

ETSI TS 124 484 V14.1.0 (2017-04)



**LTE;
Mission Critical Services (MCS) configuration management;
Protocol specification
(3GPP TS 24.484 version 14.1.0 Release 14)**



Reference

RTS/TSGC-0124484ve10

Keywords

LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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 2017.
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.....	7
1 Scope	8
2 References	8
3 Definitions and abbreviations.....	10
3.1 Definitions	10
3.2 Abbreviations	10
4 General	11
4.1 MCS service administrator configuration.....	11
4.1.1 Common configuration	11
4.1.2 MCPTT configuration.....	11
4.1.3 MCVideo configuration	12
4.1.4 MCDData configuration	12
4.2 MC UE configuration	12
4.2.1 General.....	12
4.2.2 Online configuration	13
4.2.2.1 General	13
4.2.2.2 MCPTT	14
4.2.2.3 MCVideo configuration	14
4.2.2.4 MCDData configuration	14
4.2.3 Offline configuration	14
4.2.3.1 General	14
4.2.3.2 MCPTT	14
4.2.3.3 MCVideo configuration	14
4.2.3.4 MCDData configuration	15
4.3 MCS server.....	15
4.3.1 General.....	15
4.3.2 MCPTT Server.....	15
4.3.3 MCVideo Server.....	15
4.3.4 MCDData Server	15
4.4 Configuration management server.....	15
5 Functional entities	16
5.1 Configuration management client (CMC).....	16
5.2 Configuration management server (CMS)	16
5.3 MCS server.....	17
6 Procedures	17
6.1 Introduction	17
6.2 Common procedures.....	18
6.2.1 General.....	18
6.2.2 Client procedures	18
6.2.3 MCS server procedures.....	18
6.2.4 Configuration management server procedures.....	18
6.3 Configuration management procedures.....	18
6.3.1 General.....	18
6.3.1.1 Client procedures	18
6.3.1.2 Configuration management server procedures.....	18
6.3.2 Configuration management document creation procedure	19
6.3.2.1 General	19
6.3.2.2 Configuration management client (CMC) procedures	19
6.3.2.3 Configuration management server (CMS) procedures.....	19

6.3.3	Configuration management document retrieval procedure	19
6.3.3.1	General	19
6.3.3.2	Client procedures	19
6.3.3.2.1	General client (GC) procedures	19
6.3.3.2.2	Configuration management client (CMC) procedures	19
6.3.3.2.3	MCS server procedures	19
6.3.3.3	Configuration management server procedures	19
6.3.4	Configuration management document update procedure	20
6.3.4.1	General	20
6.3.4.2	Configuration management client procedures	20
6.3.4.3	Configuration management server procedures	20
6.3.5	Configuration management document deletion procedure	20
6.3.5.1	General	20
6.3.5.2	Configuration management Client (CMC) procedures	20
6.3.5.3	Configuration management server (CMS) procedures	20
6.3.6	Configuration management document element creation or replacement procedure	20
6.3.6.1	General	20
6.3.6.2	Client procedures	20
6.3.6.2.1	General client procedures	20
6.3.6.2.2	Configuration management client procedures	21
6.3.6.3	Configuration management server procedures	21
6.3.7	Configuration management document element deletion procedure	21
6.3.7.1	General	21
6.3.7.2	Client procedures	21
6.3.7.2.1	General client procedures	21
6.3.7.2.2	Configuration management client procedures	21
6.3.7.3	Configuration management server procedures	21
6.3.8	Configuration management document element fetching procedure	21
6.3.8.1	General	21
6.3.8.2	Client procedures	21
6.3.8.2.1	General client procedures	21
6.3.8.2.2	Configuration management client procedures	22
6.3.8.2.3	MCS server procedures	22
6.3.8.3	Configuration management server procedures	22
6.3.9	Configuration management document attribute creation or replacement procedure	22
6.3.9.1	General	22
6.3.9.2	Client procedures	22
6.3.9.2.1	General client procedures	22
6.3.9.2.2	Configuration management client procedures	22
6.3.9.3	Configuration management server procedures	22
6.3.10	Configuration management document attribute deletion procedure	22
6.3.10.1	General	22
6.3.10.2	Client procedures	23
6.3.10.2.1	General client procedures	23
6.3.10.2.2	Configuration management client procedures	23
6.3.10.3	Configuration management server procedures	23
6.3.11	Configuration management document attribute fetching procedure	23
6.3.11.1	General	23
6.3.11.2	Client procedures	23
6.3.11.2.1	General client procedures	23
6.3.11.2.2	Configuration management client procedures	23
6.3.11.2.3	MCPTT server procedures	23
6.3.11.3	Configuration management server procedures	23
6.3.12	Configuration management document namespace binding fetching procedure	24
6.3.12.1	General	24
6.3.12.2	Client procedures	24
6.3.12.2.1	General client procedures	24
6.3.12.2.2	Configuration management client procedures	24
6.3.12.2.3	MCS server procedures	24
6.3.12.3	Configuration management server procedures	24
6.3.13	Configuration management subscription and notification procedure	24
6.3.13.1	General	24

