ETSI TS 136 579-5 V13.5.0 (2020-04)

LTE;
Mission Critical (MC) services over LTE;
Part 5: Abstract test suite (ATS)
(3GPP TS 36.579-5 version 13.5.0 Release 13)

Reference
RTS/TSGR-0536579-5vd50

Keywords
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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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.

The present document is part 1 of a multi-part conformance test specification for Mission Critical Push To Talk (MCPTT) over LTE consisting of:

3GPP TS 36.579-1 [2]: "Mission Critical (MC) services over LTE; Part 1: Common test environment"

3GPP TS 36.579-2 [3]: "Mission Critical (MC) services over LTE; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification"

3GPP TS 36.579-3 [4]: "Mission Critical (MC) services over LTE; Part 3: Mission Critical Push To Talk (MCPTT) Server Application conformance specification"

3GPP TS 36.579-4 [5]: "Mission Critical (MC) services over LTE; Part 4: Test Applicability and Implementation Conformance Statement (ICS) proforma specification"

3GPP TS 36.579-5: "Mission Critical (MC) services over LTE; Part 5: Abstract test suite (ATS)" (the present specification)

In the present release of the specification only Mission Critical Push To Talk (MCPTT) services are considered. Future releases may include other Mission Critical services.

1 Scope

The present document specifies the protocol and signalling conformance testing in TTCN-3 for the Mission Critical services over LTE signalling and protocol requirements defined by 3GPP.

The following TTCN test specification and design considerations can be found in the present document:

- the test system architecture;
- the overall test suite structure;
- the test models and ASP definitions;
- the test methods and usage of communication ports definitions;
- the test configurations;
- the design principles and assumptions;
- TTCN styles and conventions;
- the partial Implementation eXtra Information for Testing (IXIT) proforma;
- the test suites.

The Abstract Test Suites designed in the document are based on the test cases specified in 3GPP TS 36.579-2 [3]. The test cases specified in 3GPP TS 36.579-3 [4] are out of scope of the present document.

The applicability of the individual test cases is specified in the test ICS proforma specification in 3GPP TS 36.579-4 [5]). Where appropriate the Abstract Test Suites belonging to the present specification may refer to other Abstract Test Suites e.g. 3GPP TS 36.523-3 [27] for test requirements related to the EPS (LTE) bearers which carry the Mission Critical services data.

The present document is valid for TTCN development for Mission Critical services clients' conformance tests according to 3GPP Releases starting from Release 13 up to the Release indicated on the cover page of the present document.

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* unless the context in which the reference is made suggests a different Release is relevant (information on the applicable release in a particular context can be found in e.g. test case title, description or applicability, message description or content).

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 36.579-1: "Mission Critical (MC) services over LTE; Part 1: Common test environment".

[3] 3GPP TS 36.579-2: "Mission Critical (MC) services over LTE; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification".

[4] 3GPP TS 36.579-3: "Mission Critical (MC) services over LTE; Part 3: Mission Critical Push To Talk (MCPTT) Server Application conformance specification".

[5] 3GPP TS 36.579-4: "Mission Critical (MC) services over LTE; Part 4: Test Applicability and Implementation Conformance Statement (ICS) proforma specification".

[6] 3GPP TS 36.523-1: "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) floor 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)".

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

[17] 3GPP TS 24.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[18] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

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

[22] ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[23] ISO/IEC 9646-7: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[24] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[25] IETF RFC 4566 (July 2006): "SDP: Session Description Protocol".

[26] 3GPP TS 26.171: "Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; General description".

[27] 3GPP TS 36.523-3: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 3: Test suites".

[28] 3GPP TS 34.229-3: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[29] ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[30] ISO/IEC 9646-7: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[31] ETSI ES 201 873: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3".

[32] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[33] 3GPP TS 27.007: "AT command set for User Equipment (UE)".

[34] IETF RFC 4661: "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering".

[34] IETF RFC 4826: "Extensible Markup Language (XML) Formats for Representing Resource Lists".

[35] W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/.

[36] W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core/.

[37] OMA - poc_listService-v1_0: "List Service".

[40] OMA - xdm_commonPolicy-V1_0: "XDM - Common Policy".

[39] OMA - xdm_extensions-v1_0: "XDM - XDM2 - Extensions".

[40] OMA - xdm_rsrclst_uriusage-v1_0: "Resource List - URI usage".

[41] W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/.

[42] W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core/.

[43] 3GPP TS 33.180: "Security of the mission critical service".

[44] IETF RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".

[45] IETF RFC 6508: "Sakai-Kasahara Key Encryption (SAKKE)".

[46] IETF RFC 6509 (February 2012): "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".

[47] IETF RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm".

[48] W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core/.

[49] IETF RFC 7515: "JSON Web Signature (JWS)".

3 Definitions, symbols 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].

In addition for the purposes of the present document, the following terms, definitions, symbols and abbreviations apply:

- such given in ISO/IEC 9646-1 [22] and ISO/IEC 9646-7 [23]

NOTE: Some terms and abbreviations defined in [22] and [23] are explicitly included below with small modification to reflect the terminology used in 3GPP.

Implementation eXtra Information for Testing (IXIT): A statement made by a supplier or implementer of an UEUT which contains or references all of the information (in addition to that given in the ICS) related to the UEUT and its testing environment, which will enable the test laboratory to run an appropriate test suite against the UEUT.

IXIT proforma: A document, in the form of a questionnaire, which when completed for an UEUT becomes an IXIT.

Protocol Implementation Conformance Statement (PICS): An ICS for an implementation or system claimed to conform to a given protocol specification.

Protocol Implementation eXtra Information for Testing (PIXIT): An IXIT related to testing for conformance to a given protocol specification.

3.2 Symbols

No specific symbols have been identified so far.

3.3 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].

ASP	Abstract Service Primitive
ICS	Implementation Conformance Statement
IXIT	Implementation eXtra Information for Testing
MC	Mission Critical
MCPTT	Mission Critical Push To Talk
MCS	Mission Critical Services
PTC	Parallel Test Component
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SRTCP	Secure RTCP
SRTP	Secure RTP
SS	System Simulator
SSRC	Synchronization SouRCe
TC	Test Case
UE	User Equipment

4 Test system architecture

4.1 General system architecture

The architecture specified in TS 36.523-3 [27] applies to the present document.

4.2 Component architecture

The architecture specified in TS 36.523-3 [27] applies to the present document, with the exception that only one RAT, E-UTRAN, is within the scope of the present document.

5 Test models

5.1 MCPTT over LTE

5.1.1 MCPTT Client on-network test model

The MCPTT Client on-network test model is depicted in figure 5.1.1-1. The test model consists of an IMS component and an HTTP component, on top of the multi-testers test model (E-UTRA) specified in TS 34.229-3 [28]. These parallel test components (PTCs) handle the IMS and HTTP signalling asynchronously.

The IMS PTC controls the IPCanEmu and the IP PTC. IPCanEmu is responsible for handling the E-UTRA cell(s) configuration in the SS as well as the E-UTRA/EPC level signalling and related procedures. The IP PTC controls the IP related configurations. IPCanEmu and IP PTC interface to the SS according to TS 36.523-3[27]. In addition, the IMS PTC interfaces to the SS via a new port, SRTP, to support configuration of SRTP/SRTCP security in the SS and transport of Floor Control messages, specified in TS 24.380 [10], from / to TTCN.

