

ETSI TS 124 384 V13.1.0 (2016-07)



**Universal Mobile Telecommunications System (UMTS);
LTE;
Mission Critical Push To Talk (MCPTT)
configuration management;
Protocol specification
(3GPP TS 24.384 version 13.1.0 Release 13)**



Reference

RTS/TSGC-0124384vd10

Keywords

LTE,UMTS

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	6
1 Scope	7
2 References	7
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	8
4 General	9
4.1 MCPTT service administrator configuration.....	9
4.2 MCPTT UE configuration.....	10
4.2.1 General.....	10
4.2.2 Online configuration	10
4.2.3 Offline configuration	11
4.3 MCPTT server.....	12
4.4 Configuration management server.....	12
5 Functional entities	13
5.1 Configuration management client (CMC).....	13
5.2 Configuration management server (CMS)	13
6 Procedures	13
6.1 Introduction	13
6.2 Common procedures.....	14
6.2.1 General.....	14
6.2.2 Client procedures	14
6.2.3 MCPTT server procedures.....	14
6.2.4 Configuration management server procedures.....	14
6.3 Configuration management procedures.....	14
6.3.1 General.....	14
6.3.1.1 Client procedures	14
6.3.1.2 Configuration management server procedures.....	14
6.3.2 Configuration management document creation procedure	14
6.3.2.1 General.....	14
6.3.2.2 Configuration management client (CMC) procedures	14
6.3.2.3 Configuration management server (CMS) procedures	14
6.3.3 Configuration management document retrieval procedure.....	15
6.3.3.1 General	15
6.3.3.2 Client procedures	15
6.3.3.2.1 General client (GC) procedures	15
6.3.3.2.2 Configuration management client (CMC) procedures.....	15
6.3.3.2.3 MCPTT server procedures.....	15
6.3.3.3 Configuration management server procedures.....	15
6.3.4 Configuration management document update procedure.....	15
6.3.4.1 General	15
6.3.4.2 Configuration management client procedures.....	15
6.3.4.3 Configuration management server procedures.....	15
6.3.5 Configuration management document deletion procedure	15
6.3.5.1 General	15
6.3.5.2 Configuration management Client (CMC) procedures	16
6.3.5.3 Configuration management server (CMS) procedures.....	16
6.3.6 Configuration management document element creation or replacement procedure	16

6.3.6.1	General	16
6.3.6.2	Client procedures	16
6.3.6.2.1	General client procedures	16
6.3.6.2.2	Configuration management client procedures	16
6.3.6.3	Configuration management server procedures	16
6.3.7	Configuration management document element deletion procedure	16
6.3.7.1	General	16
6.3.7.2	Client procedures	16
6.3.7.2.1	General client procedures	16
6.3.7.2.2	Configuration management client procedures	16
6.3.7.3	Configuration management server procedures	17
6.3.8	Configuration management document element fetching procedure	17
6.3.8.1	General	17
6.3.8.2	Client procedures	17
6.3.8.2.1	General client procedures	17
6.3.8.2.2	Configuration management client procedures	17
6.3.8.2.3	MCPTT server procedures	17
6.3.8.3	Configuration management server procedures	17
6.3.9	Configuration management document attribute creation or replacement procedure	17
6.3.9.1	General	17
6.3.9.2	Client procedures	17
6.3.9.2.1	General client procedures	17
6.3.9.2.2	Configuration management client procedures	17
6.3.9.3	Configuration management server procedures	18
6.3.10	Configuration management document attribute deletion procedure	18
6.3.10.1	General	18
6.3.10.2	Client procedures	18
6.3.10.2.1	General client procedures	18
6.3.10.2.2	Configuration management client procedures	18
6.3.10.3	Configuration management server procedures	18
6.3.11	Configuration management document attribute fetching procedure	18
6.3.11.1	General	18
6.3.11.2	Client procedures	18
6.3.11.2.1	General client procedures	18
6.3.11.2.2	Configuration management client procedures	18
6.3.11.2.3	MCPTT server procedures	18
6.3.11.3	Configuration management server procedures	19
6.3.12	Configuration management document namespace binding fetching procedure	19
6.3.12.1	General	19
6.3.12.2	Client procedures	19
6.3.12.2.1	General client procedures	19
6.3.12.2.2	Configuration management client procedures	19
6.3.12.2.3	MCPTT server procedures	19
6.3.12.3	Configuration management server procedures	19
6.3.13	Configuration management subscription and notification procedure	19
6.3.13.1	General	19
6.3.13.2	Client procedures	19
6.3.13.2.1	General client (GC) procedures	19
6.3.13.2.2	Configuration management client procedures	20
6.3.13.2.3	MCPTT server procedures	20
6.3.13.3	Configuration management server procedures	20
7	Configuration management documents	20
7.1	Introduction	20
7.2	MCPTT UE initial configuration document	20
7.2.1	General	20
7.2.2	Coding	21
7.2.2.1	Structure	21
7.2.2.2	Application Unique ID	23
7.2.2.3	XML Schema	23
7.2.2.4	Default Document Namespace	23
7.2.2.5	MIME type	23

7.2.2.6	Validation Constraints.....	23
7.2.2.7	Data Semantics.....	26
7.2.2.8	Naming Conventions.....	29
7.2.2.9	Global documents	29
7.2.2.10	Resource interdependencies	29
7.2.2.11	Authorization Policies.....	29
7.2.2.12	Subscription to Changes.....	29
7.3	MCPTT UE configuration document	29
7.3.1	General.....	29
7.3.2	Coding	29
7.3.2.1	Structure.....	29
7.3.2.2	Application Unique ID.....	30
7.3.2.3	XML Schema	30
7.3.2.4	Default Document Namespace.....	30
7.3.2.5	MIME type.....	30
7.3.2.6	Validation Constraints.....	30
7.3.2.7	Data Semantics.....	32
7.3.2.8	Naming Conventions.....	33
7.3.2.9	Global documents	33
7.3.2.10	Resource interdependencies	33
7.3.2.11	Authorization Policies.....	33
7.3.2.12	Subscription to Changes.....	33
7.4	MCPTT user profile configuration document	33
7.4.1	General.....	33
7.4.2	Coding	33
7.4.2.1	Structure.....	33
7.4.2.2	Application Unique ID.....	36
7.4.2.3	XML Schema	36
7.4.2.4	Default Namespace	38
7.4.2.5	MIME type.....	38
7.4.2.6	Validation Constraints.....	38
7.4.2.7	Data Semantics.....	38
7.4.2.8	Naming Conventions.....	42
7.4.2.9	Global documents	42
7.4.2.10	Resource interdependencies	42
7.4.2.11	Access Permissions Policies.....	42
7.4.2.12	Subscription to Changes.....	42
7.5	MCPTT service configuration document	42
7.5.1	General.....	42
7.5.2	Coding	43
7.5.2.1	Structure.....	43
7.5.2.2	Application Unique ID.....	45
7.5.2.3	XML Schema	45
7.5.2.4	Default Namespace	47
7.5.2.5	MIME type.....	47
7.5.2.6	Validation Constraints.....	47
7.5.2.7	Data Semantics.....	50
7.5.2.8	Naming Conventions.....	52
7.5.2.9	Global documents	52
7.5.2.10	Resource interdependencies	52
7.5.2.11	Authorization Policies.....	52
7.5.2.12	Subscription to Changes.....	52
Annex A (informative):	 Signalling flows	53
Annex B (informative):	 Change history	54
History		55

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 configuration management documents and protocols needed to support Mission Critical Push To Talk (MCPTT) online configuration over the CSC-4 and CSC-5 reference points and the procedures to support Mission Critical Push To Talk (MCPTT) offline configuration over the CSC-11 and CSC-12 reference points. Configuration management documents defined in the present document includes:

- MCPTT UE initial configuration document;
- MCPTT UE configuration document;
- MCPTT user profile configuration document; and
- MCPTT service configuration document.

Mission critical communication services are services that require preferential handling compared to normal telecommunication services, e.g. in support of police or fire brigade.

The MCPTT service can be used for public safety applications and also for general commercial applications (e.g., utility companies and railways).

The present document is applicable to an MCPTT UE supporting the configuration management client functionality, to application server supporting the configuration management server functionality, and to application server supporting the MCPTT server functionality.

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] OMA OMA-TS-XDM_Core-V2_1-20120403-A: "XML Document Management (XDM) Specification".
- [3] 3GPP TS 22.179: "Mission Critical Push to Talk (MCPTT) over LTE; Stage 1".
- [4] 3GPP TS 24.383: "Mission Critical Push to Talk (MCPTT) Management Object (MO)".
- [5] 3GPP TS 24.381: "Mission Critical Push to Talk (MCPTT) group management Protocol specification".
- [6] 3GPP TS 24.382: "Mission Critical Push to Talk (MCPTT) identity management Protocol specification".
- [7] 3GPP TS 29.283: "Diameter Data Management Applications".
- [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] IETF RFC 5875: "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".
- [12] 3GPP TS 24.333: "Proximity-services (ProSe) Management Objects (MO)".
- [13] IETF RFC 4745: "Common Policy: A Document Format for Expressing Privacy Preferences".
- [14] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".
- [15] Void.
- [16] 3GPP TS 23.003: "Numbering, addressing and identification". [17] OMA OMA-TS-XDM_Group-V1_1-20120403-A: "Group XDM Specification".

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].

MCPTT network: A network infrastructure that supports the MCPTT service.

Offline Configuration: Configuration of the MCPTT UE without connectivity with any MCPTT network.

Configuration of the MCPTT UE is achieved using some external device (e.g. a laptop) with some kind of IP connectivity with the MCPTT UE (e.g. over USB, WLAN, Bluetooth, etc).

Off-network operation: An MCPTT UE operating without connectivity to an MCPTT network (not even via a relay).

Online Configuration: Configuration of the MCPTT UE using the MCPTT network. Configuration of the MCPTT UE is achieved using the network connectivity with the MCPTT UE (e.g. over LTE).

On-network operation: An MCPTT UE operating with connectivity to an MCPTT network including when network connectivity is achieved via a relay.

For the purposes of the present document, the following terms and definitions given in OMA OMA-TS-XDM_Core-V2_1 [2] apply:

XDMC

XDMS

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

MCPTT administrator

MCPTT UE

MCPTT User Profile

MCPTT service

Mission Critical Push To Talk

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].

AUID	Application Unique IDentity
CMC	Configuration Management Client
CMS	Configuration Management Server
DM	Device Management

E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FQDN	Fully Qualified Domain Name
GC	General Client
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
MCPTT	Mission Critical Push To Talk
MIME	Multi-Purpose Internet Mail Extensions
MO	Management Object
OMA	Open Mobile Alliance
ProSe	Proximity Services
RFC	Request For Comments
SIP	Session Initiation Protocol
UE	User Equipment
URI	Uniform Resource Identifier
URN	Uniform Resource Name
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XML Document Management Client
XDMS	XML Document Management Server
XML	eXtensible Markup Language
XUI	XCAP Unique Identifier

4 General

4.1 MCPTT service administrator configuration

An MCPTT service administrator can, using an MCPTT UE configure the:

- MPCTT UE initial configuration document;
- MPCTT UE configuration document;
- MPCTT user profile configuration document;
- MPCTT service configuration document; and
- MPCTT group document.

The format of the MPCTT UE initial configuration document for configuration by an MCPTT service administrator is defined in subclause 7.2.

The format of the MPCTT UE configuration document is defined in subclause 7.3.

The format of the MPCTT user profile configuration document is defined in subclause 7.4.

The format of the MPCTT service configuration document is defined in subclause 7.5.

The format of the MPCTT group document is defined in 3GPP TS 24.381 [5].

To create a new configuration document on the configuration management server, the MCPTT UE uses the procedures in subclause 6.3.2.2.

To update an existing configuration document on the configuration management server, the MCPTT UE uses the procedures in subclause 6.3.4.2.

To delete an existing configuration document on the configuration management server, the MCPTT UE uses the procedures in subclause 6.3.5.2.

To create a new MCPTT group document on the configuration management server, the MCPTT UE uses the procedures in 3GPP TS 24.381 [5].

To update an existing MCPTT group document on the configuration management server, the MCPTT UE uses the procedures in 3GPP TS 24.381 [5].

To delete an existing MCPTT group document on the configuration management server, the MCPTT UE uses the procedures in 3GPP TS 24.381 [5].

4.2 MCPTT UE configuration

4.2.1 General

Upon startup the MCPTT UE bootstraps the required information (e.g. FQDN or IP address) to locate the configuration management server for configuration of the MCPTT UE initial configuration management object (MO).

In order to obtain access to the MCPTT service the MCPTT UE needs to obtain configuration data either online via the network or offline using some external device (e.g. a laptop). As part of the bootstrap process the MCPTT UE needs to discover either:

1. the online configuration management server in the network that configures the MCPTT UE initial configuration MO, then the MCPTT UE:
 - a) using the URI of the configuration management server obtained from the MCPTT UE initial configuration MO, obtains:
 - the MCPTT UE configuration document; and
 - the MCPTT user profile configuration document; and
 - b) using the URI of the group management server obtained from the MCPTT UE initial configuration MO obtain the MCPTT group document; or
2. the:
 - a) offline configuration management server on the external device that configures the MCPTT UE with the:
 - MCPTT UE initial configuration MO;
 - MCPTT UE configuration MO;
 - MCPTT user profile document MO; and
 - MCPTT service configuration MO; and
 - b) offline group management server on the external device that configures the MCPTT UE with the MCPTT group MO.