6.3.13.2	Client procedures	24
6.3.13.2.1	General client (GC) procedures	24
6.3.13.2.2	Configuration management client procedures	24
6.3.13.2.3	MCS server procedures	26
6.3.13.3	Configuration management server procedures	26
6.3.13.3.1	General	26
6.3.13.3.2	Procedures for CMS performing the subscription function	27
6.3.13.3.2.1	General	27
6.3.13.3.2.2	CMC originated subscription proxy procedure	27
6.3.13.3.2.3	CMC originated subscription procedure	28
6.3.13.3.2.4	MCS server originated subscription procedure	28
7	Common configuration management documents	29
7.1	Introduction	29
7.2	MCS UE initial configuration document	29
7.2.1	General	29
7.2.2	Coding	29
7.2.2.1	Structure	29
7.2.2.2	Application Unique ID	32
7.2.2.3	XML Schema	32
7.2.2.4	Default Document Namespace	35
7.2.2.5	MIME type	35
7.2.2.6	Validation Constraints	35
7.2.2.7	Data Semantics	39
7.2.2.8	Naming Conventions	42
7.2.2.9	Global documents	42
7.2.2.10	Resource interdependencies	42
7.2.2.11	Authorization Policies	43
7.2.2.12	Subscription to Changes	43
8	MCPTT configuration management documents	43
8.1	Introduction	43
8.2	MCPTT UE configuration document	43
8.2.1	General	43
8.2.2	Coding	44
8.2.2.1	Structure	44
8.2.2.2	Application Unique ID	45
8.2.2.3	XML Schema	45
8.2.2.4	Default Document Namespace	47
8.2.2.5	MIME type	47
8.2.2.6	Validation Constraints	47
8.2.2.7	Data Semantics	49
8.2.2.8	Naming Conventions	50
8.2.2.9	Global documents	50
8.2.2.10	Resource interdependencies	50
8.2.2.11	Authorization Policies	50
8.2.2.12	Subscription to Changes	50
8.3	MCPTT user profile configuration document	51
8.3.1	General	51
8.3.2	Coding	51
8.3.2.1	Structure	51
8.3.2.2	Application Unique ID	54
8.3.2.3	XML Schema	54
8.3.2.4	Default Document Namespace	57
8.3.2.5	MIME type	57
8.3.2.6	Validation Constraints	58
8.3.2.7	Data Semantics	58
8.3.2.8	Naming Conventions	69
8.3.2.9	Global documents	69
8.3.2.10	Resource interdependencies	69
8.3.2.11	Access Permissions Policies	69
8.3.2.12	Subscription to Changes	69

8.4	MCPTT service configuration document	70
8.4.1	General.....	70
8.4.2	Coding	70
8.4.2.1	Structure.....	70
8.4.2.2	Application Unique ID.....	72
8.4.2.3	XML Schema	72
8.4.2.4	Default Document Namespace.....	75
8.4.2.5	MIME type.....	75
8.4.2.6	Validation Constraints.....	75
8.4.2.7	Data Semantics.....	78
8.4.2.8	Naming Conventions.....	81
8.4.2.9	Global documents	81
8.4.2.10	Resource interdependencies	81
8.4.2.11	Authorization Policies.....	81
8.4.2.12	Subscription to Changes.....	81
9	MCVideo configuration management documents.....	82
10	MCDATA configuration management documents.....	82
Annex A (informative): Signalling flows		83
Annex B (informative): IANA registration templates.....		84
B.1	IANA registration templates for MIME types.....	84
B.1.1	application/vnd.3gpp.mcptt-ue-init-config+xml IANA registration template	84
B.1.2	application/vnd.3gpp.mcptt-ue-config+xml IANA registration template.....	85
B.1.3	application/vnd.3gpp.mcptt-user-profile+xml IANA registration template	87
B.1.4	application/vnd.3gpp.mcptt-service-config+xml IANA registration template	88
Annex C (informative): Change history		91
History		93

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 service online configuration over the CSC-4 and CSC-5 reference points and the procedures to support Mission critical service offline configuration over the CSC-11 and CSC-12 reference points.