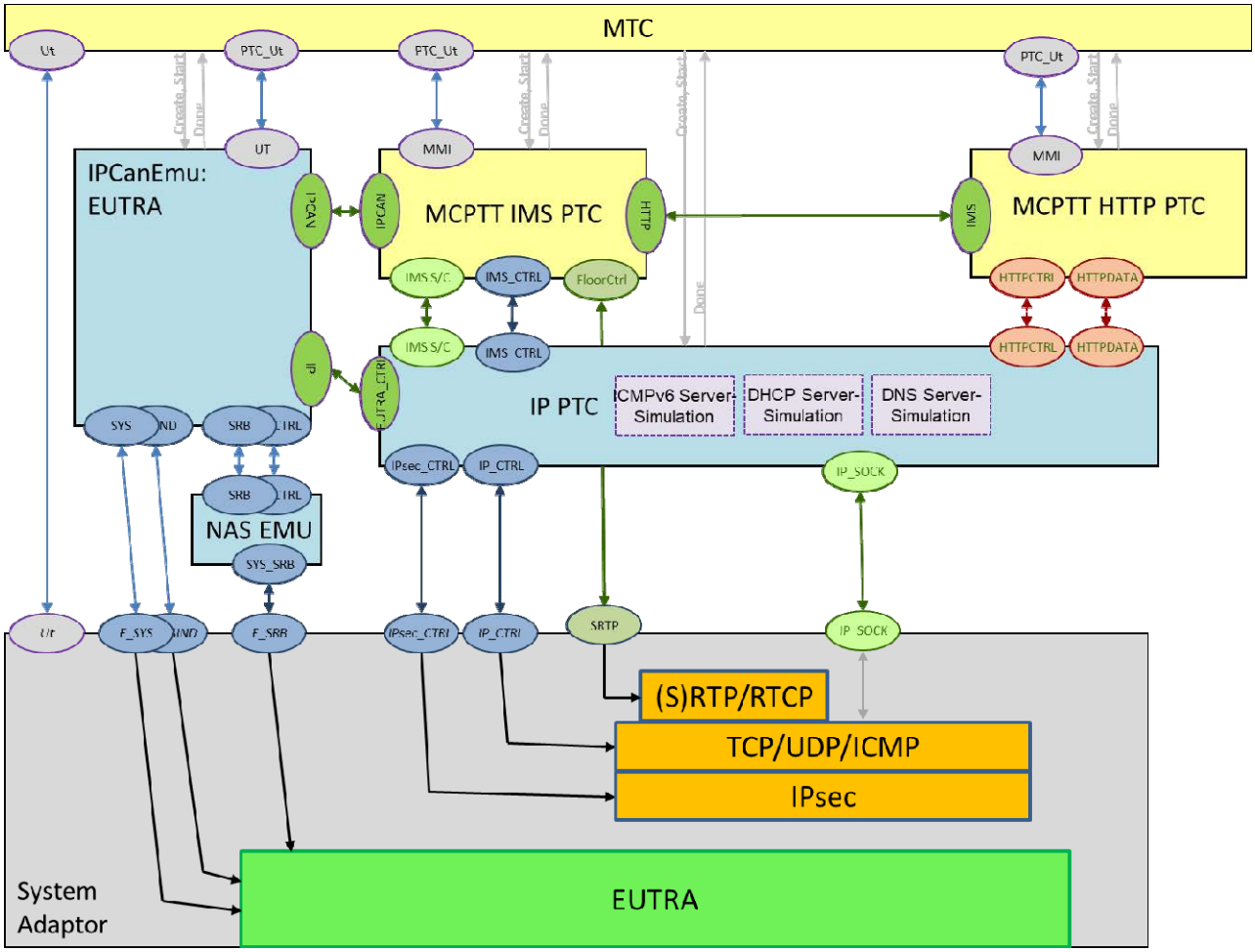

Figure 5.1.1-1: MCPTT Client on-network test model over LTE

5.1.2 MCPTT Client off-network test model

This test model is not supported by the present version of the specification.

5.2 MCPTT over IP

5.2.1 MCPTT Client on-network test model

In order to facilitate testing of MCPTT signalling at the IMS and HTTP level and execute the test cases in an environment without E-UTRA components and associated hardware, a test model over IP may be used as shown below in Figure 5.2.1-1.

It consists of the same components, ports and ASPs as in the test model in subclause 5.1.1 except for the IPCanEmu EUTRA component which is replaced by a dummy one. The ASPs defined for the system ports IP_SOCK, IPsec_CTRL, IP_CTRL and SRTP are identical to those defined in subclause 5.1.1.

This test model may be considered RAT agnostic. It will setup the simulated MCPTT servers, configure the corresponding UDP, TCP, IPsec, TLS and RTP/SRTP ports and run the IMS and HTTP signalling as required by the test cases.