The mechanism to discover the online or offline configuration management server is dependent on the protocol used to manage and configure the MO and is out of scope of the present document.

4.2.2 Online configuration

The format of the MCPTT UE initial configuration MO downloaded to the MCPTT UE during online configuration is defined in 3GPP TS 24.383 [4].

The format of the MCPTT UE configuration document downloaded to the MCPTT UE during online configuration is defined in subclause 7.3.

The format of the MCPTT user profile configuration document downloaded to the MCPTT UE during online configuration is defined in subclause 7.4.

The format of the MCPTT group document downloaded to the MCPTT UE during online configuration is defined in 3GPP TS 24.381 [5].

Figure 4.2.2-1 shows the MCPTT UE online configuration time sequence.

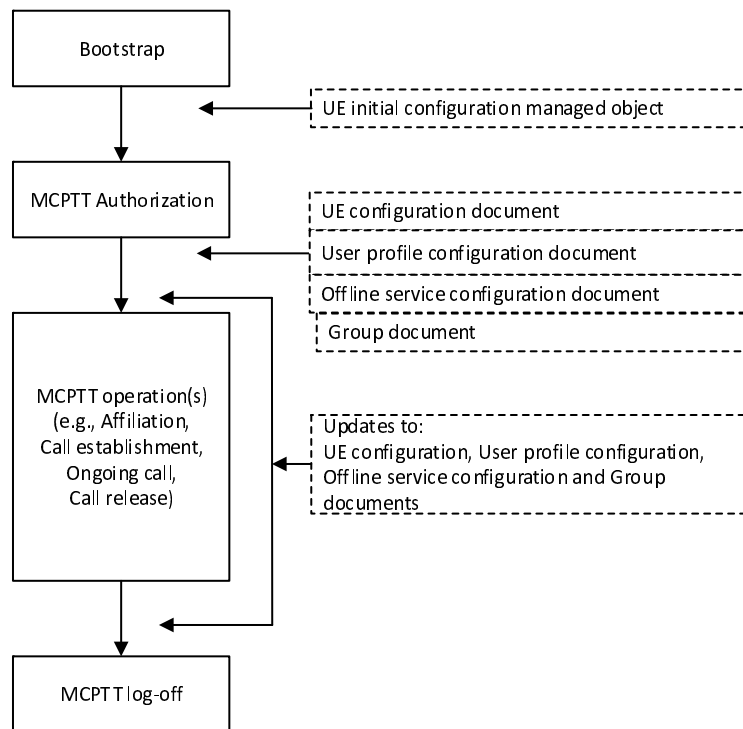


Figure 4.2.2-1 MCPTT UE online configuration time sequence

If the MCPTT UE initial configuration MO has changed from the version stored in the MCPTT UE, the updated MCPTT UE initial configuration MO is downloaded to the MCPTT UE.

The MCPTT UE contacts the identity management server using the HTTPS URI stored in the MCPTT UE initial configuration MO and performs MCPTT User authentication as specified in 3GPP TS 24.382 [6].

The MCPTT UE, using the MCPTT ID obtained during MCPTT user authentication, subscribes to the MCPTT UE configuration document, the MCPTT user profile configuration document and the MCPTT service configuration document using the procedure specified in subclause 6.1.2.1.2 of OMA OMA-TS-XDM_Core-V2_1 [2] "XDMC" (i.e., the CMS acts as a Subscription Proxy) and subscribes to the MCPTT group document using the procedure specified in 3GPP TS 24.381 [5]. If these documents have been updated since the current version stored in the MCPTT UE, then the MCPTT UE will receive a SIP NOTIFY request with an XCAP Diff document (see IETF RFC 5875 [11]), in which case the CMC updates its local document copies in accordance with OMA OMA-TS-XDM_Core-V2_1 [2]. Retrieval by the MCPTT UE using the notified HTTPS URI of the MCPTT group document is performed as specified in 3GPP TS 24.381 [5].

NOTE: The MCPTT UE can be notified of changes to the configuration documents at any time while using the MCPTT service.

4.2.3 Offline configuration

When configuring an MCPTT UE offline the offline configuration management server will need to support the MCPTT administrator providing the MCPTT ID of the MCPTT user for whom the MCPTT UE is being configured so that the correct configuration data for that MCPTT user can be configured in the MOs.

The format of the MCPTT UE initial configuration MO downloaded to the MCPTT UE during offline configuration is defined in 3GPP TS 24.383 [4].

The format of the MCPTT UE configuration MO downloaded to the MCPTT UE during offline configuration is defined in 3GPP TS 24.383 [4].

The format of the MCPTT user profile configuration MO downloaded to the MCPTT UE during offline configuration is defined in 3GPP TS 24.383 [4].

The format of the MCPTT service configuration MO downloaded to the MCPTT UE during offline configuration is defined in 3GPP TS 24.383 [4].

The format of the MCPTT group document MO to the MCPTT UE during offline configuration is defined in 3GPP TS 24.383 [4].

4.3 MCPTT server

The MCPTT server obtains the MCPTT service configuration document that contains the mission critical organisation configured parameters that defined the behaviour of the MCPTT service from the configuration management server.

The format of the MCPTT service configuration document downloaded to the MCPTT server is defined in subclause 7.5.

The MCPTT server obtains the MCPTT service configuration document that contains the mission critical organisation configured parameters that defined the behaviour of the MCPTT service from the configuration management server.

The MCPTT server subscribes to the MCPTT service configuration document for each mission critical organisation that is provisioned that is supported by the MCPTT server using the procedure specified in subclause 6.3.13.2.3. How the MCPTT server is provisioned with the identities of the mission critical organisations is out of scope of the present document.

If the MCPTT service configuration document has been updated since the current version stored at the MCPTT server, then the MCPTT server will receive a SIP NOTIFY request containing an HTTPS URI of the MCPTT service configuration document. Retrieval by the MCPTT server, using the notified HTTPS URI, of the MCPTT service configuration document is performed as specified in subclause 6.3.3.2.3.

NOTE: The MCPTT server can be notified of changes to the MCPTT service management configuration document at any time while operating the MCPTT service.

The format of the MCPTT service configuration document downloaded to the MCPTT server is defined in subclause 7.5.

4.4 Configuration management server

The following applies to the configuration management server used for online configuration.

The configuration management server needs to convert the MCPTT UE initial configuration document received from a MCPTT administrator into an appropriate format for configuration of the MCPTT UE initial configuration MO.

Once an MCPTT User Profile configuration document has been created or updated by the MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to store MCPTT user profile configuration document as the user profile in the MCPTT user database.

In order to download MCPTT the user profile configuration document to an MCPTT UE or to support an MCPTT UE updating the MCPTT user profile configuration document, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to obtain the MCPTT user profile from the MCPTT user database.

In order to be notified of changes to an MCPTT user profile configuration document that have been subscribed to by an MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to be notified of changes to the MCPTT user profile stored in the MCPTT user database.

In order to delete the MCPTT user profile when requested by an MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to delete the MCPTT user profile from the MCPTT user database.

NOTE: The configuration management server and group management server functionality for offline configuration is out of scope of the present document.

5 Functional entities

5.1 Configuration management client (CMC)

The CMC shall:

- support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [2]; and
- support the procedures in subclause 6.3.13.2, subclause 6.3.2.2 and subclause 6.3.3.2.2.

The CMC may support the procedures in subclause 6.2.2, subclause 6.3.4.2 and subclause 6.3.5.2.

5.2 Configuration management server (CMS)

The CMS shall:

- support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [2]; and
- support the procedures in subclause 6.3.13.3, subclause 6.2.4, subclause 6.3.2.3, subclause 6.3.3.3, subclause 6.3.4.3 and subclause 6.3.5.3.

6 Procedures

6.1 Introduction

This clause specifies procedures enabling a group management client (CMC) and an MCPTT server to have the MCPTT configuration managed using the configuration management server (CMS).

The following procedures are defined for management of configuration management documents:

- configuration management document creation procedure;
- configuration management document retrieval procedure;
- configuration management document update procedure;
- configuration management document deletion procedure;
- configuration management document element creation or replacement procedure;
- configuration management document element deletion procedure;
- configuration management document element fetching procedure;
- configuration management document attribute creation or replacement procedure;
- configuration management document attribute deletion procedure;
- configuration management document attribute fetching procedure;
- configuration management document namespace binding fetching procedure; and
- configuration management document subscription and notification procedure.

6.2 Common procedures

6.2.1 General

This subclause contains common procedures applied on HTTP signalling specified in this document.

6.2.2 Client procedures

The CMC shall send the HTTP request over TLS connection as specified for the HTTP client in the UE in annex A of 3GPP TS 24.382 [6].

6.2.3 MCPTT server procedures

The MCPTT server shall send the HTTP request as specified for the HTTP client in the network entity in annex A of 3GPP TS 24.382 [6].

6.2.4 Configuration management server procedures

The CMS shall handle the HTTP request as specified for the HTTP server in annex A of 3GPP TS 24.382 [6].

6.3 Configuration management procedures

6.3.1 General

6.3.1.1 Client procedures

A CMC shall support subclause 6.1.1 "*Document Management*" and subclause 6.1.2 "*Subscribing to Changes in XDM Resources*" of OMA OMA-TS-XDM_Core-V2_1 [2].

6.3.1.2 Configuration management server procedures

A CMS shall support subclause 6.2.1 "*Document Management*", subclause 6.2.2 "*Subscriptions to Changes in XDM Resources*", subclause 6.2.4 "*Access Permissions*", and subclause 6.6 "*Procedures of the Subscription Proxy*" applicable for SIP subscription method of OMA OMA-TS-XDM_Core-V2_1 [2].

6.3.2 Configuration management document creation procedure

6.3.2.1 General

This subclause addresses the scenario for configuration management creation by administrators as described in 3GPP TS 23.179 [8].

6.3.2.2 Configuration management client (CMC) procedures

In order to create a configuration management document, a CMC shall create an XML document of one of the appropriate application usages specified in subclause 7.3.1, subclause 7.4.1, subclause 7.5.1 or subclause 7.2.1, and shall send the XML document to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Create or Replace a Document*".

6.3.2.3 Configuration management server (CMS) procedures

A CMS shall support receiving XML documents of the application usage specified in subclause 7.3.1, subclause 7.4.1, subclause 7.5.1 and subclause 7.2.1 according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an XML document of the appropriate application usage.

6.3.3 Configuration management document retrieval procedure

6.3.3.1 General

This subclause describes how retrieval of a configuration management document takes place.

6.3.3.2 Client procedures

6.3.3.2.1 General client (GC) procedures

In order to retrieve a configuration management document, a GC shall send an HTTP GET request with the Request URI that references the document to be updated to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Retrieve a Document*".

6.3.3.2.2 Configuration management client (CMC) procedures

In order to retrieve a configuration management document, a CMC shall perform the procedures in subclause 6.3.3.2.1 specified for GC. Subclause 7.5 specifies which configuration management documents can be retrieved from the CMS over the CSC-4 reference point.

6.3.3.2.3 MCPTT server procedures

In order to retrieve a configuration management document via the CSC-5 reference point, an MCPTT Server shall perform the procedures in subclause 6.3.3.2.1 specified for GC. Subclause 7.5 specifies which configuration management documents can be retrieved from the CMS via the CSC-5 reference point.

6.3.3.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from a CMC and an MCPTT Server according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an XML document of the appropriate application usage.

6.3.4 Configuration management document update procedure

6.3.4.1 General

This subclause describes the procedures for updating of a configuration management document.

6.3.4.2 Configuration management client procedures

In order to update a configuration management document, a CMC shall create an XML document of one of the appropriate application usages specified in subclause 7.2.1, subclause 7.3.1, subclause 7.4.1, or subclause 7.5.1, and shall send the XML document to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Create or Replace a Document*".

6.3.4.3 Configuration management server procedures

A CMS shall support receiving an XML document of the application usages specified in subclause 7.2.1, subclause 7.3.1, subclause 7.4.1, and subclause 7.5.1 according to the procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an XML document of the appropriate application usage.

6.3.5 Configuration management document deletion procedure

6.3.5.1 General

This subclause describes deletion of a configuration management document.

6.3.5.2 Configuration management Client (CMC) procedures

In order to delete a configuration management document, a CMC shall send an HTTP DELETE request with the Request URI that references the XML document to be deleted to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Delete a Document*".

6.3.5.3 Configuration management server (CMS) procedures

A CMS shall support handling an HTTP DELETE request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an XML document of the appropriate application usage.

6.3.6 Configuration management document element creation or replacement procedure

6.3.6.1 General

This procedure enables the CMC to create or replace an element of a configuration management document from CMS.

6.3.6.2 Client procedures

6.3.6.2.1 General client procedures

In order to create or replace an element of a configuration management document, a GC shall send an HTTP PUT request with the Request URI that references the element of the document to be created or replaced to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Create or Replace an Element*".

6.3.6.2.2 Configuration management client procedures

In order to create or replace an element of a configuration management document, a CMC shall perform the procedures in subclause 6.3.6.2.1 specified for GC.