Mission critical services include:

- Mission Critical Push To Talk (MCPTT);
- Mission Critical Video (MCVideo); and
- Mission Critical Data (MCData).

Configuration management documents defined in the present document includes:

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

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

The Mission critical services 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 MC UE supporting the configuration management client functionality, to application servers supporting the configuration management server functionality, and to application servers supporting the:

- MCPTT server functionality;
- MCVideo server functionality; or
- MCData 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 24.483: "Mission Critical Services (MCS) Management Object (MO)".
- [5] 3GPP TS 24.481: "Mission Critical Services (MCS) group management Protocol specification".
- [6] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management Protocol specification".
- [7] 3GPP TS 29.283: "Diameter Data Management Applications".
- [8] 3GPP TS 23.379: "Functional architecture and information flows to support mission critical push to talk (MCPTT); Stage 2".
- [8A] 3GPP TS 23.280: " Common functional architecture to support mission critical 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".
- [18] 3GPP TS 23.303: "Proximity-based Services (ProSe); Stage 25".
- [19] 3GPP TS 4.334: "Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects; Stage 3".
- [20] draft-holmberg-dispatch-mcptt-rp-namespace-02 (January 2017) "Resource-Priority Namespace for Mission Critical Push To Talk service".

Editor's note [CT#73, CP-160472]: The above document cannot be formally referenced until it is published as an RFC.

- [21] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
- [22] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [23] IETF RFC 6050: "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

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].

MCS network: A network infrastructure that supports the MCS.

Offline Configuration: Configuration of the MC UE without connectivity with any MCS network. Configuration of the MC UE is achieved using some external device (e.g. a laptop) with some kind of IP connectivity with the MC UE (e.g. over USB, WLAN, Bluetooth, etc).

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

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

On-network operation: An MC UE operating with connectivity to an MCS 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

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

Pre-selected MCPTT user profile

3.2 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
MC	Mission Critical
MCPTT	Mission Critical Push To Talk
MCS	Mission Critical Service

MIME	Multi-Purpose Internet Mail Extensions
MO	Management Object
OMA	Open Mobile Alliance
ProSe	Proximity Services
RFC	Request For Comments
SIP	Session Initiation Protocol
SNR	Serial Number
TAC	Type Allocation Code
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 MCS service administrator configuration

4.1.1 Common configuration

An MCS service administrator can, using an MC UE configure the:

- MCS UE initial configuration document;

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

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

NOTE: If the MCS administrator includes a <Default-user-profile> element in the MCS UE initial configuration document as defined in subclause 7.2.2.1, at least one instance of an MCS user profile configuration document needs to first be created on the configuration management server, containing the "XUI-URI" attribute and "user-profile-index" attribute (as defined in subclause 8.3.2.1) that are included in the <Default-user-profile> element.

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

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

To create a new MC group document on the configuration management server, the MC UE uses the procedures in 3GPP TS 24.481 [5].

To update an existing MCPTT group document on the configuration management server, the MC UE uses the procedures in 3GPP TS 24.481 [5].

To delete an existing MC group document on the configuration management server, the MC UE uses the procedures in 3GPP TS 24.481 [5].

4.1.2 MCPTT configuration

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

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

The format of the MPCTT UE configuration document is defined in subclause 8.2.

The format of the MPCTT user profile configuration document is defined in subclause 8.3.

The format of the MPCTT service configuration document is defined in subclause 8.4.

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

4.1.3 MCVideo configuration

Editor's Note: [C1-170137, MCImp-MCVIDEO-CT] Text for MCVideo is FFS.

4.1.4 MCDATA configuration

Editor's Note: [C1-170137, MCImp-MCDATA-CT] Text for MCDATA is FFS.

4.2 MC UE configuration

4.2.1 General

Upon start up the MC UE bootstraps the required information (e.g. FQDN or IP address) to locate the configuration management server for configuration of the MCS UE initial configuration management object (MO) and the default MCPTT user profile configuration management object (MO).