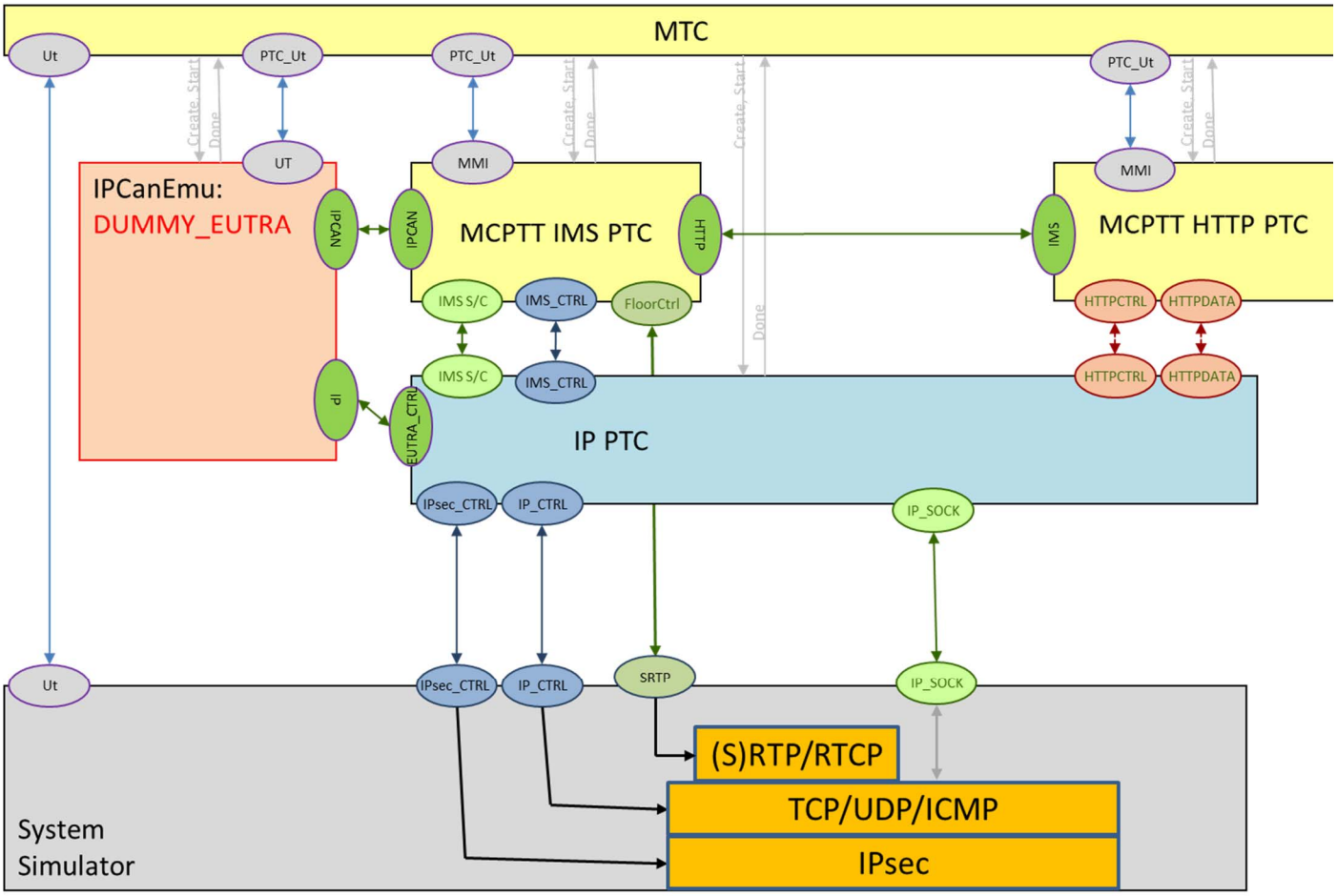

Figure 5.2.1-1: MCPTT Client on-network test model over IP

6 System interface

6.1 Upper tester interface

The Upper Tester (UT) interface is the same as defined in TS 36.523-3 [27] clause 5, with additional IMS-specific AT commands as specified in TS 34.229-3 [28] clause 8.4 and IMS-specific MMI commands as specified in TS 34.229-3 [28] annex B.2.

The following MMI commands are defined.

Table 6.1-1: MMI commands

Command	Parameters	
	Name	Value
“MCX_USERACTION”	“UserAction”	<charstring>
“MCX_USERCHECK”	“UserCheck”	<charstring>
“MCX_GROUP_CALL”	*Uri”	<charstring>

The following AT commands are applied in TTCN.

Table 6.1-2.: AT Commands

Command	Reference
AT+CAPTT	TS 27.007 [33]

6.2 Abstract system primitives

This clause specifies the abstract system primitives (ASPs) used on the system interface to configure and control the SS. The MCPTT test system interface re-uses the ASPs specified in TS 36.523-3 [27] (see clause 6 and Annex D) and TS 34.229-3 [28] (see clause 6).

7 Test methods and design considerations

7.1 MCPTT

7.1.1 MCPTT Client

7.1.1.1 Introduction

Test cases for on-network operation are described in terms of IMS, Floor Control and HTTP signalling, see TS 36.579-2 [3]. Thus, on-network test cases are written in TTCN code running on the IMS and HTTP PTCs, see figure 5.1.1-1. Floor Control messages are sent and received within the IMS PTC.

7.1.1.2 UDP/IP handling

The same mechanisms specified in TS 36.523-3 [27] for UDP/IP configuration and Routing Table configuration are applied.

For MCPTT test cases with RTP/RTCP media streams, the TTCN shall configure the loopback mode specified in TS 36.523-3 [27] subclause 4.2.4.4.

7.1.1.3 RTP/RTCP handling

The RTP/RTCP loopback mechanism specified in TS 36.523-3 [27] applies as baseline.

MCPTT test cases require SRTP (secure RTP) for their media stream, which means that the loopback mechanism needs to be enhanced: the RTP/RTCP packet in uplink needs to be decrypted with the Rx or uplink key, encrypted with the Tx or downlink key and then sent back to the UE.

TTCN controls the usage of security for SRTP/SRTCP and provides the necessary security parameters to the SS via the SRTP port. Once security has been configured by TTCN, the SS shall handle media plane encryption and decryption.

7.1.1.4 Floor Control handling

MCPTT requires that Floor Control messages are made available and handled in TTCN as structured messages.

The TTCN configures the SS, via the SRTP port, to setup the dedicated UDP media port for floor control which was negotiated via SDP at call setup and also to set encryption keys for SRTP if secure RTP has been negotiated.

The SRTP system interface is defined in Annex C.

7.1.1.5 SS pseudo-algorithm

The following summarizes the requirements on the SS with regards to RTP / RTCP / Floor Control handling within the SS:

- Uplink direction:
  - Upon reception of an SRTP/SRTCP packet, the SS shall extract the UDP payload and decrypt it using the RX crypto parameters.
  - If SSRC is configured, the SS shall overwrite its value (octets 8 to 11 for SRTP and octets 4 to 7 for SRTCP, see IETF RFC 3711 [32] clauses 3.1 and 3.4).
  - If it is a RTCP APP packet containing a Floor Control message (RTCP packet with name field = "MCPT", TS 24.380 [10] subclause 8.1.2), the SS shall extract and decode the Floor Control message and forward it to TTCN via the SRTP port.
  - Else the SS shall encrypt the packet using the Tx crypto parameters and send via UDP to the UE on the remote port.
- Downlink direction:
  - Upon reception of a Floor Control message from TTCN on the SRTP port, the SS shall encode the message, encrypt it and send it via UDP to the UE on the remote port.

8 Other SS requirements with TTCN-3 impact

8.1 Codec requirements

The requirements specified in TS 36.523-3 [27] clause 8.1 and TS 34.229-3 [28] clause 7 apply to the present document.

8.2 External function definitions

The external functions specified in TS 36.523-3 [27] clause 8.2 apply to the present document.

In addition there are the following MCX specific external functions:

TTCN-3 External Function		
Name	**fx_SAKKE_GeneratePublicKey**	
Description	Generate KMS public key (Z_T) for SAKKE (RFC 6508 [45] clause 2.2): Z_T := [z_T]P	
Parameters	p_MasterSecret	master secret z_T
	p_ParameterSet	parameter set to be used; in general parameter set 1 is used as defined in appendix A of RFC 6509 [46] Editor's note: parameter may be removed when it is clear that parameter set 1 shall always be used
Return Value	octetstring	

TTCN-3 External Function		
Name	**fx_SAKKE_GenerateRSK**	
Description	Generate receiver secret key (RSK) for SAKKE (RFC 6508 [45] clause 2.2): RSK := [(a + z_T)^-1]P with 'a' being the identifier (UID) corresponding to the receiver's URI	
Parameters	p_MasterSecret	master secret z_T
	p_Identifier	UID for a given URI
	p_ParameterSet	parameter set to be used; in general parameter set 1 is used as defined in appendix A of RFC 6509 [46] Editor's note: parameter may be removed when it is clear that parameter set 1 shall always be used
Return Value	octetstring	

TTCN-3 External Function		
Name	**fx_SAKKE_EncapsulateKey**	
Description	Generate encapsulated data for SAKKE exchange according to RFC 6508 [45]	
Parameters	p_SSV	Shared secret value: Key to be exchanged; according to 33.180 [43] E.1.1: The GMK, PCK, CSK and MuSiK shall be 16 octets in length
	p_SakkePublicKey	SAKKE public key generated with fx_SAKKE_GeneratePublicKey
	p_UID	UID generated for the receiving entity's URI (in general the same URI as in IDRr payload of the MIKEY message carrying the encapsulated data)
	p_ParameterSet	parameter set to be used; in general parameter set 1 is used as defined in appendix A of RFC 6509 [46] Editor's note: parameter may be removed when it is clear that parameter set 1 shall always be used
Return Value	octetstring (16 octets)	

TTCN-3 External Function		
Name	**fx_SAKKE_ExtractKey**	
Description	Extract 16 octet key from the encapsulated date for SAKKE exchange according to RFC 6508 [45]	
Parameters	p_EncapsulatedData	encapsulated data as received in the SAKKE payload of a MIKEY message
	p_SakkeRSK	receiver secret key (RSK) for SAKKE
	p_UID	UID generated for the receiving entity's URI (should be the same URI as in IDRr payload of the MIKEY message carrying the encapsulated data
	p_ParameterSet	parameter set to be used; in general parameter set 1 is used as defined in appendix A of RFC 6509 [46] Editor's note: parameter may be removed when it is clear that parameter set 1 shall always be used
Return Value	octetstring (16 octets)	