6.3.6.3 Configuration management server procedures

A CMS shall support handling an HTTP PUT request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an element of XML document of the appropriate application usage.

6.3.7 Configuration management document element deletion procedure

6.3.7.1 General

This procedure enables the CMC to delete an element of a configuration management document from CMS.

6.3.7.2 Client procedures

6.3.7.2.1 General client procedures

In order to delete an element of a configuration management document, a GC shall send an HTTP DELETE request with the Request URI that references the element of the document to be deleted to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Delete an Element*".

6.3.7.2.2 Configuration management client procedures

In order to delete an element of a configuration management document, a CMC shall perform the procedures in subclause 6.3.7.2.1 specified for GC.

6.3.7.3 Configuration management server procedures

A CMS shall support handling an HTTP DELETE request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an element of XML document of the appropriate application usage.

6.3.8 Configuration management document element fetching procedure

6.3.8.1 General

This procedure enables the CMC or the MCPTT server to fetch an element of a configuration management document from the CMS.

6.3.8.2 Client procedures

6.3.8.2.1 General client procedures

In order to fetch an element of a configuration management document, a GC shall send an HTTP GET request with the Request URI that references the element of the document to be fetched to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Retrieve an Element*".

6.3.8.2.2 Configuration management client procedures

In order to fetch an element of a configuration management document, a CMC shall perform the procedures in subclause 6.3.8.2.1 specified for GC.

6.3.8.2.3 MCPTT server procedures

In order to fetch an element of a configuration management document, an MCPTT server shall perform the procedures in subclause 6.3.8.2.1 specified for GC.

6.3.8.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an element of XML document of the appropriate application usage.

6.3.9 Configuration management document attribute creation or replacement procedure

6.3.9.1 General

This procedure enables the CMC to create or replace an attribute of a configuration management document from CMS.

6.3.9.2 Client procedures

6.3.9.2.1 General client procedures

In order to create or replace an attribute of a configuration management document, a GC shall send an HTTP PUT request with the Request URI that references the element of the document to be created or replaced to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Create or Replace an Attribute*".

6.3.9.2.2 Configuration management client procedures

In order to create or replace an attribute of a configuration management document, a CMC shall perform the procedures in subclause 6.3.9.2.1 specified for GC.

6.3.9.3 Configuration management server procedures

A CMS shall support handling an HTTP PUT request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an attribute of XML document of the appropriate application usage.

6.3.10 Configuration management document attribute deletion procedure

6.3.10.1 General

This procedure enables the CMC to delete an attribute of a configuration management document from the CMS.

6.3.10.2 Client procedures

6.3.10.2.1 General client procedures

In order to delete an attribute of a configuration management document, a GC shall send an HTTP DELETE request with the Request URI that references the attribute of the document to be deleted to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Delete an Element*".

6.3.10.2.2 Configuration management client procedures

In order to delete an attribute of a configuration management document, a CMC shall perform the procedures in subclause 6.3.10.2.1 specified for GC.

6.3.10.3 Configuration management server procedures

A CMS shall support handling an HTTP DELETE request from CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an attribute of XML document of the appropriate application usage.

6.3.11 Configuration management document attribute fetching procedure

6.3.11.1 General

This procedure enables the CMC or the MCPTT server to fetch an attribute of a configuration management document from the CMS.

6.3.11.2 Client procedures

6.3.11.2.1 General client procedures

In order to fetch an attribute of a configuration management document, a GC shall send an HTTP GET request with the Request URI that references the attribute of the document to be fetched to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Retrieve an Attribute*".

6.3.11.2.2 Configuration management client procedures

In order to fetch an attribute of a configuration management document, a CMC shall perform the procedures in subclause 6.3.11.2.1 specified for GC.

6.3.11.2.3 MCPTT server procedures

In order to fetch an attribute of a configuration management document, an MCPTT server shall perform the procedures in subclause 6.3.11.2.1 specified for GC.

6.3.11.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an attribute of XML document of the application usage specified in subclause 7.2.

6.3.12 Configuration management document namespace binding fetching procedure

6.3.12.1 General

This procedure enables the CMC or the MCPTT server to fetch a namespace binding of a configuration management document from the CMS.

6.3.12.2 Client procedures

6.3.12.2.1 General client procedures

In order to fetch a namespace binding of a configuration management document, a GC shall send an HTTP GET request according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Fetch Namespace Bindings*".

6.3.12.2.2 Configuration management client procedures

In order to fetch a namespace binding of a configuration management document, a CMC shall perform the procedures in subclause 6.3.12.2.1 specified for GC.

6.3.12.2.3 MCPTT server procedures

In order to fetch a namespace binding of a configuration management document, an MCPTT server shall perform the procedures in subclause 6.3.12.2.1 specified for GC.

6.3.12.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from a CMC according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*GET Handling*" where the Request-URI of the HTTP GET request identifies a namespace binding of XML document of the appropriate application usage.

6.3.13 Configuration management subscription and notification procedure

6.3.13.1 General

This subclause describes subscription to a configuration management document.

6.3.13.2 Client procedures

6.3.13.2.1 General client (GC) procedures

In order to subscribe to a Configuration document, a GC shall send a SIP SUBSCRIBE request to the network according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Subscribing to Changes in the XDM Resources*". In the SUBSCRIBE request, the GC:

- a) if direct subscription is used, shall set the Request URI to a SIP URI containing:
 - the XUI part of the XCAP URI pointing to the MCPTT configuration management document being subscribed to as defined in clause 7; and
 - an "auid" parameter set to the application unique ID for the configuration management document being subscribed to as defined in clause 7; and

- b) if subscription to multiple documents simultaneously using the subscription proxy function is used, shall set the Request URI to the URI from the "CMS" element in the MCPTT UE initial configuration management object as defined in subclause 8.2.44 of 3GPP TS 24.383 [4].

NOTE: The body of the SIP SUBSCRIBE request contains a list of XCAP URIs pointing to the configuration management document(s) that the GC subscribes to as described in OMA OMA-TS-XDM_Core-V2_1 [2].

6.3.13.2.2 Configuration management client procedures

In order to subscribe to Configuration management document, a CMC shall perform the procedures in subclause 6.3.13.2.1 specified for GC.

6.3.13.2.3 MCPTT server procedures

In order to subscribe to Configuration management document, an MCPTT server shall perform the procedures in subclause 6.3.13.2.1 specified for GC.

6.3.13.3 Configuration management server procedures

A CMS shall support handling a SIP SUBSCRIBE request from CMC and MCPTT Server according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Subscriptions to Changes in XDM Resources*".

A CMS shall support handling a SIP SUBSCRIBE request containing subscription to multiple documents simultaneously from CMC and MCPTT Server according to procedures specified in OMA OMA-TS-XDM_Core-V2_1 [2] "*Procedures at the Subscription Proxy*".

7 Configuration management documents

7.1 Introduction

This subclause defines the structure, default document namespace, AUID, XML schema, MIME type, validation constraints and data semantics of the following documents:

- MCPTT UE initial configuration document;
- MCPTT UE configuration document;
- MCPTT user profile configuration document; and
- MCPTT service configuration document.

7.2 MCPTT UE initial configuration document

7.2.1 General

The MCPTT UE initial configuration document is specified in this subclause. The MCPTT UE initial configuration document content is based on requirements of Annex B.6 of 3GPP TS 23.179 [8], and structure and procedures of OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCPTT UE initial configuration in the MCPTT service is described in 3GPP TS 24.379 [9] and 3GPP TS 24.380 [10]. The schema definition is provided in subclause 7.2.2.3. A MCPTT UE initial configuration document may apply to all MCPTT UEs of a mission critical organization or apply to specific MCPTT UEs identified by the optional <mcptt-ue-id> element. If the MCPTT UE is to be configured with a specific MCPTT UE initial configuration document that document is identified by comparing the instance ID of the MCPTT UE with the criteria in the <mcptt-ue-id> element.

7.2.2 Coding

7.2.2.1 Structure

The MCPTT UE initial configuration document structure is specified in this subclause.

The <mcptt-UE- initial-configuration> document:

- 1) shall include a "domain" attribute;
- 2) may include a list of <mcptt-UE-id> elements;
- 3) may include a <name> element;
- 4) may include a <Default-user-profile> element;
- 5) shall include a <common> element;
- 6) shall include an <on-network> element;
- 7) shall include an <off-network> element; and
- 8) may include any other attribute for the purposes of extensibility.

The <Default-user-profile> element shall contain:

- 1) a "User-ID" attribute; and
- 2) a "user-profile-index" attribute.

The <on-network> element:

- 1) shall contain a <Timers> element containing:
 - a) a <T100> element;
 - b) a <T101> element;
 - c) a <T103> element;
 - d) a <T104> element; and
 - e) a <T132> element;
- 2) shall contain an <HPLMN> element containing:
 - a) a "PLMN" attribute;
 - b) a <service> element; and
 - c) a list of <VPLMN> elements;
- 3) shall contain an <App-Server-Info> element containing:
 - a) an <idms> element;
 - b) a <gms> element;
 - c) a <cms> element; and
 - d) a <kms> element; and
- 4) shall contain a <GMS-URI> element.

The <off-network> element:

- 1) shall contain a <Timers> element containing:

- a) a <TFG1> element;
 - b) a <TFG2> element;
 - c) a <TFG3> element;
 - d) a <TFG4> element;
 - e) a <TFG5> element.
 - f) a <TFG11> element;
 - g) a <TFG12> element;
 - h) a <TFG13> element;
 - i) a <TFP1> element;
 - j) a <TFP2> element;
 - k) a <TFP3> element;
 - l) a <TFP4> element;
 - m) a <TFP5> element;
 - n) a <TFP6> element;
 - o) a <TFP7> element;
 - p) a <TFB1> element;
 - q) a <TFB2> element;
 - r) a <TFB3> element;
 - s) a <T201> element;
 - t) a <T203> element;
 - u) a <T204> element;
 - v) a <T205> element;
 - w) a <T230> element;
 - x) a <T233> element;
 - y) a <TFE1> element; and
 - z) a <TFE2> element; and
- 2) shall contain a <Counters> element containing:
- a) a <CFP1> element;
 - b) a <CFP3> element;
 - c) a <CFP4> element;
 - d) a <CFP6> element;
 - e) a <CFG11> element.
 - f) a <CFG12> element;
 - g) a <C201> element;
 - h) a <C204> element; and

i) a <C205> element.

The <VPLMN> element shall contain:

- 1) a "PLMN" attribute; and
- 2) a <service> element.

The <service> element of the <HPLMN> element and the <VPLMN> element shall contain:

- 1) an <MCPTT-to-con-ref> element;
- 2) an <MC-common-core-to-con-ref> element; and
- 3) an <MC-ID-to-con-ref> element.

The <mcptt-UE-id> element.

Editor's Note: The format of the <mcptt-UE-id> that contains the identity(s) of the MCPTT UE(s) for whom this configuration is intended is FFS

7.2.2.2 Application Unique ID

The AUID shall be set to "org.3gpp.mcptt.ue-init-config".

7.2.2.3 XML Schema

Editor's Note: XML schema needs to be provided

7.2.2.4 Default Document Namespace

The default document namespace used in expanding URIs shall be "urn:3gpp:ns:mcpttUEinitConfig:1.0" defined in subclause 7.2.2.3.

7.2.2.5 MIME type

The MIME type for the service configuration document shall be "vnd.3gpp.mcptt-ue-init-config+xml".

7.2.2.6 Validation Constraints

If the AUID value of the document URI or node URI in the Request-URI is other than that specified in subclause 7.5.2.2, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid application id used".

If the XUI value of the document URI or node URI in the Request-URI does not match the XUI of the MCPTT UE initial configuration document URI, the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid XUI".

The MCPTT UE initial configuration document shall conform to the XML Schema described in subclause 7.3.2.3.

The <mcptt-UE-initial-configuration> element is the root element of the XML document. The <mcptt-UE-initial-configuration> element can contain sub-elements.

The <mcptt-UE-initial-configuration> element shall contain one <on-network> element and one <off-network> element.

If the <mcptt-UE-initial-configuration> element does not conform to one of the three choices above, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the "domain" attribute does not contain a syntactically correct domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect domain name".

If the "domain" attribute contains an unknown domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "unknown domain name".

If the "User-ID" attribute of the <Default-user-profile> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect User ID URI".

If any of the following elements of the <Timers> element of the <on-network> element do not conform to the range of values specified below:

- a) the <T100> element contains an integer value between 0 and 255;
- b) the <T101> element contains an integer value between 0 and 255;
- c) the <T103> element contains an integer value between 0 and 255;
- d) the <T104> element contains an integer value between 0 and 255;
- e) the <T132> element contains an integer value between 0 and 255,

then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect timer value" and also contain the identity of the non-conformant timer (e.g. "T101").

If the <idms> element of the <AppServerInfo> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect identity management server URI".

If the <gms> element of the <AppServerInfo> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect group management server URI".

If the <cms> element of the <AppServerInfo> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect configuration management server URI".

If the <kms> element of the <AppServerInfo> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect key management server URI".

If the <GMS-URI> element of the <on-network> element does not conform to a valid URI as specified in 3GPP TS 23.003 [X], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect GMS-URI".

If the "PLMN" attribute of the <HPLMN> element does not conform to the syntax of a valid PLMN code as defined in 3GPP TS 23.003 [X] then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect HPLMN value".

