ETSI TS 137 579-2 V17.0.0 (2025-02)

LTE;
5G;
Mission Critical (MC) services;
Part 2: Mission Critical Push To Talk (MCPTT)
User Equipment (UE) Protocol conformance specification
(3GPP TS 37.579-2 version 17.0.0 Release 17)

Reference
RTS/TSGR-0537579-2vh00

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.

The present document is part 1 of a multi-part deliverable covering conformance test specification for Mission Critical Services consisting of:

3GPP TS 37.579-1 [2]: "Mission Critical (MC) services; Part 1: Common test environment" (the present document)

3GPP TS 37.579-2: "Mission Critical (MC) services; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification"

3GPP TS 37.579-4 [4]: "Mission Critical (MC) services; Part 4: Test Applicability and Implementation Conformance Statement (ICS)"

3GPP TS 37.579-5 [5]: "Mission Critical (MC) services; Part 5: Abstract test suite (ATS)"

3GPP TS 37.579-6 [37]: "Mission Critical (MC) services: Mission Critical Video (MCVideo) User Equipment (UE) Protocol conformance specification"

3GPP TS 37.579-7 [38]: "Mission Critical (MC) services; Part 7: Mission Critical Data (MCData) User Equipment (UE) Protocol conformance specification"

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the protocol conformance testing for testing a MCPTT Client for compliance to the Mission Critical Push To Talk (MCPTT) over LTE protocol requirements defined by 3GPP.

In particular the present document contains:

- the overall test structure;
- the test configurations;
- the conformance requirement and reference to the core specifications;
- the test purposes; and
- a brief description of the test procedure, the specific test requirements and short message exchange table.

The present document is valid for MCPTT Clients implemented according to 3GPP releases starting from Release 13 up to the Release indicated on the cover page of the present document.

The following information relevant to testing specified in the present document could be found in accompanying specifications:

- default setting of the test parameters TS 37.579-1 [2];
- Implementation Conformance Statement (ICS) TS 37.579-4 [4] and Implementation eXtra Information for Testing (IXIT) TS 37.579-5 [5];
- the applicability of each test case TS 37.579-4 [4].

The test cases are expected to be executed through the 3GPP radio interface. The present document does not specify the protocol conformance testing for the EPS (LTE) bearers which carry the MCPTT data sent or received by the MCPTT Client and which are required to be supported by the UE in which the MCPTT Client is installed. This is defined in TS 36.523-1 [6].

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 37.579-1: "Mission Critical (MC) services; Part 1: Common test environment".

[3] Void.

[4] 3GPP TS 37.579-4: " Mission Critical (MC) services; Part 4: Test Applicability and Implementation Conformance Statement (ICS).

[5] 3GPP TS 37.579-5: "Mission Critical (MC) services; Part 5: Abstract test suite (ATS)".

[6] 3GPP TS 36.523-1: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[7] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE; Stage 1".

[8] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[9] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

[10] 3GPP TS 24.380: "Mission Critical Push To Talk (MCPTT) media plane control; Protocol specification ".

[11] 3GPP TS 24.481: "Mission Critical Services (MCS) group management; Protocol specification".

[12] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management; Protocol specification".

[13] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[14] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management; Protocol specification".

[15] 3GPP TS 33.179: " Security of Mission Critical Push To Talk (MCPTT) over LTE ".

[16] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[17] Void.

[18] Void.

[19] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[20] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[21] Void.

[22] Void.

[23] 3GPP TS 36.509: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Special conformance testing functions for User Equipment (UE)".

[24] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Common Test Environments for User Equipment (UE) Conformance Testing".

[25] OpenID Connect 1.0: "OpenID Connect Core 1.0 incorporating errata set 1", http://openid.net/specs/openid-connect-core-1_0.html.

[26] Void.

[27] Void

[28] Void.

[29] Void.

[30] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[31] Void.

[32] 3GPP TS 23.003: "Numbering, addressing and identification".

[33] 3GPP TS 33.180: "Security of the mission critical service".

[34] IETF RFC 4354 "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service"

[35] IETF RFC 4575 " A Session Initiation Protocol (SIP) Event Package for Conference State"

[36] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[37] 3GPP TS 37.579-6: "Mission Critical (MC) services; Part 6: Mission Critical Video (MCVideo) User Equipment (UE) Protocol conformance specification"

[38] 3GPP TS 37.579-7: "Mission Critical (MC) services; Part 7: Mission Critical Data (MCData) User Equipment (UE) Protocol conformance specification"

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

For the purpose of the present document, the following terms and definitions given in 3GPP TS 24.379 [9] apply:

An MCPTT user is affiliated to an MCPTT group
An MCPTT user is affiliated to an MCPTT group at an MCPTT client
Affiliation status
Group identity
In-progress emergency private call state
In-progress imminent peril group state
MCPTT client ID
MCPTT emergency alert state
MCPTT emergency group state
MCPTT emergency group call state
MCPTT emergency private call state
MCPTT emergency private priority state
MCPTT imminent peril group call state
MCPTT imminent peril group state
MCPTT private emergency alert state
MCPTT speech
Media-floor control entity
Temporary MCPTT group identity
Trusted mutual aid
Untrusted mutual aid