In order to obtain access to MC services the MC 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 MC UE needs to discover either:

1. the online configuration management server in the network that configures the MCS UE initial configuration MO and the default MCS user profile configuration MO(s), then the MC UE:
 - a) using the URI of the configuration management server obtained from the MCS UE initial configuration MO, obtains for each MCS that is enabled:
 - the appropriateMCS UE configuration document;
 - the appropriateMCS user profile configuration document; and
 - the appropriateMCS service configuration document; and
 - b) using the URI of the group management server obtained from the MCS UE initial configuration MO obtain the MCS group document; or
2. the:
 - a) offline configuration management server on the external device that configures the MC UE with the:
 - MCS UE initial configuration MO;
 - appropriate MCS UE configuration MO(s);
 - appropriate MCS user profile MO(s); and
 - appropriate MCS service configuration MO(s); and
 - b) offline group management server on the external device that configures the MC UE with the MCS 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

4.2.2.1 General

The format of the MCS UE initial configuration MO downloaded to the MC UE during online configuration is defined in 3GPP TS 24.483 [4].

The format of the MCS group document downloaded to the MC UE during online configuration is defined in 3GPP TS 24.481 [5].

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

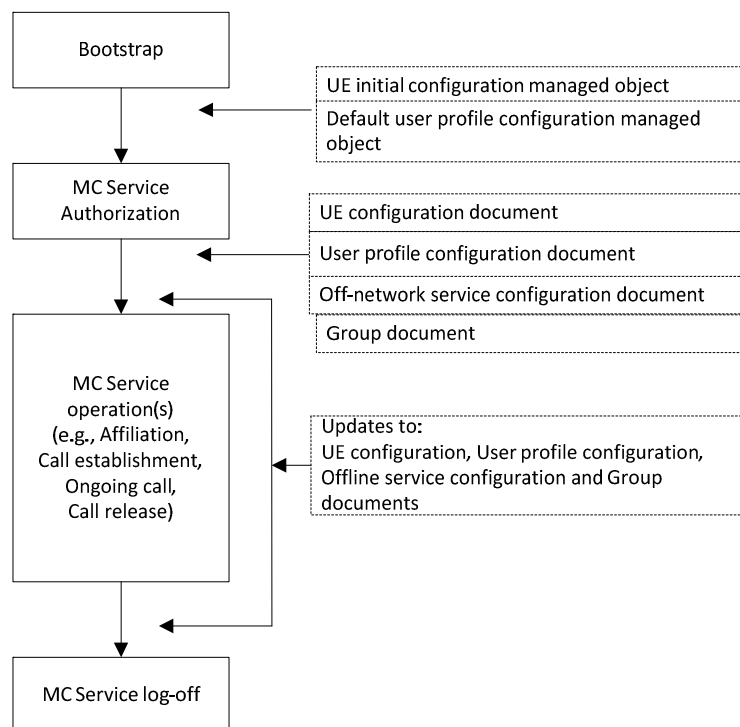


Figure 4.2.2-1 MC UE online configuration time sequence

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

If the MCS UE initial configuration MO contains a <default-user-profile> element and the identified default MCS user profile configuration MO(s) have changed from the version stored in the MC UE, the updated default MCS user profile configuration MO(s) are downloaded to the MC UE.

NOTE 1: The default MCS user profile configuration MO(s) define the default identity(s) for the enabled mission critical service(s) and the profile of services available to the user (e.g. emergency MCPTT services) prior to user authentication.

The MC UE contacts the identity management server using the HTTPS URI stored in the MCS UE initial configuration MO and performs MC User authentication as specified in 3GPP TS 24.482 [6].

The MC UE, using the identities obtained during MC user authentication, subscribes to the MCS UE configuration document, the MCS user profile configuration document and the MCS service configuration document for each enabled MCS using the procedure for subscribing to multiple documents simultaneously using the subscription proxy function specified in subclause 6.3.13.2.2 (i.e., the CMS acts as a Subscription Proxy) and subscribes to the MCS group document using the procedure specified in 3GPP TS 24.481 [5]. If these documents have been updated since the current version stored in the MC UE, then the MC 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 . Retrieval by the MC UE using the notified HTTPS URI of the MCS group document is performed as specified in 3GPP TS 24.481 [5].

NOTE 2: The MC UE can be notified of changes to an configuration documents at any time while using the MCS.

4.2.2.2 MCPTT

The format of the MPCTT UE configuration document downloaded to the MCPTT UE during online configuration is defined in subclause 8.2.

The format of the MPCTT user profile configuration document downloaded to the MCPTT UE during online configuration is defined in subclause 8.3.

The format of the MPCTT service configuration document downloaded to the MCPTT UE during online configuration is defined in subclause 8.4.

4.2.2.3 MCVideo configuration

Editor's Note: [C1-170137, MCImp-MCVIDEO-CT] Text for MCVideo is FFS.

4.2.2.4 MCDATA configuration

Editor's Note: [C1-170137, MCImp-MCDATA-CT] Text for MCDATA is FFS.