If the "PLMN" attribute of a <VPLMN> element then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect VPLMN value" and also contain the contents of the non-conformant "PLMN" attribute.

If any of the following elements of the <Timers> element of the <off-network> element do not conform to the range of values specified below:

- a) the <TFG1> element contains an integer value between 0 and 65535;
- b) the <TFG2> element contains an integer value between 0 and 65535;
- c) the <TFG3> element contains an integer value between 0 and 65535;
- d) the <TFG4> element contains an integer value between 0 and 60;
- e) the <TFG5> element contains an integer value between 0 and 255;
- f) the <TFG11> element contains an integer value between 0 and 255;
- g) the <TFG12> element contains an integer value between 0 and 255;
- h) the <TFG13> element contains an integer value between 0 and 255;
- i) the <TFP1> element contains an integer value between 0 and 65535;
- j) the <TFP2> element contains an integer value between 0 and 60;
- k) the <TFP3> element contains an integer value between 0 and 65535;
- l) the <TFP4> element contains an integer value between 0 and 65535;
- m) the <TFP5> element contains an integer value between 0 and 600;
- n) the <TFP6> element contains an integer value between 0 and 65535;
- o) the <TFP7> element contains an integer value between 0 and 255;
- p) the <TFB1> element contains an integer value between 0 and 600;
- q) the <TFB2> element contains an integer value between 0 and 10;
- r) the <TFB3> element contains an integer value between 0 and 60;
- s) the <T201> element contains an integer value between 0 and 255;
- t) the <T203> element contains an integer value between 0 and 255;
- u) the <T204> element contains an integer value between 0 and 255;
- v) the <T205> element contains an integer value between 0 and 255;
- w) the <T230> element contains an integer value between 0 and 255;
- x) the <T233> element contains an integer value between 0 and 255;
- y) the <TFE1> element contains an integer value between 0 and 60;
- z) the <TFE2> element contains an integer value between 0 and 10,

then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect timer value" and also contain the identity of the non-conformant timer (e.g. "TFG1").

If any of the following elements of the <Counters> element of the <off-network> element do not conform to the range of values specified below:

- a) the <CFP1> element contains an integer value between 0 and 255;
- b) the <CFP3> element contains an integer value between 0 and 255;
- c) the <CFP4> element contains an integer value between 0 and 255;
- d) the <CFP6> element contains an integer value between 0 and 255;

- e) the <CFP11> element contains an integer value between 0 and 255;
- f) the <CFP12> element contains an integer value between 0 and 255;
- g) the <C201> element contains an integer value between 0 and 255;
- h) the <C204> element contains an integer value between 0 and 255;
- i) the <C205> element contains an integer value between 0 and 255,

then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect counter value" and also contain the identity of the non-conformant counter (e.g. "CFP1").

7.2.2.7 Data Semantics

The "domain" attribute of the <mcptt-UE-initial-configuration> element contains the domain name of the mission critical organization.

Editor's Note: The semantics of the <mcptt-UE-id is FFS

The <name> element of the <mcptt-UE-initial-configuration> element contains the user displayable name of the MCPTT UE initial configuration document and corresponds to the "Name" element of subclause 8.2.3 in 3GPP TS 24.383 [4].

The "User-ID" attribute of the <Default-user-profile> element contains the XUI contained in the "XUI-URI" attribute of the user profile that is intended to be used as default user profile as defined in subclause 7.4.2.1 and corresponds to the "UserID" element of subclause 8.2.6 in 3GPP TS 24.383 [4].

The "user-profile-index" attribute of the <Default-user-profile> element contains an indicator for the particular user profile document when multiple user profiles are defined for that user and is of type "token" and matches a value in a "user-profile-index" attribute of the user profile that is intended to be used as default user profile as defined in subclause 7.4.2.1. and corresponds to the "UserProfileIndex" element of subclause 8.2.X in 3GPP TS 24.383 [4]

The <on-network> element contains MCPTT UE initial configuration data for on-network service only.

The <off-network> element contains MCPTT UE initial configuration data for off-network service only.

In the <on-network> element:

- 1) the <Timers> element;
 - a) the <T100> element contains the timer value in seconds for floor release as specified in 3GPP TS 24.380 [10] and corresponds to the "T100" element of subclause 8.2.12 in 3GPP TS 24.383 [4];
 - b) the <T101> element contains the timer value in seconds for floor request as specified in 3GPP TS 24.380 [10] and corresponds to the "T101" element of subclause 8.2.13 in 3GPP TS 24.383 [4];
 - c) the <T103> element contains the timer value in seconds for end of RTP media as specified in 3GPP TS 24.380 [10] and corresponds to the "T103" element of subclause 8.2.14 in 3GPP TS 24.383 [4];
 - d) the <T104> element contains the timer value in seconds for floor queue position request as specified in 3GPP TS 24.380 [10] and corresponds to the "T104" element of subclause 8.2.15 in 3GPP TS 24.383 [4]; and
 - e) the <T132> element contains the timer value in seconds for queued request granted MCPTT user action as specified in 3GPP TS 24.380 [10] and corresponds to the "T132" element of subclause 8.2.16 in 3GPP TS 24.383 [4].
- 2) the "PLMN" attribute of the <HPLMN> element contains the PLMN code of the HPLMN as defined in 3GPP TS 23.003 [X] and corresponds to the "PLMN" element of subclause 8.2.18 in 3GPP TS 24.383 [4];
- 3) the "PLMN" attribute of the <VPLMN> element contains the PLMN code of a VPLMN as defined in 3GPP TS 23.003 [X] and corresponds to the "PLMN" element of subclause 8.2.30 in 3GPP TS 24.383 [4];
- 4) the <AppServerInfo> element:

- a) the <idms> element contains the URI used to contact the identity management server and corresponds to the "IDMS" element of subclause 8.2.42 in 3GPP TS 24.383 [4];
 - b) the <gms> element contains the URI used to contact the group management server and corresponds to the "GMS" element of subclause 8.2.43 in 3GPP TS 24.383 [4];
 - c) the <cms> element contains the URI used to contact the configuration management server and corresponds to the "CMS" element of subclause 8.2.44 in 3GPP TS 24.383 [4]; and
 - d) the <kms> element contains the URI used to contact the key management server and corresponds to the "KMS" element of subclause 8.2.45 in 3GPP TS 24.383 [4]; and
- 5) the <GMS-URI> element contains the group management service URI information to enable hiding of MCPTT ID (or MCPTT group ID) and corresponds to the "GMSURI" element of subclause 8.2.9 in 3GPP TS 24.383 [4].

In the <off-network> element:

- 1) the <Timers> element:
 - a) the <TFG1> element contains the timer value in milliseconds for wait for call announcement as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG1" element of subclause 8.2.48 in 3GPP TS 24.383 [4];
 - b) the <TFG2> element contains the timer value in milliseconds for call announcement as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG2" element of subclause 8.2.49 in 3GPP TS 24.383 [4];
 - c) the <TFG3> element contains the timer value in milliseconds for call probe retransmission as specified in 3GPP TS 24.379 [9]; and corresponds to the "TFG3" element of subclause 8.2.50 in 3GPP TS 24.383 [4]
 - d) the <TFG4> element contains the timer value in seconds for waiting for the MCPTT user as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG4" element of subclause 8.2.51 in 3GPP TS 24.383 [4];
 - e) the <TFG5> element contains the timer value in seconds for not present incoming call announcements as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG5" element of subclause 8.2.52 in 3GPP TS 24.383 [4];
 - f) the <TFG11> element contains the timer value in seconds for MCPTT emergency end retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG11" element of subclause 8.2.53 in 3GPP TS 24.383 [4];
 - g) the <TFG12> element contains the timer value in seconds for MCPTT imminent peril end retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG12" element of subclause 8.2.54 in 3GPP TS 24.383 [4];
 - h) the <TFG13> element contains the timer value in seconds for timer for implicit priority downgrade as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG13" element of subclause 8.2.55 in 3GPP TS 24.383 [4];
 - i) the <TFP1> element contains the timer value in milliseconds for private call request retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP1" element of subclause 8.2.56 in 3GPP TS 24.383 [4];
 - j) the <TFP2> element contains the timer value in seconds for waiting for call response message as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP2" element of subclause 8.2.57 in 3GPP TS 24.383 [4];
 - k) the <TFP3> element contains the timer value in milliseconds for private call release retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP3" element of subclause 8.2.58 in 3GPP TS 24.383 [4];
 - l) the <TFP4> element contains the timer value in milliseconds for private call accept retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP4" element of subclause 8.2.59 in 3GPP TS 24.383 [4];
 - m) the <TFP5> element contains the timer value in seconds for call release as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP5" element of subclause 8.2.60 in 3GPP TS 24.383 [4];

- n) the <TFP6> element contains the timer value in milliseconds for MCPTT emergency private call cancel retransmission as specified as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP6" element of subclause 8.2.61 in 3GPP TS 24.383 [4];
 - o) the <TFP7> element contains the timer value in seconds for waiting for any message with same call identifier as specified in 3GPP TS 24.379 [9] and corresponds to the "TFP7" element of subclause 8.2.62 in 3GPP TS 24.383 [4];
 - p) the <TFB1> element contains the timer value in seconds for max duration as specified in 3GPP TS 24.379 [9] and corresponds to the "TFB1" element of subclause 8.2.63 in 3GPP TS 24.383 [4];
 - q) the <TFB2> element contains the timer value in seconds for broadcast retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFB2" element of subclause 8.2.64 in 3GPP TS 24.383 [4];
 - r) the <TFB3> element contains the timer value in seconds for waiting for the MCPTT user as specified in 3GPP TS 24.379 [9] and corresponds to the "TFB3" element of subclause 8.2.65 in 3GPP TS 24.383 [4];
 - s) the <T201> element contains the timer value in seconds for floor request as specified in 3GPP TS 24.380 [10] and corresponds to the "T201" element of subclause 8.2.66 in 3GPP TS 24.383 [4];
 - t) the <T203> element contains the timer value in seconds for end of RTP media as specified in 3GPP TS 24.380 [10] and corresponds to the "T203" element of subclause 8.2.67 in 3GPP TS 24.383 [4];
 - u) the <T204> element contains the timer value in seconds for floor queue position request as specified in 3GPP TS 24.380 [10] and corresponds to the "T204" element of subclause 8.2.68 in 3GPP TS 24.383 [4];
 - v) the <T205> element contains the timer value in seconds for floor granted request as specified in 3GPP TS 24.380 [10] and corresponds to the "T205" element of subclause 8.2.69 in 3GPP TS 24.383 [4];
 - w) the <T230> element contains the timer value in seconds for during silence as specified in 3GPP TS 24.380 [10] and corresponds to the "T230" element of subclause 8.2.70 in 3GPP TS 24.383 [4];
 - x) the <T233> element contains the timer value in seconds for pending user action as specified in 3GPP TS 24.380 [10] and corresponds to the "T233" element of subclause 8.2.71 in 3GPP TS 24.383 [4];
 - y) the <TFE1> element contains the timer value in seconds for MCPTT emergency alert as specified in 3GPP TS 24.380 [10] and corresponds to the "TFE1" element of subclause 8.2.72 in 3GPP TS 24.383 [4]; and
 - z) the <TFE2> element contains the timer value in seconds for MCPTT emergency alert retransmission as specified in 3GPP TS 24.380 [10] and corresponds to the "TFE2" element of subclause 8.2.73 in 3GPP TS 24.383 [4]; and
- 2) the <Counters> element.
- a) the <CFP1> element contains the counter value for private call request retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP1" element of subclause 8.2.75 in 3GPP TS 24.383 [4];
 - b) the <CFP3> element contains the counter value for private call release retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP3" element of subclause 8.2.76 in 3GPP TS 24.383 [4];
 - c) the <CFP4> element contains the counter value for private call accept retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP4" element of subclause 8.2.77 in 3GPP TS 24.383 [4];
 - d) the <CFP6> element contains the counter value for private call accept retransmission t as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP6" element of subclause 8.2.78 in 3GPP TS 24.383 [4];
 - e) the <CFP11> element contains the counter value for MCPTT group call emergency end retransmission ia as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP11" element of subclause 8.2.79 in 3GPP TS 24.383 [4];
 - f) the <CFP12> element contains the counter value for MCPTT imminent peril call emergency end retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "CFP12" element of subclause 8.2.80 in 3GPP TS 24.383 [4];

- g) the <C201> element contains the counter value for floor request as specified in 3GPP TS 24.380 [10] and corresponds to the "C201" element of subclause 8.2.81 in 3GPP TS 24.383 [4];
- h) the <C204> element contains the counter value for floor queue position request as specified in 3GPP TS 24.380 [10] and corresponds to the "C204" element of subclause 8.2.82 in 3GPP TS 24.383 [4]; and
- i) the <C205> element contains the counter value for floor granted request as specified in 3GPP TS 24.380 [10] and corresponds to the "C205" element of subclause 8.2.83 in 3GPP TS 24.383 [4].

7.2.2.8 Naming Conventions

The present document defines no naming conventions.

7.2.2.9 Global documents

The present document requires no global documents.

7.2.2.10 Resource interdependencies

There are no resource interdependencies.