TTCN-3 External Function		
Name	**fx_ECCSI_GenerateKPAK**	
Description	Generate KMS Public Authentication Key (KPAK) for ECCSI (RFC 6507 [44] clause 4.2): KPAK := [KSAK]G	
Parameters	p_KSAK	KMS Secret Authentication Key (KSAK): random secret non-zero integer modulo q
	p_ParameterSet	static parameters for ECCSI as according to clause 4.1 of RFC 6507 [44] Editor's note: It is not clear whether the same type of parameterset can be used to ECCSI as for SAKKE and whether the same values shall be used; parameter may be removed when it is clear which parameter set shall always be used
Return Value	octetstring	

TTCN-3 External Function		
Name	**fx_ECCSI_GenerateSskPvtPair**	
Description	Generate (SSK,PVT) Pair according to clause 5.1.1 of RFC 6507 [44]	
Parameters	p_UID	User ID
	p_KSAK	KMS Secret Authentication Key (KSAK)
	p_KPAK	KMS Public Authentication Key (KPAK)
	p_ParameterSet	static parameters for ECCSI as according to clause 4.1 of RFC 6507 [44] Editor's note: It is not clear whether the same type of parameterset can be used to ECCSI as for SAKKE and whether the same values shall be used; parameter may be removed when it is clear which parameter set shall always be used

Return Value	type record ECCSI_SskPvtPair_Type {
	octetstring SSK,
	octetstring PVT
	}	

TTCN-3 External Function		
Name	**fx_ECCSI_SignMessage**	
Description	Sign a message according to RFC 6507 [44] clause 5.2.1: return signature of the message	
Parameters	p_Message	Message to be signed
	p_KPAK	KMS Public Authentication Key (KPAK)
	p_UID	Signer's User ID
	p_SSK	Secret Signing Key
	p_PVT	Public Validation Token
	p_ParameterSet	static parameters for ECCSI as according to clause 4.1 of RFC 6507 [44] Editor's note: It is not clear whether the same type of parameterset can be used to ECCSI as for SAKKE and whether the same values shall be used; parameter may be removed when it is clear which parameter set shall always be used
Return Value	octetstring	

TTCN-3 External Function		
Name	**fx_ECCSI_VerifySignature**	
Description	Verify a signature according to RFC 6507 [44] clause 5.2.2: return true, when the signature is valid, false otherwise	
Parameters	p_Message	Message
	p_Signature	Message's signature
	p_KPAK	KMS Public Authentication Key (KPAK)
	p_UID	Signer's User ID
	p_PVT	Public Validation Token
	p_ParameterSet	static parameters for ECCSI as according to clause 4.1 of RFC 6507 [44] Editor's note: It is not clear whether the same type of parameterset can be used to ECCSI as for SAKKE and whether the same values shall be used; parameter may be removed when it is clear which parameter set shall always be used
Return Value	boolean	

TTCN-3 External Function		
Name	**fx_XML_Encrypt**	
Description	Encrypt data NOTE: the function is defined similar to openssl_encrypt and in principle it is independent from XML; nevertheless it is used for XML encrytion in context of MCX	
Parameters	p_Data	

	p_Method	type enumerated XML_EncryptionMethod_Type {
		AES_128_GCM,
		AES_256_KEY_WRAP // according to RFC 3394 [47]
		}

	p_Key	key for encryption
	p_IV	initial vector
Return Value	octetstring	

TTCN-3 External Function		
Name	**fx_MCX_XML_AddSignature**	
Description	Add XML signature to the given XML document and return resulting XML document; according to 33.180 [43] clause 9.3.5 and W3C: "XML Signature Syntax and Processing (Second Edition)" [48]: 1. The given document has a Signature element with the name of the key to be used to sign the Signature's SignedInfo 2. Object(s) to be signed: For objects which are addressed by a reference URI in the Signature's SignedInfo the DigestValue shall be generated and added to the corresponding Reference element of the Signature's SignedInfo 3. The SignedInfo shall be signed by generating the hash for the Signature's SignedInfo using the given key; this hash vulue shall be added to the Signature's SignatureValue.	
Parameters	p_XmlDocument	XML document to be signed; the document contains all inforamtion to get signed with the given key: - id(s) for the object(s) to be signed (e.g. KMS response) - SignedInfo with reference(s) to objects to be signed (URI with the object's id, DigestAlgorithm, empty DigestValue)
	p_Key	Key corresponding to the KeyName in the Signature's KeyInfo element
Return Value	charstring containing the document with all DigestValues and the signature of the SignedInfo	

TTCN-3 External Function		
Name	**fx_SHA_2**	
Description	Generic SHA-2 function	

Parameters	p_Function	type enumerated HASH_Function_Type {
		SHA_256
		// may be extended e.g SHA_224 etc.
		}

	p_Data	
Return Value	octetstring (representing 256 bits for SHA-256, 224 bits for SHA-224, ...)	

TTCN-3 External Function		
Name	**fx_JWK_Signature**	
Description	Generate JWK signature according to RFC 7515 [49]	
Parameters	p_String	string for which the signature shall be generated

	p_Algorithm	algorithm to generate the hash:
		
		type enumerated JWK_HashAlgorithm_Type { // RFC 7515 [49]
		HS256, // HMAC SHA-256
		RS256 // RSASSA-PKCS1-v1_5 SHA-256
		}

	p_Key	
Return Value	charstring (base64url encoded signature according to RFC 7515 [49])	

9 IXIT Proforma

9.1 General

This partial IXIT proforma contained in the present document is provided for completion, when the related Abstract Test Suite is to be used against the Implementation Under Test (IUT).

Text in italics is a comment for guidance for the production of an IXIT, and is not to be included in the actual IXIT.

The completed partial IXIT will normally be used in conjunction with the completed ICS, as it adds precision to the information provided by the ICS.

9.2 MCPTT

9.2.1 MCPTT Client PIXIT

Table 9.2.1-1: MCPTT Client Common PIXIT

Parameter Name	Parameter Type	Default Value	Supported Values	Description
Client relevant IXIT				
px_MCPTT_Client_A_ID	charstring	"mcptt-client-A@mcptt-op.gov"		The URI of the MCPTT client which is installed on the implementation under test. The MCPTT client will assign this ID when the Client communicate for the first time with the MCPTT Server and will retain it unless factory reset is done.
px_MCPTT_Client_B_ID	charstring	"mcptt-client-B@mcptt-op.gov"		The URI of the MCPTT client which is to be simulated by the SS.
Users relevant IXIT				
px_MCPTT_User_A_ID	charstring	"mcptt-user-A-id@mcptt-op.gov"		MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_A_Profile_Name	charstring	"mcptt-user-A-Profile-Name"		Profile name for the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_A_Alias	charstring	"mcptt-user-A-alias"		Alphanumeric alias of MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_A_ParticipantType	charstring	"first responder"		Participant type of the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_A_Organization	charstring	"mcptt-op.gov"		Indicates the organization the MCPTT user belongs to. Ref. TS 24.483 [13]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCX_DomainName_Organization_A	charstring	"mcptt-op.gov"		Domain name of the organization the user belongs to.
px_MCPTT_User_A_username	charstring	"MCPTT#U01"		UE's User username used for user authentication
px_MCPTT_User_A_password	charstring	"psw@MCPTT&7"		UE's User password used for user authentication
px_MCPTT_UserDecryptKey_name	charstring	“tk.12.userA_decrypt@mcptt-op.gov”		Name of the key being used to cipher the SAKKE "Receiver Secret Key". in the KMS Key Set.
px_MCPTT_UserDecryptKey_value	bitstring			Value of the key being used to cipher the SAKKE "Receiver Secret Key" in the KMS Key Set
px_MCPTT_UserSigningKeySSK_name	charstring	“tk.12.userA_sign@mcptt-op.gov”		Name of the key being used to cipher the ECCSI private Key, "SSK". in the KMS Key Set
px_MCPTT_UserSigningKeySSK_value	bitstring			Value of the key being used to cipher the ECCSI private Key, "SSK", in the KMS Key Set
px_MCPTT_UserPubTokenPVT_name	charstring	“tk.12.userA_pub@mcptt-op.gov”		Name of the key being used to cipher the ECCSI public validation token, "PVT". in the KMS Key Set
px_MCPTT_UserPubTokenPVT_value	bitstring			Value of the key being used to cipher the ECCSI public validation token, "PVT", in the KMS Key Set
px_MCPTT_SigningKey_name	charstring	“tk.12.userA_signing@mcptt-op.gov”		Name of the key being used to sign the kmsResponse carrying the key set
px_MCPTT_SigningKey_value	bitstring			Value of the key being used to sign the kmsResponse carrying the key set