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.179 [7] apply:

In-progress emergency
MCPTT emergency alert
MCPTT emergency group call
MCPTT emergency state
Partner MCPTT system
Primary MCPTT system

For the purpose of the present document, the following terms and definitions given in 3GPP TS 24.380 [10] apply:

MBMS subchannel

For the purpose of the present document, the following terms and definitions given in 3GPP TS 23.179 [8] apply:

Pre-selected MCPTT user profile

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

ECGI	E-UTRAN Cell Global Identification
FFS	For Further Study
ICS	Implementation Conformance Statement
IPEG	In-Progress Emergency Group
IPEPC	In-Progress Emergency Private Call
IPIG	In-Progress Imminent peril Group
IUT	Implementation Under Test
IXIT	Implementation eXtra Information for Testing
MBMS	Multimedia Broadcast and Multicast Service
MBSFN	Multimedia Broadcast multicast service Single Frequency Network
MCPTT	Mission Critical Push To Talk
MCPTT group ID	MCPTT group IDentity
MEA	MCPTT Emergency Alert
MEG	MCPTT Emergency Group
MEGC	MCPTT Emergency Group Call
MEPC	MCPTT Emergency Private Call
MEPP	MCPTT Emergency Private Priority
MES	MCPTT Emergency State
MIME	Multipurpose Internet Mail Extensions
MIG	MCPTT Imminent peril Group
MIGC	MCPTT Imminent peril Group Call
MONP	MCPTT Off-Network Protocol
MPEA	MCPTT Private Emergency Alert
NAT	Network Address Translation
PLMN	Public Land Mobile Network
QCI	QoS Class Identifier
RTP	Real-time Transport Protocol
SAI	Service Area Identifier
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS	System Simulator
SSRC	Synchronization SouRCe
TGI	Temporary MCPTT Group Identity
TMGI	Temporary Mobile Group Identity
TP	Transmission Point
TP	Test Purpose
UE	User Equipment
URI	Uniform Resource Identifier

4 General

4.1 Test methodology

4.1.1 Testing of optional functions and procedures

Any function or procedure which is optional, may be subject to a conformance test if it is implemented in the MCPTT Client.

A declaration by the MCPTT Client supplier (to use the Implementation Conformance Statement (ICS) proforma specified in TS 37.579-4 [4]) is used to determine whether an optional function/procedure has been implemented.

4.1.2 Test interfaces and facilities

Detailed descriptions of the MCPTT Client test interfaces and special facilities for testing are provided in 3GPP TS 36.509 [23].

4.2 Implicit testing

For some 3GPP MCPTT protocol features conformance is not verified explicitly in the present document. This does not imply that correct functioning of these features is not essential, but that these are implicitly tested to a sufficient degree in tests which are not explicitly dedicated to test the feature.

4.3 Repetition of tests

As a general rule, the test cases specified in the present document are highly reproducible and do not need to be repeated unless otherwise stated.

4.4 Handling of differences between conformance requirements in different releases of cores specifications

The conformance requirements which determine the scope of each test case are explicitly copy-pasted from relevant core specifications in the especially dedicated for this clause of each test with the title 'Conformance requirements'.

NOTE: When in the copy/pasted text there are references to other specifications the reference numbers will not match the reference numbers used in the present document. This approach has been taken in order to allow easy copy and then search for conformance requirements in those specifications.

When differences between conformance requirements in different releases of the cores specifications have impact on the Pre-test conditions, Test procedure sequence or/and the Specific message contents, the Conformance requirements related to different releases are specified separately with clear indication of the Release of the spec from which they were copied.

When there is no Release indicated for a conformance requirement text, this should be understood either as the Conformance requirements in the latest version of the spec with release = the TC Applicability release (which can be found in TS 37.579-4 [4], Table 4-1: Applicability of tests and additional information for testing, column 'Release'), or, as the Conformance requirements in the latest version of the spec of the release when the feature was introduced to the core specs.

4.5 Reference conditions

The reference environments used by all signalling and protocol tests is specified in TS 37.579-1 [2]. Where a test requires an environment that is different, this will be specified in the test itself.

For all test cases in this document unless specified otherwise the condition MCPTT applies for all message contents.

4.6 Generic setup procedures

A set of basic generic procedures for MCPTT Client-Server communication are described in TS 37.579-1 [2]. These procedures will be used in numerous test cases throughout the present document.