7.2.2.11 Authorization Policies

The authorization policies for manipulating an MCPTT UE initial configuration document shall conform to those described in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 5.1.5 "*Authorization*".

7.2.2.12 Subscription to Changes

The MCPTT UE initial configuration document application usage shall support subscription to changes as specified in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 6.2.2 "*Subscriptions to changes in the XDM Resources*".

7.3 MCPTT UE configuration document

7.3.1 General

The MCPTT UE configuration document is specified in this subclause. The MCPTT UE configuration document content is based on requirements of Annex B.2 of 3GPP TS 23.179 [8], and structure and procedures of OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCPTT UE configuration in the MCPTT service is described in 3GPP TS 24.379 [9] and 3GPP TS 24.380 [10]. The schema definition is provided in subclause 7.3.2.3. Each MCPTT UE of a mission critical organization is configured with an MCPTT UE configuration document that is identified by the instance ID of the MCPTT UE.

7.3.2 Coding

7.3.2.1 Structure

The MCPTT UE configuration document structure is specified in this subclause.

The <mcptt-UE-configuration> document:

- 1) shall include a "domain" attribute;
- 2) may include a list of <mcptt-UE-id> elements;
- 3) may include a <common> element;
- 4) may include an <on-network> element; and

5) may include any other attribute for the purposes of extensibility.

The <common> element:

- 1) shall contain a <private-call> element containing:
 - a) a <Max-Simul-Call-N10> element; and
- 2) shall contain an <MCPTT-Group-Call> element containing:
 - a) a <Max-Simul-Call-N4> element;
 - b) a <Max-Simul-Trans-N5> element; and
 - c) a <Prioritized-MCPTT-Group> element containing:
 - i) a list of <MCPTT-Group-Priority> elements containing:
 - 1) an <MCPTT-Group-ID> element; and
 - 2) a <group-priority-hierarchy> element.

The <on-network> element:

- 1) shall contain a <IPv6Preferred> element;
- 2) shall contain a <Relay-Service> element; and
- 3) shall contain a list of <Relayed-MCPTT-Group> elements containing:
 - a) a <MCPTT-Group-ID> element; and
 - b) a <Relay-Service-Code> element.

The <mcptt-UE-id> element:

Editor's Note: The format of the <mcptt-UE-id> that contains the identity(s) of the MCPTT UE(s) for whom this configuration is intended is FFS

7.3.2.2 Application Unique ID

The AUID shall be set to "org.3gpp.mcptt.ue-config".

7.3.2.3 XML Schema

Editor's Note: XML schema needs to be provided

7.3.2.4 Default Document Namespace

The default document namespace used in expanding URIs shall be "urn:3gpp:ns:mcpttUEConfig:1.0" defined in subclause 7.3.2.3.

7.3.2.5 MIME type

The MIME type for the service configuration document shall be "vnd.3gpp.mcptt-ue-config+xml".

7.3.2.6 Validation Constraints

If the AUID value of the document URI or node URI in the Request-URI is other than that specified in subclause 7.3.2.2, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid application id used".

If the XUI value of the document URI or node URI in the Request-URI does not match the XUI of the service configuration document URI, the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid XUI".

The MCPTT UE configuration document shall conform to the XML Schema described in subclause 7.3.2.3.

The <mcptt-UE-configuration> element is the root element of the XML document. The <mcptt-UE-configuration> element can contain sub-elements.

The <mcptt-UE-configuration> element shall contain either:

- 1) one <common> element only;
- 2) one <common> element and one <on-network> element; or
- 3) one <on-network> element only.

If the <mcptt-UE-configuration> element does not conform to one of the three choices above, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the "domain" attribute does not contain a syntactically correct domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect domain name".

If the "domain" attribute contains an unknown domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "unknown domain name".

Editor's Note: The validation of the <mcptt-UE-id> is FFS

If the <Max-Simul-Call-N10> element of the <private-call> element contains a value less than 1 and greater than 4, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

If the <Max-Simul-Call-N4> element, or <Max-Simul-Trans-N5> element of the <MCPTT-Group-Call> element contains a value less than 1, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

If the <MCPTT-Group-ID> element of the <MCPTT-group-priority> element or <Relayed-MCPTT-Group> element does not conform to the syntax of a "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1[17], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the <group-priority-hierarchy> element of the <MCPTT-group-priority> element contains a value less than 8 and greater than or equal to 0, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

If the <Relay-Service> element of the <On-Network> element does not contain a value of "true" or "false", then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

If the <Relay-Service-Code> element of the <Relayed-MCPTT-Group> element does not conform to the syntax of a valid Relay service code as defined in 3GPP TS 24.333 [12], then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the <IPv6-Preferred> element of the <On-Network> element does not contain a value of "true" or "false", then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

7.3.2.7 Data Semantics

The "domain" attribute of the <mcptt-UE-configuration> element contains the domain name of the mission critical organization.

Editor's Note: The semantics of the <mcptt-UE-id> is FFS

The <common> element contains MCPTT UE configuration data common to both on and off network service.

The <on-network> element contains MCPTT UE configuration data for on-network service only.

In the <common> element:

- 1) the <Max-Simul-Call-N10> element of the <private-call> element contains an integer indicating the maximum number of simultaneous calls (N10) allowed for an on-network or off-network private call with floor control and corresponds to the "MaxCallN10" element of subclause 4.2.7 in 3GPP TS 24.383 [4];
- 2) the <Max-Simul-Call-N4> element of the <MCPTT-Group-Call> element contains an integer indicating the number of simultaneous calls (N4) allowed for an on-network or off-network group call and corresponds to the "MaxCallN4" element of subclause 4.2.9 in 3GPP TS 24.383 [4];
- 3) the <Max-Simul-Trans-N5> element of the <MCPTT-Group-Call> element contains an integer indicating the maximum number of allowed simultaneous transmissions for an on-network or off-network group call and corresponds to the "MaxTransmissionN5" element of subclause 4.2.10 in 3GPP TS 24.383 [4]; and
- 4) the <Prioritized-MCPTT-Group> element of the <MCPTT-Group-Call> element corresponds to the "PrioritizedMCPTTGroup" element of subclause 4.2.11 in 3GPP TS 24.383 [4] contains a list of <MCPTT-Group-Priority> elements that contains:
 - a) <MCPTT-Group-ID> element identifying an MCPTT group that corresponds to the "MCPTTGroupID" element of subclause 4.2.13 in 3GPP TS 24.383 [4]; and
 - b) a <group-priority-hierarchy> element that contains an integer that identifies the relative priority level of that MCPTT group with 0 being the lowest priority and 7 being the highest priority and corresponds to the "MCPTTGroupPriorityHierarchy" element of subclause 4.2.14 in 3GPP TS 24.383 [4].

In the <on-network> element:

- 1) if the <Relay-Service> element is set to "true" the MCPTT UE is allowed to offer a relay service, and if set to "false" the MCPTT UE is not allowed to offer relay service. This attribute corresponds to the "OfferRelayService" element of subclause 4.2.16 in 3GPP TS 24.383 [4];
- 2) an <IPv6Preferred> element which corresponds to the "IPv6Preferred" element of subclause 4.2.17 in 3GPP TS 24.383 [4],
 - a) if the UE has both IPv4 and IPv6 host configuration::
 - i) if IPv6Preferred is set to true then the UE shall user IPv6 for all on-network signalling and media; otherwise
 - ii) if IPv6Preferred is set to false then the UE shall user IPv4 for all on-network signalling and media;
 - b) if the UE has only IPv4 host configuration then the UE shall user IPv4 for all on-network signalling and media; and
 - c) if the UE has only IPv6 host configuration then the UE shall user IPv6 for all on-network signalling and media; and
- 2) the <Relayed-MCPTT-Groups> element of the <Relay-Service> element which corresponds to the "RelayedMCPTTGroup" element of subclause 4.2.18 in 3GPP TS 24.383 [4] contains:
 - a) a list of <Relay-MCPTT-Group-ID> elements that contains:
 - i) "MCPTT-Group-ID" attribute identifying an MCPTT group that is allowed to be used via a relay and corresponds to the "MCPTTGroupID" element of subclause 4.2.20 in 3GPP TS 24.383 [4]; and

- ii) a <Relay-Service-Code> element as specified in 3GPP TS 24.333 [12] which corresponds to the "RelayServiceCode" element of subclause 4.2.21 in 3GPP TS 24.383 [4].

7.3.2.8 Naming Conventions

The present document defines no naming conventions.

7.3.2.9 Global documents

The present document requires no global documents.

7.3.2.10 Resource interdependencies

There are no resource interdependencies.

7.3.2.11 Authorization Policies

The authorization policies for manipulating an MCPTT UE configuration document shall conform to those described in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 5.1.5 "Authorization".

7.3.2.12 Subscription to Changes

The MCPTT UE configuration document application usage shall support subscription to changes as specified in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 6.2.2 "Subscriptions to changes in the XDM Resources".

7.4 MCPTT user profile configuration document

7.4.1 General

The user profile configuration document is specified in this subclause. The MCPTT user profile configuration document content is based on requirements of Annex B.3 of 3GPP TS 23.179 [8], and structure and procedures of OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCPTT user profile in the MCPTT service is described in 3GPP TS 24.379 [9]. The schema definition is provided in subclause 7.4.2.

7.4.2 Coding

7.4.2.1 Structure

The user profile configuration document structure is specified in this subclause.

The <user-profile> document:

- 1) shall include an "XUI-URI" attribute that contains the XUI of the user for whom this user profile configuration document is intended;
- 2) shall include a "user-profile-index" attribute that indicates the particular user profile configuration document in the collection;
- 3) may include any other attribute for the purposes of extensibility;
- 4) may include one <ProfileName> element specifying the name of the user profile configuration document;
- 5) may include zero or more <common> elements, each of which:
 - a) shall have an "index" attribute for uniqueness purposes;
 - b) shall include one <UserAlias> element containing one or more <alias-entry> elements, each indicating an alphanumeric alias of the user. Each <alias-entry> element shall have an "index" attribute for uniqueness purposes;

- c) shall include one <MCPTTUserID> element that contains a <uri-entry> that contains the MCPTT User ID , which is a URI, and may contain a <display-name> element with a human readable name;
- d) shall include one <MaxAffiliations> element indicating the maximum number of group affiliations of the user;
- e) shall include one <PrivateCall> element. The <PrivateCall> element contains one or more <entry> elements indicating users who can be called in a private call. Each <entry> element shall contain a <uri-entry> element containing either a SIP URI or a TEL URI set to a valid user address, and may contain a <display-name> child string element containing a human readable name;
- f) shall contain one <MCPTT-group-call> element containing:
 - i) one <MaxCalls> element indicating the maximum number of simultaneously received group calls;
 - ii) one <MaxTransmissions> element indicating the maximum number of simultaneous transmissions received in one group call;
 - iii) one <EmergencyCall> element containing:
 - A) one <MCPTTGroupInitiation> element indicating the group to be used for initiation of an MCPTT emergency group call. The <MCPTTGroupInitiation> element shall contain a <uri-entry> element containing an MCPTT Group Identity, which is a URI, and may contain a <display-name> string element containing a human readable name of the group; and
 - B) one <Recipient> element containing one or more <entry> element, each containing a <uri-entry> element containing either a SIP URI or TEL URI of a recipient for an emergency private call, and may contain a <display-name> string element. Each <entry> element shall have an "index" attribute;
 - iv) one <ImminentPerilCall> element containing:
 - A) one <MCPTTGroupInitiation> element containing a <uri-entry> element containing the MCPTT Group ID, which is a URI, to be used for initiation of an MCPTT imminent peril group call, and may contain a <display-name> with a human readable name of the group; and
 - v) one <EmergencyAlert> element containing:
 - A) a <Recipient> element containing a list of <entry> elements containing a <uri-entry> element containing either a SIP URI or TEL URI of a recipient for an emergency alert, and may contain a <display-name> string element containing a human readable name. Each <entry> element shall have an "index" attribute; and
- g) shall contain one <Priority> element indicating the priority for the user initiating or receiving calls;
- 6) shall include zero or more <OffNetwork> elements each of which:
 - a) shall have an "index" attribute for uniqueness purposes; and
 - b) shall include one or more <MCPTTGroupInfo> elements, each containing one or more <entry> elements. Each <entry> element shall contain a <uri-entry> element with an MCPTT Group ID, and may contain a <display-name> element with a human readable name of the group. Each <MCPTTGroupInfo> and each <entry> element shall have an "index" attribute;
- 7) shall include zero or more <OnNetwork> elements each of which:
 - a) shall have an "index" attribute for uniqueness purposes;
 - b) shall include one or more <MCPTTGroupInfo> elements, each containing one or more <entry> elements. Each <entry> element shall contain a <uri-entry> element with an MCPTT Group ID, and may contain a <display-name> element with a human readable name of the group. Each <MCPTTGroupInfo> and each <entry> element shall have an "index" attribute;
 - c) shall include one User Info ID containing a URI in accordance with 3GPP TS 24.333 [12];
 - d) shall include one <MaxAffiliations> element indicating the maximum number of group affiliations of the user; and