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCPTT_User_B_ID	charstring	"mcptt-user-B-id@mcptt-op.gov"		MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_B_Profile_Name	charstring	"mcptt-user-B-Profile-Name"		Profile name for the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_B_Alias	charstring	"mcptt-user-B-alias"		Alphanumeric alias of MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_B_ParticipantType	charstring	"first responder"		Participant type of the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_B_Organization	charstring	"mcptt-op.gov"		Indicates the organization the MCPTT user belongs to. Ref. TS 24.483 [13]. Editor's note: To be removed.
px_MCPTT_User_C_ID	charstring	"mcptt-user-C-id@mcptt-op.gov"		MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_C_Profile_Name	charstring	"mcptt-user-C-Profile-Name"		Profile name for the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_C_Alias	charstring	"mcptt-user-C-alias"		Alphanumeric alias of MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_C_ParticipantType	charstring	"first responder"		Participant type of the MCPTT user. Ref. TS 24.483 [13].
px_MCPTT_User_C_Organization	charstring	"mcptt-op.gov"		Indicates the organization the MCPTT user belongs to. Ref. TS 24.483 [13]. Editor's note: To be removed.
Groups relevant IXIT				
px_MCPTT_Group_A_ID	charstring	"mcptt-group-A@mcptt-op.gov"		Group ID for a group. Value is an "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id. Ref. TS 24.483 [13].
px_MCPTT_Group_A_Name	charstring	"mcptt-group-A-name"		A human readable Group name for the group
px_MCPTT_Group_A_ProSeLayer2GroupID	charstring	"prose.mcptt-op-A.gov"		Indicates the Prose layer-2 group ID for the group. Ref. TS 23.303 [24].
px_MCPTT_Group_A_Owner_Organization	charstring	"mcptt-op.gov"		Indicates the group's owner organization the group belongs to. Ref. TS 24.483 [13].
px_MCPTT_Group_A_preferred_VCodec	charstring	"AMR-WB"		Preferred voice codec for the group (a RTP payload). MCPTT clients shall support the AMR-WB codec. RFC 4566 [25] TS 26.171 [26]
px_MCPTT_Group_B_ID	charstring	"mcptt-group-B@mcptt-op.gov"		Group ID for a group. Value is an "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id. Ref. TS 24.483 [13].
px_MCPTT_Group_B_Name	charstring	"mcptt-group-B-name"		A human readable Group name for the group
px_MCPTT_Group_B_ProSeLayer2GroupID	charstring	"prose.mcptt-op-B.gov"		Indicates the Prose layer-2 group ID for the group. Ref. TS 23.303 [241].
px_MCPTT_Group_B_Owner_Organization	charstring	"mcptt-op.gov"		Indicates the group's owner organization the group belongs to. Ref. TS 24.483 [13].

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCPTT_Group_B_preferred_VCodec	charstring	"AMR-WB"		Preferred voice codec for the group (a RTP payload). MCPTT clients shall support the AMR-WB codec. RFC 4566 [25] TS 26.171 [26]
px_MCPTT_Group_C_ID	charstring	"mcptt-group-C@mcptt-op.gov"		Group ID for a group. Value is an "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id. Ref. TS 24.483 [13].
px_MCPTT_Group_C_Name	charstring	"mcptt-group-C-name"		A human readable Group name for the group
px_MCPTT_Group_C_ProSeLayer2GroupID	charstring	"prose.mcptt-op-C.gov"		Indicates the Prose layer-2 group ID for the group. Ref. TS 23.303 [24].
px_MCPTT_Group_C_Owner_Organization	charstring	"mcptt-op.gov"		Indicates the group's owner organization the group belongs to. Ref. TS 24.483 [13].
px_MCPTT_Group_C_preferred_VCodec	charstring	"AMR-WB"		Preferred voice codec for the group (a RTP payload). MCPTT clients shall support the AMR-WB codec. RFC 4566 [25] TS 26.171 [26]
px_MCPTT_Group_D_ID	charstring	"mcptt-group-D@mcptt-op.gov"		Group ID for a group. Value is an "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id. Ref. TS 24.483 [13].
px_MCPTT_Group_D_Name	charstring	"mcptt-group-D-name"		A human readable Group name for the group
px_MCPTT_Group_D_ProSeLayer2GroupID	charstring	"prose.mcptt-op-D.gov"		Indicates the Prose layer-2 group ID for the group. Ref. TS 23.303 [241].
px_MCPTT_Group_D_Owner_Organization	charstring	"mcptt-op.gov"		Indicates the group's owner organization the group belongs to. Ref. TS 24.483 [13].
px_MCPTT_Group_D_preferred_VCodec	charstring	"AMR-WB"		Preferred voice codec for the group (a RTP payload). MCPTT clients shall support the AMR-WB codec. RFC 4566 [25] TS 26.171 [26]
px_MCPTT_Group_T_ID	charstring	"mcptt-group-T@mcptt-op.gov"		Group ID for a temporary group. Value is an "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id. Ref. TS 24.483 [13].
px_MCPTT_Group_T_Name	charstring	"mcptt-group-T-name"		A human readable Group name for the group
px_MCPTT_Group_T_ProSeLayer2GroupID	charstring	"prose.mcptt-op-T.gov"		Indicates the Prose layer-2 group ID for the group. Ref. TS 23.303 [241].
px_MCPTT_Group_T_Owner_Organization	charstring	"mcptt-op.gov"		Indicates the group's owner organization the group belongs to. Ref. TS 24.483 [13].
px_MCPTT_Group_T_preferred_VCodec	charstring	"AMR-WB"		Preferred voice codec for the group (a RTP payload). MCPTT clients shall support the AMR-WB codec. RFC 4566 [25] TS 26.171 [26]
Sessions relevant IXIT				