5 MCPTT Client Configuration

5.1 Configuration / Authentication / User Authorisation / UE Configuration / User Profile / Key Generation

5.1.1 Test Purpose (TP)

(1)

```
with { UE (MCPTT Client) attached to EPS services }
ensure that {
  when { the MCPTT User activates an MCPTT application and requests MCPTT initialisation }
    then { UE (MCPTT Client) performs MCPTT User Authentication }
            }
```

(2)

```
with { UE (MCPTT Client) user authenticated }
ensure that {
  when { the UE (MCPTT Client) has established a secure HTTP tunnel  }
    then { UE (MCPTT Client) performs key management authorization and obtains identity management
key material }
            }
```

(3)

```
with { UE (MCPTT Client) has obtained identity management key material }
ensure that {
  when { the UE (MCPTT Client) requests user service authorization }
    then { UE (MCPTT Client) sends a user authorization request to the MCPTT Server }
            }
```

(4)

```
with { UE (MCPTT Client) authorized for user services }
ensure that {
  when { the UE (MCPTT Client) requests configuration management authorization}
    then { UE (MCPTT Client) requests subscription to multiple documents simultaneously and request
the retrieval of the MCPTT UE Configuration document, the MCPTT User Profile Configuration Document
and the MCPTT Service Configuration Document }
            }
```

(5)

```
with { UE (MCPTT Client) having obtained user configuration data }
ensure that {
  when { the UE (MCPTT Client) requests group management authorization }
    then { UE (MCPTT Client) receives the group profile including group traffic keys }
            }
```

(6)

```
with { UE (MCPTT Client) having obtained all required configuration data }
ensure that {
  when { the UE (MCPTT Client) requires to refresh its service settings }
    then { UE (MCPTT Client) sends a SIP PUBLISH request }
            }
```

5.1.2 Conformance requirements

References: The conformance requirements covered in the present TC are specified in: TR 24.980 clauses 4.2.1, 4.3.1, TS 24.482 clause 6.2.1, Annex A.2.1.2, TS 24.484 clauses 4.2.1, 4.2.2.1, 6.2.2, 6.3.1.1, 6.3.2.1, 6.3.2.2, 6.3.13.2.1, 6.3.13.2.2, TS 24.481 clauses 6.2.2.2, 6.2.3, 6.3.3.2.1, 6.3.3.2.2, 6.3.13.2.1, TS 24.379 clauses 7.2.1, 7.2.1AA, 7.2.1A, 7.2.2, 7.2.3, TS 33.180 clauses 5.1.3.1, 5.3.3, 6.1.2, Annex D.1. The. Unless otherwise stated these are Rel-14 requirements.

[TR 24.980, clause 4.2.1]

The MCPTT UE follows the SIP registration procedures defined in 3GPP TS 24.229 [4]. In addition, when the conditions for performing IMS registration in bullets 2, 3, 4, 5 and 6 in subclause L.3.1.2 of 3GPP TS 24.229 [4] evaluate to true, the MCPTT UE registers with the IMS.

[TR 24.980, clause 4.3.1]

The MCPTT UE follows the procedures defined in 3GPP TS 24.229 [4] and 3GPP TS 33.203 [7] for authentication with IMS Authentication and Key Agreement (IMS-AKA), Sec-Agree and IPSec. The MCPTT UE supports integrity protection.

[TS 24.482, clause 6.2.1]

Upon an indication from the MC service client to initiate MC service user authentication, the IdM client shall perform the user authentication procedure according to 3GPP TS 33.180 [17] with the following clarifications:

1) shall establish a TLS tunnel to the authorisation endpoint of the IdM server as specified in 3GPP TS 33.180 [17] using the configured URL of the authorisation endpoint of the IdM server as specified in the "/<x>/OnNetwork/AppServerInfo/IDMSAuthEndpoint" leaf node defined in 3GPP TS 24.483 [11] and the clarifications in annex A;

2) shall generate an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

a) shall generate an HTTP GET request method according to IETF RFC 2616 [4];

b) shall include the configured parameter IdM client id as the client_id parameter specified in 3GPP TS 33.180 [17] in the query component of the authorization endpoint's URI using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [7]; and

NOTE 1: The configuration of client_id is specified in 3GPP TS 24.483 [11].

c) shall include the remaining required parameters as specified in 3GPP TS 33.180 [17] in the query component of the authorization endpoint's URI using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [7]; and

3) shall send the HTTP GET request method towards the IdM server.

NOTE 2: The OpenID Connect 1.0 [6] specification allows for an alternative mechanism for sending the OIDC Authentication request message using an HTTP POST request method which can be used in place of steps 1, 2, and 3 above.

Upon receipt of an HTTP 200 (OK) response from the IdM server, the IdM client:

1) shall prompt the MC service user for their username and password;

NOTE 3: Other types of authentication are supported and are not defined by the OIDC specifications. 3GPP TS 33.180 [17] has defined username and password as a mandatory authentication method to be supported, hence a procedure to realize that method is included here.

2) shall generate an HTTP POST request method containing the MC service user's username and password; and

3) shall send the HTTP POST request method towards the IdM server.

Upon receipt of an OIDC Authentication Response message, the IdM client:

1) shall establish a TLS tunnel to the token endpoint of the IdM server as specified in 3GPP TS 33.180 [17] using the configured URL of the token endpoint of the IdM server as specified in the "/<x>/OnNetwork/AppServerInfo/IDMSTokenEndpoint" leaf node defined in 3GPP TS 24.483 [11] and the clarifications in annex A;

2) shall generate an OIDC Token Request message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

a) shall generate an HTTP POST request method according to IETF RFC 2616 [4]; and