- e) shall include one or more <ImplicitAffiliations> elements, each containing one or more <entry> elements. Each <entry> element shall contain a <uri-entry> element with an MCPTT Group ID to which the MCPTT user requests to be implicitly affiliated. Each <entry> element may contain a <display-name> element with a human readable name of the group. Each <ImplicitAffiliations> and each <entry> element shall have an "index" attribute;
- 8) a <ruleset> element conforming to IETF RFC 4745 [13] containing a sequence of zero or more <rule> elements:
 - a) the <conditions> of a <rule> element may include the <identity> element as described in IETF RFC 4745 [13];
 - b) the <actions> child element of any <rule> element may contain:
 - i) an <allow-private-call> element indicating the user is authorized to make a private call;
 - ii) an <allow-manual-commencement> element indicating the user is authorized to make a private call with manual commencement;
 - iii) an <allow-automatic-commencement> element indicating the user is authorized to make a private call with automatic commencement;
 - iv) an <allow-force-auto-answer> element indicating the user is authorized to force automatic answer for a private call;
 - v) an <allow-failure-restriction> element indicating the user is authorized to restrict notification of a call failure reason for a private call;
 - vi) an <allow-emergency-group-call> element indicating the user is authorized to make an emergency group call;
 - vii) an <allow-emergency-private-call> element indicating the user is authorized to make an emergency private call;
 - viii) an <allow-cancel-group-emergency> element indicating the user is authorized to cancel an emergency with this group;
 - ix) an <allow-cancel-private-emergency-call> element indicating the user is authorized to cancel a private emergency call;
 - x) an <allow-imminent-peril-call> element indicating the user is authorized to make an imminent peril group call;
 - xi) an <allow-cancel-imminent-peril> element indicating the user is authorized to cancel an imminent peril group call;
 - xii) an <allow-activate-emergency-alert> element indicating the user is authorized to activate an emergency alert;
 - xiii) an <allow-cancel-emergency-alert> element indicating the user is authorized to cancel an emergency alert;
 - xiv) an <allow-offnetwork> element indicating the user is authorized for off-network services;
 - xv) an <allow-imminent-peril-change> element that indicates the user is authorized to change an off-network group call in progress to an off-network imminent peril group call;
 - xvi) an <allow-private-call-media-protection> element indicating that confidentiality and integrity of media is applied for all on-network and off-network private calls; and
 - xvii) an <allow-private-call-floor-control-protection> element indicating that confidentiality and integrity of floor control signalling is applied for all on-network and off-network private calls; and
- 9) may include any other element for the purposes of extensibility.

7.4.2.2 Application Unique ID

The AUID shall be "org.3gpp.mcptt.user-profile".

7.4.2.3 XML Schema

The userprofile configuration document shall be composed according to the following XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns="urn:3gpp:mcptt:user-profile:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:mcptt:user-profile:1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
    schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <xs:element name="user-profile">
    <xs:complexType>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="ProfileName" type="ProfileNameType"/>
        <xs:element name="Common" type="CommonType"/>
        <xs:element name="OffNetwork" type="OffNetworkType"/>
        <xs:element name="OnNetwork" type="OnNetworkType"/>
        <xs:any namespace="##other" processContents="lax"/>
      </xs:choice>
      <xs:attribute name="XUI-URI" type="xs:anyURI" use="required"/>
      <xs:attribute name="user-profile-index" type="xs:anyURI" use="required"/>
      <xs:anyAttribute processContents="lax"/>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="ProfileNameType">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attribute ref="xml:lang"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="CommonType">
    <xs:choice minOccurs="1" maxOccurs="unbounded">
      <xs:element name="UserAlias" type="UserAliasType"/>
      <xs:element name="MCPTTUserID" type="EntryType"/>
      <xs:element name="MaxAffililations" type="xs:nonNegativeInteger"/>
      <xs:element name="PrivateCall" type="ListEntryType"/>
      <xs:element name="MCPTT-group-call" type="MCPTTGroupCallType"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:anyAttribute processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="UserAliasType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="alias-entry" type="AliasEntryType"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:attributeGroup ref="IndexType"/>
    <xs:anyAttribute processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="AliasEntryType">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attributeGroup ref="IndexType"/>
        <xs:attribute ref="xml:lang"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="ListEntryType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="entry" type="EntryType"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:attribute ref="xml:lang"/>
  </xs:complexType>
```

```

    <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="EntryType">
  <xs:sequence>
    <xs:element name="uri-entry" type="xs:anyURI" />
    <xs:element name="display-name" type="DisplayNameElementType" minOccurs="0" maxOccurs="1" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:sequence>
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="DisplayNameElementType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute ref="xml:lang" />
      <xs:anyAttribute processContents="lax" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="MCPTTGroupCallType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MaxCalls" type="xs:positiveInteger" />
    <xs:element name="MaxTransmissions" type="xs:positiveInteger" />
    <xs:element name="EmergencyCall" type="EmergencyCallType" />
    <xs:element name="ImminentPerilCall" type="ImminentPerilCallType" />
    <xs:element name="EmergencyAlert" type="EmergencyAlertType" />
    <xs:element name="Priority" type="xs:nonNegativeInteger" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:choice>
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="EmergencyCallType">
  <xs:sequence>
    <xs:element name="MCPTTGroupInitiation" type="EntryType" />
    <xs:element name="Recipient" type="ListEntryType" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:sequence>
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="ImminentPerilCallType">
  <xs:sequence>
    <xs:element name="MCPTTGroupInitiation" type="EntryType" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:sequence>
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="EmergencyAlertType">
  <xs:sequence>
    <xs:element name="Recipient" type="ListEntryType" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:sequence>
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="OffNetworkType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MCPTTGroupInfo" type="ListEntryType" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:choice>
  <xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:complexType name="OnNetworkType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MCPTTGroupInfo" type="ListEntryType" />
    <xs:element name="UserInfoID" type="xs:anyURI" />
    <xs:element name="MaxAffiliations" type="xs:nonNegativeInteger" />
    <xs:element name="ImplicitAffiliations" type="ListEntryType" />
    <xs:element name="PrivateCall" type="ListEntryType" />
    <xs:any namespace="##other" processContents="lax" />
  </xs:choice>

```