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCPTT_session_A_ID	charstring	"12345678@mcptt-server-A.mcptt-op.gov"		The URI of the MCPTT session A identity. Ref. TS 24.483 [13].
px_MCPTT_session_B_ID	charstring	"sessionB@cf-B@ims-op.net"		The URI of the MCPTT session B identity. Ref. TS 24.483 [13].
px_MCPTT_CT_call_ID	charstring	"11111111@mcptt-op.gov"		The call ID of a Client Terminated call that can be used for call identification in the SIP messages. Ref. TS 24.483 [13].
Miscellaneous IXIT				
px_MCPTT_vendor_specific_information_init_config	charstring	""		UE initial configuration vendor specific name for the application vendor, device vendor etc. Ref. TS 24.483 [13].
px_MCPTT_vendor_specific_information_config	charstring	""		UE configuration vendor specific name for the application vendor, device vendor etc. Ref. TS 24.483 [13].
px_MCPTT_vendor_specific_information_user_profile	charstring	""		User Profile vendor specific name for the application vendor, device vendor etc. Ref. TS 24.483 [13].
px_MCPTT_vendor_specific_service_conf	charstring	""		MCPTT service configuration vendor specific name for the application vendor, device vendor etc. Ref. TS 24.483 [13].
px_MCPTT_CertUri	charstring	“cert1.mcptt-op.gov”		The URI of the Certificate (this object). Ref. TS 33.179 [15]
px_MCPTT_IP_ConnectionAddressAll	charstring	"0.0.0.0"		The unicast IP address
px_MCPTT_IP_ConnectionAddressAudio	charstring	"0.0.0.0"		The media=audio plane control channel IP address. NOTE: Can be the same as the unicast IP address.
px_MCPTT_IP_ConnectionAddressApp	charstring	"0.0.0.0"		The media=application plane control channel IP address. NOTE: Can be the same as the unicast IP address.
px_MCPTT_ALL_APN	charstring	"mcptt-apn"		A single APN which the UE shall use to access each and all MCPTT relevant services including the MCPTT SIP-1 reference point, the MC common core services for the HTTP-1 reference point and the MC identity management service for the CSC-1 reference point. The APN is provided in the initial UE configuration as specified in TS 36.579-1 [2] Table 5.5.8.1-1.
px_MCX_InitialRegistration_TypeOfPDN1	MCX_Registration_PDN_Type	mcx	ims, internet, mcx	First PDN registered during initial registration (either ‘ims’ or ‘internet’ or ‘mcx’; ‘none’ is not applicable as first PDN)
px_MCX_InitialRegistration_TypeOfPDN2	MCX_Registration_PDN_Type	none	ims, internet, mcx, none	Second PDN registered during initial registration; in addition to ‘ims’ or ‘internet’ or ‘mcx’ it may be ‘none’ to indicate that there is no second PDN connectivity requested by the UE during initial registration

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCX_InitialRegistration_TypeOfPDN3	MCX_Registration_PDN_Type	none	ims, internet, mcx, none	Third PDN registered during initial registration; in addition to 'ims' or 'internet' or 'mcx' it may be 'none' to indicate that there is no third PDN connectivity requested by the UE during initial registration

9.2.2 MCPTT Server PIXIT

Table 9.2.2-1: MCPTT Server Common PIXIT

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCPTT_Server_A_URI	charstring	"mcptt-server-A@mcptt-op.gov"		The URI of the MCPTT Server which is simulated by the SS
px_MCPTT_Server_B_URI	charstring	"mcptt-server-B@mcptt-op.gov"		The URI of a second MCPTT Server which is implemented in the DUT used in MCPTT Server testing.
px_MCPTT_PCSCF_A_URI	charstring	"mcptt-p-cscf-A@mcptt-op.gov"		The URI of the P-CSCF simulated by the SS.
px_MCPTT_GMSURI	charstring	"mcptt-gms@mcptt-op.gov"		The group management service URI information which contains the public service identity for performing subscription proxy function of the GMS. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCPTT_GroupCreationXUI	charstring	"mcptt-gms@mcptt-op.gov"		Indicates the group creation XUI information for creation of groups. Ref. TS 23.003 [21].
px_MCPTT_GroupConfigDoc_URI	charstring	“xcap.mcptt-op.gov/group_config.xml”		Points to the group configuration document. Ref. TS 24.481 [11].
px_MCPTT_GMSXCAPRootURI	charstring	"xcap.mcptt-op.gov"		Indicates the group management server XCAP Root URI information. Ref. TS 23.003 [21].
px_MCPTT_CMSXCAPRootURI	charstring	"xcap.mcptt-op.gov"		Indicates the configuration management server XCAP Root URI information. Ref. TS 23.003 [21].
px_MCPTT_IDMSAuthEndpoint	charstring	"IDMSAuthEndpoint.mcptt-op.gov"		Identity management server authorisation endpoint identity information. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCPTT_IDMSTokenEndpoint	charstring	"IDMSTokenEndpoint.mcptt-op.gov"		Identity management server token endpoint identity information. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCPTT_GMS	charstring	"mcptt-gms.mcptt-op.gov"		Indicates the group management server identity information. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCX_GMSURI	charstring			used for <GMS-URI> element in the MCS UE initial configuration document according to TS 24.484 [14] clause 7.2.2.7 and TS 24.483 [13] clause 8.2.9.
px_MCPTT_CMS	charstring	"mcptt-cms.mcptt-op.gov"		Indicates the configuration management server identity information. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore
px_MCPTT_KMS	charstring	"kms.mcptt-op.gov"		Indicates the key management server identity information. Ref. TS 23.003 [21]. Editor's note: To be removed when not used in 36.579-1 anymore

Parameter Name	Parameter Type	Default Value	Supported Values	Description
px_MCPTT_IdM_Server_URI	charstring	"IdM.server.com:9031"		Request-URI (AUID) for HTTP GET (IdM server) Editor's note: To be removed when not used in 36.579-1 anymore
px_MCPTT_XCAP_UE_Config_URI	charstring	“xcap.org.3gpp.mcptt.ue-config”		Request-URI (AUID) for HTTP GET (UE configuration)
px_MCPTT_XCAP_User_Profile_URI	charstring	“xcap.org.3gpp.mcptt.user-profile”		Request-URI (AUID) for HTTP GET (User Profile)
px_MCPTT_XCAP_Service_Config_URI	charstring	“xcap.org.3gpp.mcptt.service-config”		Request-URI (AUID) for HTTP GET (Service Configuration)
px_MCPTT_XCAP_Group_Config_URI	charstring	“xcap.org.3gpp.mcptt.group-config”		Request-URI (AUID) for HTTP GET (Group Configuration)
px_MCPTT_User_XUI_URI	charstring			"XUI-URI" attribute of the user profile document
px_MCX_IdMS_auth_IPAddress	charstring			IPv4/IPv6 address of the IdMS authorization endpoint
px_MCX_IdMS_auth_Port	integer			Port number of the IdMS authorization endpoint
px_MCX_IdMS_auth_Certificate	charstring			Identifier or file name of the certificate to be used during establishment of the TLS tunnel to the IdMS authorization endpoint
px_MCX_IdMS_token_IPAddress	charstring			IPv4/IPv6 address of the IdMS token endpoint
px_MCX_IdMS_token_Port	integer			Port number of the IdMS token endpoint
px_MCX_IdMS_token_Certificate	charstring			Identifier or file name of the certificate to be used during establishment of the TLS tunnel to the IdMS token endpoint
px_MCX_HTTP_Proxy_IPAddress	charstring			IPv4/IPv6 address of the HTTP proxy
px_MCX_HTTP_Proxy_Port	integer			Port number of the HTTP proxy
px_MCX_HTTP_Proxy_Certificate	charstring			Identifier or file name of the certificate to be used during establishment of the TLS tunnel to the HTTP proxy
px_MCX_InitialConfigServer_IPAddress	charstring			IPv4/IPv6 address of the server optionally being used to download the Initial UE Configuration document
px_MCX_InitialConfigServer_Port	integer			Port number of the server optionally being used to download the Initial UE Configuration document
px_MCX_InitialConfigServer_UriPath	charstring	"/cms/initial-ue-config"		URI Path component: Absolute path used for HTTP requests addressing a server to download the UE initial configuration document
px_MCX_TLS_CipherSuite	TLS_CIPHER_Type	TLS_RSA_WITH_NULL_SHA		Cipher suite to be used for TLS connections
px_MCX_OAuth_ClientId_A	charstring			Client ID of the UE's MCX application as used in OAuth signalling with the IdMS
px_MCX_OAuth_RedirectURI_A	charstring			Redirect URI used by the UE implementation (user agent, MCX client and OS) to redirect the OAuth authentication response to the MCX client application

9.2.3 MCPTT Constant PIXIT Definitions

Several parameters for MCX conformance testing can be defined as constants as they are neither preconfigured at the UE nor at the SS. Table 9.2.3-1 lists these constants.

