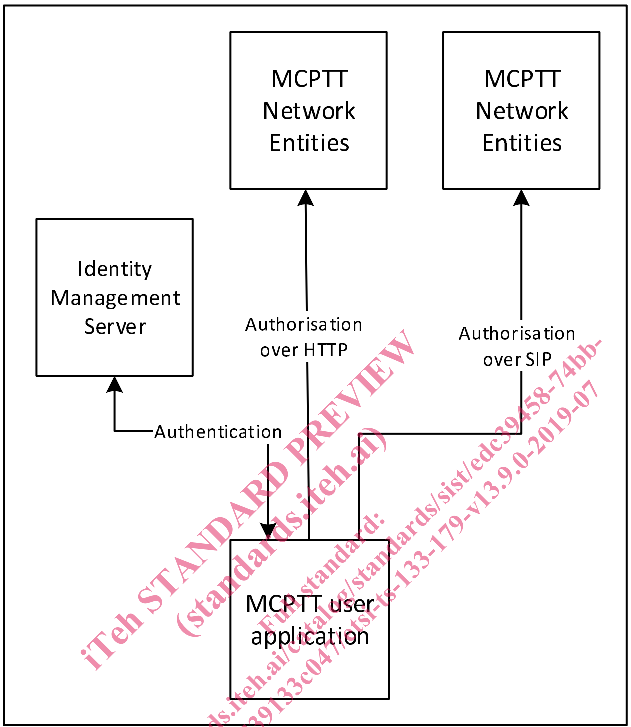

Figure 4.3.2-1: User authentication and authorisation

While not shown in Figure 4.3.2-1, authorisation occurs over HTTP or SIP and hence uses signalling plane protection to encrypt HTTP to a HTTP proxy and to encrypt SIP to a SIP core.

The mechanism to perform user authentication and authorisation is defined in clause 5.

4.3.3 Identity keying of users and services

Once a MCPTT client has obtained user authorisation to access the MCPTT domain, the client may obtain key material associated with the user's identity using the authorisation token. Identity keys are required to support key distribution for application signalling, floor control and media. Identity key material is obtained via an HTTP request to a Key Management Server as shown in Figure 4.3.3-1.

Identitiy keying is repeated periodically (e.g. monthly). This ensures that user identities are regularly verified and that users that are no longer part of the MCPTT domain are removed from the system.