```
<xs:anyAttribute processContents="lax" />
</xs:complexType>

<xs:attributeGroup name="IndexType">
  <xs:attribute name="index" type="xs:token" />
</xs:attributeGroup>
</xs:schema>
```

7.4.2.4 Default Namespace

The default namespace used in expanding URIs shall be "urn:3gpp:mcptt:user-profile:1.0" defined in subclause [7.4.2.3](#).

7.4.2.5 MIME type

The MIME type for the user profile configuration document shall be "application/vnd.3gpp.mcptt.user-profile+xml".

7.4.2.6 Validation Constraints

The user profile configuration document shall conform to the XML Schema described in subclause 7.4.2.3 "*XML Schema*", with the clarifications given in this subclause.

The value of the "XUI-URI" attribute of the <user-profile> element shall be the same as the XUI value of the Document URI for the user profile configuration document. If not, the XDMS shall return an HTTP "409 Conflict" response as described in IETF RFC 4825 [14], including the <constraint-failure> error element. If included, the "phrase" attribute SHOULD be set to "Wrong User Profile URI".

The default value for the <allow-private-call-media-protection> element is "true" indicating that confidentiality and integrity of media is applied for all on-network and off-network private calls.

The default value for the <allow-private-call-floor-control-protection> element is "true" indicating confidentiality and integrity of floor control signalling is applied for all on-network and off-network private calls.

7.4.2.7 Data Semantics

The <ProfileName> element is of type "token", and corresponds to the "Name" element of subclause 5.2.3 in 3GPP TS 24.383 [4].

The <alias-entry> element is of type "token", and corresponds to the leaf nodes of the "UserAlias" element of subclause 5.2.8 in 3GPP TS 24.383 [4].

The <display-name> element is of type "string", is optional, and does not appear in the user profile configuration managed object specified in 3GPP TS 24.383 [4].

The <uri-entry> element is of type "anyURI".

The "index" attribute is of type "token".

The "user-profile-index" is of type "token".

The <MCPTTUser ID> element contains the element <uri-entry> which is of type "anyURI", and corresponds to the "MCPTTUserID" element of subclause 5.2.9 in 3GPP TS 24.383 [4].

The <MaxAffiliations> element is of type "nonNegativeInteger", and corresponds to the "MaxAffiliations" element of subclause 5.2.10 in 3GPP TS 24.383 [4].

The <MaxCalls> element is of type "positiveInteger", and corresponds to the "MaxCalls" element of subclause 5.2.19 in 3GPP TS 24.383 [4].

The <MaxTransmissions> element is of type "positiveInteger", and corresponds to the "MaxTransmissions" element of subclause 5.2.20 in 3GPP TS 24.383 [4].

The <Priority> element is of a type "unsignedShort" with a range of 0 to 7 and corresponds to the "Priority" element of subclause 5.2.41 in 3GPP TS 24.383 [4].

The <allow-private-call> element is of type Boolean, as specified in table 7.4.2.7-1, and corresponds to the "Authorized" element of subclause 5.2.12 in 3GPP TS 24.383 [4].

Table 7.4.2.7-1: Values of <allow-private-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request a private call request using procedures as defined by the enabler. The recipient must be a user identified in a <user-entry> element of the <PrivateCall> element, which corresponds to leaf nodes of "UserAuthorized" in subclause 5.2.13 in 3GPP TS 24.383 [4].
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, to reject private call request using procedures as defined by the enabler. This shall be the default value taken in the absence of the element;

The <allow-manual-commencement> element is of type Boolean, as specified in table 7.4.2.7-2, and corresponds to the "ManualCommence" element of subclause 5.2.14 in 3GPP TS 24.383 [4].

Table 7.4.2.7-2: Values of <allow-manual-commencement>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request a private call with manual commencement using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request a private call with manual commencement using procedures as defined by the enabler.

The <allow-automatic-commencement> element is of type Boolean, as specified in table 7.4.2.7-3, corresponds to the "AutoCommence" element of subclause 5.2.15 in 3GPP TS 24.383 [4].

Table 7.4.2.7-3: Values of <allow-automatic-commencement>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request a private call with automatic commencement using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request a private call with automatic commencement using procedures as defined by the enabler.

The <allow-force-auto-answer> element is of type Boolean, as specified in table 7.4.2.7-4, and corresponds to the "AutoAnswer" element of subclause 5.2.16 in 3GPP TS 24.383 [4].

Table 7.4.2.7-4: Values of <allow-force-auto-answer>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request a private call with forced automatic commencement using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request a private call with forced automatic commencement using procedures as defined by the enabler.

The <allow-failure-restriction> element is of type Boolean, as specified in table 7.4.2.7-5, and corresponds to the "FailRestrict" element of subclause 5.2.17 in 3GPP TS 24.383 [4].

Table 7.4.2.7-5: Values of <allow-failure-restriction>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorised to restrict the provision of a notification of call failure reason for private call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorised to restrict the provision of a notification of call failure reason for private call using procedures as defined by the enabler.

The <allow-emergency-group-call> element is of type Boolean, as follows, and corresponds to the "Enabled" element of subclause 5.2.22 in 3GPP TS 24.383 [4].

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request an emergency group call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request an emergency group call using procedures as defined by the enabler.

The <allow-emergency-private-call> element is of type Boolean, as specified in table 7.4.2.7-6, and corresponds to the "Authorized" element of subclause 5.2.23 in 3GPP TS 24.383 [4].

Table 7.4.2.7-6: Values of <allow-emergency-private-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request an emergency private call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request an emergency private call using procedures as defined by the enabler.

The <allow-cancel-group-emergency-call> element is of type Boolean, as specified in table 7.4.2.7-7, and corresponds to the "CancelMCPTTGroup" element of subclause 5.2.25 in 3GPP TS 24.383 [4].

Table 7.4.2.7-7: Values of <allow-cancel-group-emergency-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to cancel an emergency group call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to cancel an emergency group call using procedures as defined by the enabler.

The <allow-cancel-private-emergency-call> element is of type Boolean, as specified in table 7.4.2.7-8, and corresponds to the "CancelPrivate" of subclause 5.2.26 in 3GPP TS 24.383 [4].

Table 7.4.2.7-8: Values of <allow-cancel-private-emergency-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to cancel an emergency private call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to cancel an emergency private call using procedures as defined by the enabler.

The <allow-imminent-peril-call> element is of type Boolean, as specified in table 7.4.2.7-9, and corresponds to the "Authorized" of subclause 5.2.29 in 3GPP TS 24.383 [4].

Table 7.4.2.7-9: Values of <allow-imminent-peril-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to request an imminent peril group call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to request an imminent peril group call using procedures as defined by the enabler.

The <allow-cancel-imminent-peril-call> element is of type Boolean, as specified in table 7.4.2.7-10, and corresponds to the "Cancel" of subclause 5.2.30 in 3GPP TS 24.383 [4].

Table 7.4.2.7-10: Values of <allow-cancel-imminent-peril-call>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to cancel an imminent peril group call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to cancel an imminent peril group call using procedures as defined by the enabler.

The <allow-activate-emergency-alert> element is of type Boolean, as specified in table 7.4.2.7-11, and corresponds to the "Authorized" of subclause 5.2.33 in 3GPP TS 24.383 [4].

Table 7.4.2.7-11: Values of <allow-activate-emergency-alert>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to activate an emergency alert using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to activate an emergency alert using procedures as defined by the enabler.

The <allow-cancel-emergency-alert> element is of type Boolean, as specified in table 7.4.2.7-12, and corresponds to the "Cancel" of subclause 5.2.34 in 3GPP TS 24.383 [4].

Table 7.4.2.7-12: Values of <allow-cancel-emergency-alert>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to cancel an emergency alert using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to cancel an emergency alert using procedures as defined by the enabler.

The <allow-offnetwork> element is of type Boolean, as specified in table 7.4.2.7-13, and corresponds to the "Authorized" of subclause 5.2.42 in 3GPP TS 24.383 [4].

Table 7.4.2.7-13: Values of <allow-offnetwork>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized for off-network service using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized for off-network service using procedures as defined by the enabler.

The <allow-imminent-peril-change> element is of type Boolean, as specified in table 7.4.2.7-14, and corresponds to the "Change" of subclause 5.2.47 in 3GPP TS 24.383 [4].

Table 7.4.2.7-14: Values of <allow-imminent-peril-change>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to change an off-network group call in-progress to an off-network emergency group call using procedures as defined by the enabler.
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to change an off-network group call in-progress to an off-network emergency group call using procedures as defined by the enabler.

The <allow-private-call-media-protection> element is of type Boolean, as specified in table 7.4.2.7-15, and corresponds to the "AllowedMediaProtection" of subclause 5.2.24 in 3GPP 24.383 [4];

Table 7.4.2.7-15: Values of <allow-private-call-media-protection>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to protect the confidentiality and integrity of media for on-network and off-network private calls
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to protect the confidentiality and integrity of media for on-network and off-network private calls

The <allow-private-call-floor-control-protection> element is of type Boolean, as specified in table 7.4.2.7-16, and corresponds to the "AllowedFloorControlProtection" of subclause 5.2.25 in 3GPP 24.383 [4];

Table 7.4.2.7-16: Values of <allow-private-call-floor-control-protection>

"true"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is authorized to protect the confidentiality and integrity of floor control signalling for both on-network and off-network private calls
"false"	instructs the Application Server performing the originating participating MCPTT function for the user, that the user is not authorized to protect the confidentiality and integrity of floor control signalling for both on-network and off-network private calls

7.4.2.8 Naming Conventions

The name of user profile configuration document shall be "user-profile".

7.4.2.9 Global documents

The present document requires no global documents.

7.4.2.10 Resource interdependencies

This Application Usage is interdependent on user profile data in the MCPTT Database and the MCPTT Management Object.

7.4.2.11 Access Permissions Policies

The authorization and access policies for a user profile configuration document shall conform to those described in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 5.1.5 "*Authorization*" and subclause 5.6.7 "*Access Permissions Document*" with the following exceptions:

- 1) The Principal (i.e., the user) of the user profile configuration document shall have permission to create, modify, or delete <alias-entry> child elements of the <UserAlias> elements, if the rule of the Access Permissions document associated with the user profile configuration document contains the action element <allow-any-operation-own-data>, as specified in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 5.6.7 "*Access Permissions Document*".

7.4.2.12 Subscription to Changes

The User Access Policy Application Usage shall support subscription to changes as specified in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 6.2.2 "*Subscriptions to changes in the XDM Resources*".

7.5 MCPTT service configuration document

7.5.1 General

The MCPTT service configuration document is specified in this subclause. The MCPTT service configuration document content is based on requirements of Annex B.5 of 3GPP TS 23.179 [8], and structure and procedures of OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCPTT service configuration in the MCPTT

service is described in 3GPP TS 24.379 [9] and 3GPP TS 24.380 [10]. The schema definition is provided in subclause 7.5.2.3. Each mission critical organization is configured with an MCPTT service configuration document.

7.5.2 Coding

7.5.2.1 Structure

The service configuration document structure is specified in this subclause.

The <service configuration> document:

- 1) shall include a "domain" attribute;
- 2) may include a <common> element;
- 3) may include an <on-network> element;
- 4) may include an <off-network> element; and
- 5) may include any other attribute for the purposes of extensibility.

The <common> element:

- 1) may include an <alias> element;
- 2) may contain a <broadcast-group> element containing:
 - a) a <num-levels-group-hierarchy> element; and
 - b) a <num-levels-user-hierarchy> element;

The <on-network> element:

- 1) may contain a <emergency-call> element containing:
 - a) a <private-cancel-timeout> element; and
 - b) a <group-time-limit> element.
- 2) may contain a <private-call> element containing:
 - a) a <hang-time> element;
 - b) a <max-duration- with-floor-control > element; and
 - c) a <max-duration-without-floor-control> element;
- 3) may contain a <num-levels-hierarchy> element;
- 4) may contain a <transmit-time> element containing:
 - a) a <time-limit> element; and
 - b) a <time-warning> element;
- 5) may contain a <hang-time-warning> element;
- 6) may contain a <floor-control-queue> element containing:
 - a) a <depth> element; and
 - b) a <max-user-request-time> element; and
- 7) shall contain a <fc-timers-counters> element containing:
 - a) a <T1-end-of-rtp-media> element;

- b) a <T3-stop-talking-grace> element;
 - c) a <T7-floor-idle> element;
 - d) a <T8-floor-revoke> element;
 - e) a <T11-end-of-RTP-dual> element;
 - f) a <T12-stop-talking-dual> element;
 - g) a <T15-conversation> element;
 - h) a <T16-map-group-to-bearer> element;
 - i) a <T17-unmap-group-to-bearer> element;
 - j) a <T20-floor-granted> element;
 - k) a <T55-connect> element;
 - l) a <T56-disconnect> element;
 - m) a <C7-floor-idle> element;
 - n) a <C17-unmap-group-to-bearer> element;
 - o) a <C20-floor-granted> element;
 - p) a <C55-connect> element; and
 - q) a <C56-disconnect> element; and
- 8) shall contain a <signalling-protection> element containing:
- a) a <confidentiality-protection> element; and
 - b) an <integrity-protection> element.

The <off-network> element:

- 1) may contain a <emergency-call> element containing:
 - a) a <private-cancel-timeout> element; and
 - b) a <group-time-limit> element.
- 2) may contain a <private-call> element containing:
 - a) a <hang-time> element; and
 - b) a <max-duration-with-floor-control> element;
- 3) may contain a <num-levels-hierarchy> element;
- 4) may contain a <transmit-time> element containing:
 - a) a <time-limit> element; and
 - b) a <time-warning> element.
- 5) may contain a <hang-time-warning> element;
- 6) may contain a <default-prose-per-packet-priority> element; and
- 7) may contain a <allow-log-metadata> element.

7.5.2.2 Application Unique ID

The AUID shall be set to "org.3gpp.mcptt.service-config".

7.5.2.3 XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:3gpp:ns:mcpttServiceConfig:1.0"
xmlns:mcpttsc="urn:3gpp:ns:mcpttServiceConfig:1.0">

<!-- the root element -->
  <xs:element name="service-configuration-info" type="mcpttsc:service-configuration-info-Type"/>

<!-- the root type -->
<!-- this is refined with one or more sub-types -->
  <xs:complexType name="service-configuration-info-Type">
    <xs:sequence>
      <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

<!-- definition of an element of one of the subtypes -->
  <xs:element name="service-configuration-params" type="mcpttsc:service-configuration-params-Type"/>

<!-- definition of the service-configuration-params-Type subtype-->
  <xs:complexType name="service-configuration-params-Type">
    <xs:sequence>
      <xs:element name="common" type="mcpttsc:commonType" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="on-network" type="mcpttsc:on-networkType" minOccurs="0"
maxOccurs="unbounded"/>
      <xs:element name="off-network" type="mcpttsc:off-networkType" minOccurs="0"
maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="domain" type="xs:anyURI" use="required"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="commonType">
    <xs:sequence>
      <xs:element name="alias" type="xs:string" minOccurs="0"/>
      <xs:element name="broadcast-group" type="mcpttsc:broadcast-groupType" minOccurs="0"/>
      <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="on-networkType">
    <xs:sequence>
      <xs:element name="emergency-call" type="mcpttsc:emergency-callType" minOccurs="0"/>
      <xs:element name="private-call" type="mcpttsc:private-callType" minOccurs="0"/>
      <xs:element name="num-levels-priority-hierarchy" type="xs:unsignedShort" minOccurs="0"/>
      <xs:element name="transmit-time" type="mcpttsc:transmit-timeType" minOccurs="0"/>
      <xs:element name="hang-time-warning" type="xs:duration" minOccurs="0"/>
      <xs:element name="floor-control-queue" type="mcpttsc:floor-control-queueType" minOccurs="0"/>
      <xs:element name="fc-timers-counters" type="mcpttsc:fc-timers-countersType" minOccurs="1"
maxOccurs="1"/>
      <xs:element name="signalling-protection" type="mcpttsc:signalling-protectionType"
minOccurs="0"/>
      <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="off-networkType">
    <xs:sequence>
      <xs:element name="emergency-call" type="mcpttsc:emergency-callType" minOccurs="0"/>
      <xs:element name="private-call" type="mcpttsc:private-callType" minOccurs="0"/>
      <xs:element name="num-levels-priority-hierarchy" type="xs:unsignedShort" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```

    <xs:element name="transmit-time" type="mcpttsc:transmit-timeType" minOccurs="0"/>
    <xs:element name="hang-time-warning" type="xs:duration" minOccurs="0"/>
    <xs:element name="default-prose-per-packet-priority" type="mcpttsc:default-prose-per-packet-
priorityType" minOccurs="0"/>
    <xs:element name="allow-log-metadata" type="xs:boolean" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="private-callType">
  <xs:sequence>
    <xs:element name="hang-time" type="xs:duration" minOccurs="0"/>
    <xs:element name="max-duration-with-floor-control" type="xs:duration" minOccurs="0"/>
    <xs:element name="max-duration-without-floor-control" type="xs:duration" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="broadcast-groupType">
  <xs:sequence>
    <xs:element name="num-levels-group-hierarchy" type="xs:unsignedShort" minOccurs="0"/>
    <xs:element name="num-levels-user-hierarchy" type="xs:unsignedShort" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="fc-timers-countersType">
  <xs:sequence>
    <xs:element name="T1-end-of-rtp-media" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T3-stop-talking-grace" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T7-floor-idle" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T8-floor-revoke" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T11-end-of-RTP-dual" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T12-stop-talking-dual" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T15-conversation" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T16-map-group-to-bearer" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T17-unmap-group-to-bearer" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T20-floor-granted" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T55-connect" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="T56-disconnect" type="xs:duration" minOccurs="1" maxOccurs="1"/>
    <xs:element name="C7-floor-idle" type="xs:unsignedShort" minOccurs="1" maxOccurs="1"/>
    <xs:element name="C17-unmap-group-to-bearer" type="xs:unsignedShort" minOccurs="1"
maxOccurs="1"/>
    <xs:element name="C20-floor-granted" type="xs:unsignedShort" minOccurs="1" maxOccurs="1"/>
    <xs:element name="C55-connect" type="xs:unsignedShort" minOccurs="1" maxOccurs="1"/>
    <xs:element name="C56-disconnect" type="xs:unsignedShort" minOccurs="1" maxOccurs="1"/>
    <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="emergency-callType">
  <xs:sequence>
    <xs:element name="private-cancel-timeout" type="xs:duration" minOccurs="0"/>
    <xs:element name="group-time-limit" type="xs:duration" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="transmit-timeType">
  <xs:sequence>
    <xs:element name="time-limit" type="xs:duration" minOccurs="0"/>
    <xs:element name="time-warning" type="xs:duration" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="floor-control-queueType">