Table 9.2.3-1: MCPTT Server Common PIXIT

Constant Name	Constant Type	Value	Description
tsc_MCX_KMS_Hostname	charstring	"kms.mcx-op.gov"	FQDN of the KMS; used in initial UE configuration as domain name for the 'kms' URI in the App-Server-Info.
tsc_MCX_CMS_Hostname	charstring	"cms.mcx-op.gov"	FQDN of the CMS; used in initial UE configuration as domain name for the 'cms' URI in the App-Server-Info.
tsc_MCX_GMS_Hostname	charstring	"gms.mcx-op.gov"	FQDN of the GMS; used in initial UE configuration as domain name for the 'gms' URI in the App-Server-Info.
tsc_MCX_KMS_CertUri	charstring	"certificate1." & tsc_MCX_KMS_Hostname	Name of the KMS certificate sent to the UE during MCX user authentication
tsc_MCX_IdMS_auth_UriPath	charstring	"/idms/auth"	URI path to address the IdMS authorization endpoint
tsc_MCX_IdMS_token_UriPath	charstring	"/idms/token"	URI path to address the IdMS token endpoint
tsc_MCX_KMS_init_UriPath	charstring	"/keymanagement/identity/v1/init"	Request-URI for "KMS Initialize" request according to TS 33.180 [43] D.2.3
tsc_MCX_KMS_keyprov_UriPath	charstring	"/keymanagement/identity/v1/keyprov"	Request-URI for "KMS KeyProvision" request according to TS 33.180 [43] D.2.4
tsc_MCX_KMS_ClientReqUrl	charstring	"https://" & tsc_MCX_KMS_Hostname & "/" & tsc_MCX_KMS_keyprov_UriPath	used as <ClientReqUrl> entry in the KMS Key Set

10 Postambles

10.1 Introduction

The purpose of the present clause 10 is to specify the postambles used to bring the UE to a well-defined state regardless of the UE state at the termination of main test body or of the SS conditions and values of the system information inherited from the test.

10.2 MCPTT

The postambles specified in TS 34.229-3 [28] are also applicable to MCPTT test cases.

Annex A (normative): Test Suites

A.1 Introduction

This annex references the approved Test Suites, which accompany the present document. The Test Suites have been produced using the Testing and Test Control Notation version 3 (TTCN-3) according to ES 201 873 [31].

A.2 Baseline of specifications

Table A.2-1 lists the core specifications and test specifications, which the delivered Test Suites are based upon.

Table A.2-1: References of the test and Core specifications

Type	Specification	Release	Version
Core specifications	TS 24.379 [9]	Note 1	Note 2
	TS 24.380 [10]	Note 1	Note 2
	TS 24.481 [11]	Note 1	Note 2
	TS 24.482 [12]	Note 1	Note 2
	TS 24.483 [13]	Note 1	Note 2
	TS 24.484 [14]	Note 1	Note 2
	TS 33.179 [15]	Note 1	Note 2
	TS 24.229 [16]	Note 1	Note 2
Test specifications	TS 36.579-1 [2]	Note 1	Note 2
	TS 36.579-2 [3]	Note 1	Note 2
	TS 38.579-4 [5]	Note 1	Note 2
NOTE 1: Latest release available, up to the release number of the present document. NOTE 2: Latest version available, up to the version number of the present document.			

A.3 MCPTT

A.3.1 MCPTT Client Test Suites

There is no approved Test Suite in the present version of the present document.

Annex B (informative): Style Guide

B.1 Introduction

The style guide specified in TS 36.523-3 [27] Annex B applies to the present document.

Annex C (informative): TTCN-3 Definitions

C.1 SRTP_ASP_TypeDefs

SRTCP_OpMode_Type

TTCN-3 Enumerated Type	
Name	**SRTCP_OpMode_Type**
NoReporting	
ReportFloorCtrl	

Media_Crypto_Suite_Type

TTCN-3 Enumerated Type	
Name	**Media_Crypto_Suite_Type**
	See RFC 4568 clause 6.2
AES_CM_128_HMAC_SHA1_80	
AES_CM_128_HMAC_SHA1_32	
F8_128_HMAC_SHA1_80	
Null_Suite	For testing

Media_Crypto_Type

TTCN-3 Record Type			
Name	**Media_Crypto_Type**		
Rx_Key	octetstring		key | salt for Rx-direction as passed in the SDP crypto parameters, RFC 4568
Rx_CryptoSuite	Media_Crypto_Suite_Type		
Tx_Key	octetstring		key | salt for Tx-direction as passed in the SDP crypto parameters, RFC 4568
Tx_CryptoSuite	Media_Crypto_Suite_Type		

SRTCP_DataRequest_Type

TTCN-3 Union Type		
Name	**SRTCP_DataRequest_Type**	
FloorCtrlMsg	FloorControlMsg_Type	

SRTCP_DataIndication_Type

TTCN-3 Union Type		
Name	**SRTCP_DataIndication_Type**	
FloorCtrlMsg	FloorControlMsg_Type	

SRTP_ConnectionCfg_Type

TTCN-3 Record Type			
Name	**SRTP_ConnectionCfg_Type**		
RtpConnection	IP_Connection_Type		RTP/SRTP connection
FloorCtrlConnection	IP_Connection_Type		Floor Control connection
OpMode	SRTCP_OpMode_Type		Report floor control reporting, no reporting
SSRC	O4_Type	opt	Synchronization Source (SSRC) identifier to be used in Tx-direction
Crypto	Media_Crypto_Type	opt	If present we are configuring SRTP/SRTCP, if not present we have RTP/RTCP

SRTP_CTRL_REQ

TTCN-3 Record of Type	
Name	**SRTP_CTRL_REQ**
	List of SRTP connection configs (e.g. for audio and video)
record of SRTP_ConnectionCfg_Type	

SRTCP_DATA_REQ

TTCN-3 Record Type			
Name	**SRTCP_DATA_REQ**		
ConnectionId	IP_Connection_Type		
Req	SRTCP_DataRequest_Type		

SRTP_CtrlIndication_Type

TTCN-3 Union Type		
Name	**SRTP_CtrlIndication_Type**	
Success	Null_Type	
Error	Null_Type	

SRTP_CTRL_IND

TTCN-3 Record Type			
Name	**SRTP_CTRL_IND**		
Ind	SRTP_CtrlIndication_Type		

SRTCP_DATA_IND

TTCN-3 Record Type			
Name	**SRTCP_DATA_IND**		
ConnectionId	IP_Connection_Type		
Ind	SRTCP_DataIndication_Type		

C.1.1 System_Interface

SRTP_ASP_REQ

TTCN-3 Union Type		
Name	**SRTP_ASP_REQ**	
CTRL	SRTP_CTRL_REQ	
DATA	SRTCP_DATA_REQ	

SRTP_ASP_IND

TTCN-3 Union Type		
Name	**SRTP_ASP_IND**	
CTRL	SRTP_CTRL_IND	
DATA	SRTCP_DATA_IND	

SRTP_PORT

TTCN-3 Port Type		
Name	**SRTP_PORT**	
inout	SRTP_ASP_REQ	
inout	SRTP_ASP_IND	

C.2 References to TTCN-3

SRTP_ASP_TypeDefs

References to TTCN-3		
SRTP_ASP_TypeDefs	Common/SRTP_ASP_TypeDefs.ttcn	Rev 24324

Annex D (Normative): SIP Type Definitions and XSD References

D.1 XML Schema Definitions (XSD)

Common XML schema definitions according to TS 34.229-3 [28] Table G.0.1-1 are used. In addition there are the MCX specific XML schema definitions as according to table D.1-1.

Table D.1-1: MCX specific definitions

XML Schema (XSD)	Source	Name space
RFC4661-SimpleFilter	RFC 4661 [34] clause 7	urn:ietf:params:xml:ns:simple-filter
IANA-resource-lists	RFC 4826 [35] clause 3.2 https://www.iana.org/assignments/xml-registry/schema/resource-lists.xsd	urn:ietf:params:xml:ns:resource-lists
poc_listService-v1_0	OMA [37]	urn:oma:xml:poc:list-service
xdm_extensions-v1_0	OMA [39]	urn:oma:xml:xdm:extensions
xdm_rsrclst_uriusage-v1_0	OMA [40]	urn:oma:xml:xdm:resource-list:oma-uriusage
xenc-schema	W3C [41]	http://www.w3.org/2001/04/xmlenc#'
xmldsig-core-schema	W3C [42]	http://www.w3.org/2000/09/xmldsig#
TS24379_mcpttaff	TS 24.379 [9] Annex F.4.2	urn:3gpp:ns:affiliationCommand:1.0
TS24379_mcpttinfo	TS 24.379 [9] Annex F.1.2	urn:3gpp:ns:mcpttInfo:1.0
TS24379_mcpttloc	TS 24.379 [9] Annex F.3.2	urn:3gpp:ns:mcpttLocationInfo:1.0
TS24379_pidf+xml-ext	TS 24.379 [9] Table 9.3.1.2-1	urn:3gpp:ns:mcpttPresInfo:1.0
TS24481_mcptt-group	TS 24.481 [11] clause 7.2.4.2	urn:3gpp:ns:mcpttGroupInfo:1.0
TS24481_mcpttGKTP	TS 24.481 [11] clause 7.7.4.2	urn:3gpp:ns:mcpttGKTP:1.0
TS24484_ue-init-config	TS 24.484 [14] clause 7.2.2.3	urn:3gpp:mcptt:mcpttUEinitConfig:1.0
TS24484_ue-config	TS 24.484 [14] clause 8.2.2.3	urn:3gpp:mcptt:mcpttUEConfig:1.0
TS24484_mcptt-user-profile	TS 24.484 [14] clause 8.3.2.3	urn:3gpp:mcptt:user-profile:1.0
TS24484_Servconf	TS 24.484 [14] clause 8.4.2.3	urn:3gpp:ns:mcpttServiceConfig:1.0
TS33180 mcsecKMSInterface	TS 33.180 [43] Annex D.3.5.1	urn:3gpp:ns:mcsecKMSInterface:1.0
TS33180 mcsecKMSKRR	TS 33.180 [43] Annex D.4.4	urn:3gpp:ns:mcsecKMSKRR:1.0

In order to avoid ambiguities and unexpected side effects due to tool specific behaviour the schemaLocation in xs:import statements of XSD files are modified to use local references rather than references to internet locations.

The schemaLocations are shown in table D.1-2.

Table D.1-2: MCPTT Server Common PIXIT

XML Schema	Imported name space	Original schemaLocation	Modified schemaLocation
RFC4661-SimpleFilter	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd
IANA-resource-lists	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd
poc_listService-v1_0	urn:ietf:params:xml:ns:common-policy	http://www.iana.org/assignments/xml-registry/schema/common-policy.xsd	../../Common/IMS_XSD/RFC4745-common-policy.xsd (NOTE 1)
poc_listService-v1_0	urn:ietf:params:xml:ns:resource-lists	http://www.iana.org/assignments/xml-registry/schema/resource-lists.xsd	IANA-resource-lists.xsd (NOTE 2)
xdm_extensions-v1_0	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/03/xml.xsd	../../Common/IMS_XSD/xml.xsd
xenc-schema	http://www.w3.org/2000/09/xmldsig#	xmldsig-core-schema.xsd	(no change needed)
TS24484-ue-init-config	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd
TS24484-ue-config	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd
TS24484-mcptt-user-profile	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd
TS24484-mcptt-user-profile	urn:ietf:params:xml:ns:common-policy	http://www.iana.org/assignments/xml-registry/schema/common-policy.xsd	../../Common/IMS_XSD/RFC4745-common-policy.xsd (NOTE 1)
TS24484-Servconf	http://www.w3.org/XML/1998/namespace	http://www.w3.org/2001/xml.xsd	../../Common/IMS_XSD/xml.xsd

NOTE 1: The namespace urn:ietf:params:xml:ns:common-policy is specified in RFC 4745 and at http://www.iana.org/assignments/xml-registry/schema/common-policy.xsd with difference in the minOccurs for identityType and validityType. Nevertheless for use in TTCN there shall be only one schema as part 9 of the TTCN-3 language [31] does not support different variants of one and the same namespace. In addition according to DIFF1 for RFC 4745 it seems that the RFC's variant is newer than the IANA's variant.

NOTE 2: The namespace urn:ietf:params:xml:ns:resource-lists is specified in RFC 4826 and at http://www.iana.org/assignments/xml-registry/schema/resource-lists.xsd with the difference of attribute anchor not being mandatory in the RFC.

D.2 Common TTCN-3 Libraries

The same LibSip modules are used as according to TS 34.229-3 [28] annex G.0.2 and the same additional LibSip_MessageBodyTypes as according to TS 34.229-3 [28] annex G.1 and G.2

Annex E (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-02	RAN5#74	R5-171302	-	-	-	Introduction of TS 36.579-5.	0.0.1
2018-03	RAN5#78	R5-180687	-	-	-	Implements changes agreed in R5-180618 "MCPTT: Initial Test Model" R5-180657 "Various updates to 36579-5"	0.1.0
2018-03	RAN#79	RP-180130	-	-	-	Draft version for information purposes to the RAN Plenary	1.0.0
2018-05	RAN5#79	R5-182437	-	-	-	Implements changes agreed in R5-183163 R5-183164	2.0.0
2018-06	RAN#80	RP-180655	-	-	-	put under revision control as v13.0.0 with small editorial changes	13.0.0
2018-09	RAN#81	R5-184081	0001	-	F	MCPTT: Test Model updates	13.1.0
2018-12	RAN#82	R5-192380	0002	1	F	Routine maintenance for TS 36.579-5	13.2.0
2019-06	RAN#84	R5-195221	0003	1	F	Routine maintenance for TS 36.579-5	13.3.0
2019-06	RAN#84	R5-195222	0004	1	F	Introduction of MCPTT test model over IP	13.3.0
2019-12	RAN#86	R5-199050	0005	1	F	Routine maintenance for TS 36.579-5	13.4.0
2020-03	RAN#87	R5-201152	0006	1	F	Routine maintenance for TS 36.579-5	13.5.0

History

Document history		
V13.0.0	July 2018	Publication
V13.1.0	October 2018	Publication
V13.2.0	May 2019	Publication
V13.3.0	July 2019	Publication
V13.4.0	January 2020	Publication
V13.5.0	April 2020	Publication