```

```

<xs:sequence>
  <xs:element name="depth" type="xs:unsignedShort" minOccurs="0"/>
  <xs:element name="max-user-request-time" type="xs:duration" minOccurs="0"/>
  <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
  <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
<xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="default-prose-per-packet-priorityType">
  <xs:sequence>
    <xs:element name="mcptt-private-call-signalling" type="xs:unsignedShort" minOccurs="0"/>
    <xs:element name="mcptt-private-call-media" type="xs:unsignedShort" minOccurs="0"/>
    <xs:element name="mcptt-emergency-private-call-signalling" type="xs:unsignedShort"
minOccurs="0"/>
    <xs:element name="mcptt-emergency-private-call-media" type="xs:unsignedShort" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="signalling-protectionType">
  <xs:sequence>
    <xs:element name="confidentiality-protection" type="xs:boolean" minOccurs="0" default="true"/>
    <xs:element name="integrity-protection" type="xs:boolean" minOccurs="0" default="true"/>
    <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="anyExtType">
  <xs:sequence>
    <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

7.5.2.4 Default Namespace

The default namespace used in expanding URIs shall be "urn:3gpp:ns:mcpttServiceConfig:1.0" defined in subclause 7.5.2.3.

7.5.2.5 MIME type

The MIME type for the service configuration document shall be "vnd.3gpp.mcptt-service-config+xml".

7.5.2.6 Validation Constraints

If the AUID value of the document URI or node URI in the Request-URI is other than that specified in subclause 7.5.2.2, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid application id used".

If the XUI value of the document URI or node URI in the Request-URI does not match the XUI of the service configuration document URI, the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid XUI".

The service configuration document shall conform to the XML Schema described in subclause 7.5.2.3.

The <service-configuration-info> element is the root element of the XML document. The <service-configuration-info> element can contain sub-elements.

NOTE 1: The sub-elements of the <service-configuration-info> are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <mcptt-info> element.

The <service-configuration-params> element is a subelement of the <service-configuration-info> element.

If the <service-configuration-info> element does not contain a <service-configuration-params> element, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "mandatory element is missing".

If the <service-configuration-params> element does not include a <common> element, an <on-network> element or an <off-network> element, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "mandatory element is missing".

The <service-configuration-params> element shall contain either:

- 1) one <common> element only;
- 2) one <common> element and one <on-network> element;
- 3) one <common> element and one <off-network> element;
- 4) one <on-network> element only;
- 5) one <off-network> element only;
- 6) one <on-network> element and one <off-network> element; or
- 7) one <common> element, one <on-network> element and one <off-network> element.

If the <service-configuration-params> element does not confirm to one of the seven choices above, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the "domain" attribute does not contain a syntactically correct domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "syntactically incorrect domain name".

If the "domain" attribute contains an unknown domain name, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "unknown domain name".

The value of the <num-levels-group-hierarchy> element in the <broadcast-group> element refers to variable B1 defined in Annex A of 3GPP TS 22.179 [3].

The value of the <num-levels-user-hierarchy> element in the <broadcast-group> element refers to variable B2 defined in Annex A of 3GPP TS 22.179 [3].

The value of the <num-levels-group-hierarchy> element, the <num-levels-user-hierarchy> element or the <depth> element do not contain a semantically valid value, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "semantic error".

If the <num-levels-priority-hierarchy> element of the <off-network> element contains a value less than 1 and greater than 4, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

If the <num-levels-priority-hierarchy> element of the <on-network> element contains a value less than 1 and greater than 4, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

NOTE 2: The higher the <priority-hierarchy> value, the higher the priority given to override an active transmission.

If the <off-network> element contains a <private-call> element with a <max-duration-without-floor-control> element, it shall be ignored.

If any of the constituent elements of the <default-prose-per-packet-priority> element contain a value less than 1 and greater than 8, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "element value out of range".

NOTE 3: The higher the <default-prose-per-packet-priority> value, the higher the priority given to the signalling or media.

The following elements conform to the "xs: duration" XML type:

- 1) <hang-time>;
- 2) <hang-time-warning>;
- 3) <max-duration-with-floor-control>;
- 4) <max-duration-without-floor-control>;
- 5) <private-cancel-timeout>;
- 6) <group-time-limit>;
- 7) <max-user-request-time>;
- 8) <time-limit>;
- 9) <time-warning>;
- 10) <T1-end-of-rtp-media>;
- 11) <T3-stop-talking-grace>;
- 12) <T7-floor-idle>;
- 13) <T8-floor-revoke>;
- 14) <T11-end-of-RTP-dual>;
- 15) <T12-stop-talking-dual>;
- 16) <T15-conversation>;
- 17) <T16-map-group-to-bearer>;
- 18) <T17-unmap-group-to-bearer>;
- 19) <T20-floor-granted>;
- 20) <T55-connect>; and
- 21) <T56-disconnect>.

The elements of "xs: duration" type specified above shall be represented in seconds using the element value: "PT<h>H<m>M<n>S" where <n> represents a valid value in seconds.

NOTE 4: "xs:duration" allows the use of decimal notion for seconds, e.g. 300ms is represented as <PT0.3S>.

If any of the elements of "xs: duration" type specified above contain values that do not conform to the "PT <n>S" structure then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid format for duration".

If an invalid value is received for <n>, then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid value for duration".

The default value for the <confidentiality-protection> element of the <signalling-protection> element is "true" indicating that confidentiality protection is enabled.

The default value for the <integrity-protection> element of the <signalling-protection> element is "true" indicating that integrity protection is enabled.

The service configuration server ignores any unknown element and any unknown attribute.

If the configuration management server receives a duplicate element or attribute, it shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "duplicate attribute or element received".

7.5.2.7 Data Semantics

The "domain" attribute of the <service-configuration-params> element contains the domain name of the mission critical organization.

The <common> element contains service configuration data common to both on and off network service.

The <on-network> element contains service configuration data for on-network service only.

The <off-network> element contains service configuration data for off-network service only.

In the <common> element:

- 1) the <alias> element contains an alphanumeric name assigned by the MCPTT administrator of minimum length (N3);
- 2) the <num-levels- group-hierarchy> element of the <broadcast-group> element contains an integer indicating the number levels of group hierarchy for group-broadcast groups; and
- 3) the <num-levels-user-hierarchy> element of the <broadcast-group> element contains an integer indicating the number levels of user hierarchy for user-broadcast groups;

In the <on-network> element:

- 1) the <private-cancel-timeout> element of the <emergency-call> element contains the timeout value for the cancellation of an in-progress on-network emergency private call;
- 2) the <group-time-limit> element of the <emergency-call> element contains the time limit for an in-progress on-network emergency call on an MCPTT group;
- 3) the <hang-time> element of the <private-call> element contains the value of the hang timer for on-network private calls;

NOTE: The hang time is a configurable maximum length of the inactivity (silence) period between consecutive MCPTT transmissions within the same call.

- 4) the <max-duration-with-floor-control> element of the <private-call> element contains the maximum duration allowed for an on-network private call with floor control;
- 5) the <max-duration-without-floor-control > element of the <private-call> element contains the maximum duration allowed for an on-network private call without floor control;
- 6) the <num-levels-priority-hierarchy> element contains a priority hierarchy for determining what participants, participant types, and urgent transmission types shall be granted a request to override an active on-network MCPTT transmission;
- 7) the <time-limit> element of the <transmit-time> element contains the transmit time limit in an on-network group or private call transmission;
- 8) the <time-warning> element of the <transmit-time> element contains the warning time before the on-network transmit time is reached;
- 9) the <hang-time-warning> element contains the warning time before the on-network hang time is reached;
- 10) the <depth> element of the <floor-control-queue> element contains the maximum size of the floor control queue; and
- 11) the <max-user-request-time> element of the <floor-control-queue> element contains the maximum time for a user's floor control request to be queued;
- 12) the <T1-end-of-rtp-media> element of the <fc-timers-counters> element contains the maximum allowed time between RTP media packets;

- 13) the <T3-stop-talking-grace> element of the <fc-timers-counters> element contains the maximum time the floor control server shall forward RTP media packets after that the permission to send RTP media is revoked;
- 14) the <T7-floor-idle> element of the <fc-timers-counters> element contains the retransmission interval of the Floor Idle message when the floor is idle. The maximum number of times the Floor Idle is retransmitted is controlled by the counter in the <C7-floor-idle> element;
- 15) the <T8-floor-revoke> element of the <fc-timers-counters> element contains the retransmission interval time of the Floor Revoke message until the Floor Release message is received;
- 16) the <T11-end-of-RTP-dual> element of the <fc-timers-counters> element contains the maximum allowed time between RTP media packets for the interrupting participant during dual floor operations;
- 17) the <T12-stop-talking-dual> element of the <fc-timers-counters> element contains the transmit time limit in an on-network group for the interrupting participant during dual floor operations;
- 18) the <T15-conversation> element the maximum contains the maximum allowed time of silence in a group session involving an MBMS bearer before the MBMS subchannel shall be released;
- 19) the <T16-map-group-to-bearer> element contains the retransmission interval of the Map Group To Bearer message;
- 20) the <T17-unmap-group-to-bearer> element contains the retransmission interval of the Unmap Group To Bearer message;
- 21) the <T20-floor-granted> element of the <fc-timers-counters> element contains the time the floor control server shall wait before retransmitting the Floor Granted message until the Floor Request message is received. The number of times the Floor Granted message shall be sent is controlled by the counter in <C20-floor-granted> element;
- 22) the <T55-connect> element contains the retransmission interval of the Connect message. The number of times the Connect message is retransmitted is controlled by the counter in <C56-disconnect> element;
- 23) the <T56-disconnect> element contains the retransmission interval of the Disconnect message. The number of times the Disconnect message is retransmitted is controlled by the counter in <C55-connect> element;
- 24) the <C7-floor-idle> element of the <fc-timers-counters> element contains the maximum number of times the Floor Idle shall be sent;
- 25) the <C17-unmap-group-to-bearer> element contains the retransmission interval of the Unmap Group To Bearer message;
- 26) the <C20-floor-granted> element of the <fc-timers-counters> element contains the maximum times the Floor Granted message shall be retransmitted.
- 27) the <C55-connect> element contains the maximum number of times the Connect message is retransmitted;
- 28) the <C56-disconnect> element contains the maximum number of times the Disconnect message is retransmitted;
- 29) the <confidentiality-protection> element of the <signalling-protection> element contains a boolean indicating whether confidentiality protection of MCPTT signalling is enabled or disabled; and
- 30) the <integrity-protection> element of the <signalling-protection> element contains a boolean indicating whether integrity protection of MCPTT signalling is enabled or disabled;

In the <off-network> element:

- 1) the <private-cancel-timeout> element of the <emergency-call> element contains the timeout value for the cancellation of an in-progress off-network emergency private call;
- 2) the <group-time-limit> element of the <emergency-call> element contains the time limit for an in-progress off-network emergency call on an MCPTT group;
- 3) the <hang-time> element of the <private-call> element contains the value of the hang timer for off-network private calls;

- 4) the <max-duration-with-floor-control> element of the <private-call> element contains the maximum duration allowed for an off-network private call with floor control;
- 5) the <num-levels-priority-hierarchy> element contains a priority hierarchy for determining what participants, participant types, and urgent transmission types shall be granted a request to override an active off-network MCPTT transmission;
- 6) the <time-limit> element of the <transmit-time> element contains the transmit time limit in an off-network group or private call transmission;
- 7) the <time-warning> element of the <transmit-time> element contains the warning time before the off-network transmit time is reached;
- 8) the <hang-time-warning> element contains the warning time before the off-network hang time is reached;
- 9) the <default-prose-per-packet-priority> element contains priority values for off-network calls, for each of the following constituent elements:
 - a) mcptt private call signalling;
 - b) mcptt private call media;
 - c) mcptt emergency private call signalling; and
 - d) mcptt emergency private call media; and
- 10) the <allow-log-metadata> element contains one of the following values:
 - a) "true" which indicates that logging of metadata for MCPTT group calls, MCPTT private calls and non-call activities from MCPTT UEs operating in off-network mode, is enabled; and
 - b) "false" which indicates that logging of metadata for MCPTT group calls, MCPTT private calls and non-call activities from MCPTT UEs operating in off-network mode, is not enabled.

7.5.2.8 Naming Conventions

The present document defines no naming conventions.

7.5.2.9 Global documents

The present document requires no global documents.

7.5.2.10 Resource interdependencies

There are no resource interdependencies.

7.5.2.11 Authorization Policies

The authorization policies for manipulating a service configuration document shall conform to those described in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 5.1.5 "*Authorization*".

7.5.2.12 Subscription to Changes

The service configuration document application usage shall support subscription to changes as specified in OMA OMA-TS-XDM_Core-V2_1-20120403-A [2] subclause 6.2.2 "*Subscriptions to changes in the XDM Resources*".

Annex A (informative): Signalling flows

Editor's note [WID: MCPTT]: The included signalling flows will be limited to illustrate key functionalities and will not cover all possible scenarios.

Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2015-12					Initial proposal to CT1	-	0.0.0
2016-01					Agreed contributions C1-160308, C1-160309, C1-160311 from CT1#95-bis.	0.0.0	0.1.0
2016-02					Agreed contributions C1ah-160054, C1ah-160060, C1ah-160089, C1ah-160090, C1ah-160091, C1ah-160092, C1ah-160106 from CT1 Ad-Hoc on MCPTT.	0.1.0	0.2.0
2016-02					Agreed contributions C1-161130, C1-161225, C1-161226, C1-161227, C1-161355, C1-161500, C1-161511, C1-161513, C1-161531 from CT1#96.	0.2.0	0.3.0
2016-03	CT-71	CP-160057			Version 1.0.0 created for presentation for information and approval	0.3.0	1.0.0
2016-03	CT-71				Version 13.0.0 created after approval	1.0.0	13.0.0
2016-03	CT-71				Rapporteur post CT clean up	13.0.0	13.0.1
2016-04					Rapporteur intermediate version implementing CRs from CT1#97 for checking and aid for checking conflicts when developing CRs for CT1#98. NOT TO BE USED AS A BASELINE FOR GENERATING CRs	13.0.1	13.0.1 BIS
2016-06	CT-72	CP-160322	0001	3	Adding floor control configuration to the Service Configuration document.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0003	4	Service Configuration XML schema update	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0004	1	Align terminology with drafting rules	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0005	5	UE Initial Configuration document definition	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0006	3	UE Configuration document definition	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0007		Clean up reference to OMA document in 6.3.1.2	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0011	1	Update user configuration document with private call security authorisation	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0012	1	Adding security parameters to the Service Configuration document.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0014		Modify validation rules for service configuration document	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0018		Using the AUID and default namespace	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0019	1	Removal of <Resource-Priority> Element from MCPTT UE initial configuration document	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0021	2	Configuration management using OMA DM	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0022	2	Aligning User Profile terminology with TS 23.179	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0024	1	Semantics for <Resource-Priority > Element	13.0.1	13.1.0

History

Document history		
V13.0.1	May 2016	Publication
V13.1.0	July 2016	Publication