4.2.3 Offline configuration

4.2.3.1 General

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

The format of the MCS UE initial configuration MO downloaded to the MCPTT UE during offline configuration is defined in 3GPP TS 24.483 [4].

The format of the MCS group document MO to the MCPTT UE during offline configuration is defined in 3GPP TS 24.483 [4].

NOTE: If the MCPTT service administrator includes a "DefaultUserProfile" element in the MCS UE initial configuration MO as defined in 3GPP TS 24.483 [4], at least one instance of an MCS user profile configuration MO needs to first be created on the offline configuration management server, containing the "MCPTTUserID" element and "UserProfileIndex" element (as defined in 3GPP TS 24.483 [4]) that are included in the "DefaultUserProfile" element.

Editor's Note: [C1-170137, MCImp-eMCPTT-CT] Addressing the identities element is FFS.

4.2.3.2 MCPTT

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

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

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

4.2.3.3 MCVideo configuration

Editor's Note: [C1-170137, MCImp-MCVIDEO-CT] Text for MCVideo is FFS.

4.2.3.4 MCDATA configuration

Editor's Note: [C1-170137, MCImp-MCDATA-CT] Text for MCDATA is FFS.

4.3 MCS server

4.3.1 General

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

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

The MCS server subscribes to the MCS 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 MCS server is provisioned with the identities of the mission critical organisations is out of scope of the present document.

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

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

4.3.2 MCPTT Server

The format of the MCPTT service configuration document downloaded to the MCPTT server is defined in subclause 8.4.

4.3.3 MCVideo Server

Editor's Note: [C1-170137, MCImp-MCVIDEO-CT] Text for MCVideo is FFS.

4.3.4 MCDATA Server

Editor's Note: [C1-170137, MCImp-MCDATA-CT] Text for MCDATA is FFS.

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 MCS UE initial configuration document received from a MCS administrator into an appropriate format for configuration of the MCS UE initial configuration MO.

If the MCS UE initial configuration MO contains a <default-user-profile> element that identifies a MCS user profile configuration document, the configuration management server needs to convert the identified MCS user profile configuration document received from a MCS administrator into an appropriate format for configuration of the MCS user profile configuration MO.

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

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

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

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

To be compliant with the procedures in the present document the CMC shall:

- shall support the role of XCAP client as specified in IETF RFC 4825 [14];
- support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [2];
- support the procedures in subclause 6.3.1.1;
- support the procedures in subclause 6.3.2.2;
- support the procedures in subclause 6.3.3.2.2;
- support the procedures in subclause 6.3.8.2.2;
- support the procedures in subclause 6.3.11.2.2; and
- support the procedures in subclause 6.3.13.2.

The CMC may:

- support the procedures in subclause 6.2.2;
- support the procedures in subclause 6.3.4.2;
- support the procedures in subclause 6.3.5.2;
- support the procedures in subclause 6.3.6.2.2;
- support the procedures in subclause 6.3.7.2.2;
- support the procedures in subclause 6.3.9.2.2;
- support the procedures in subclause 6.3.10.2.2; and
- support the procedures in subclause 6.3.12.2.2.

5.2 Configuration management server (CMS)

To be compliant with the procedures in the present document the CMS shall:

- shall support the role of XCAP server as specified in IETF RFC 4825 [14];
- support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [2];
- support the procedures in subclause 6.2.4;
- support the procedures in subclause 6.3.1.2;
- support the procedures in subclause 6.3.2.3;

- support the procedures in subclause 6.3.3.3;
- support the procedures in subclause 6.3.4.3;
- support the procedures in subclause 6.3.5.3;
- support the procedures in subclause 6.3.6.3;
- support the procedures in subclause 6.3.7.3;
- support the procedures in subclause 6.3.8.3;
- support the procedures in subclause 6.3.9.3;
- support the procedures in subclause 6.3.10.3;
- support the procedures in subclause 6.3.11.3;
- support the procedures in subclause 6.3.12.3; and
- support the procedures in subclause 6.3.13.3.

5.3 MCS server

To be compliant with the procedures in the present document, the MCS server:

- shall support the role of XCAP client as specified in IETF RFC 4825 [14];
- shall support the role of XDMC as specified in OMA OMA-TS-XDM_Core-V2_1 [2];
- shall support the procedure in subclause 6.2.3;
- shall support the procedure in subclause 6.3.3.2.3;
- shall support the procedure in subclause 6.3.8.2.3;
- shall support the procedure in subclause 6.3.11.2.3;
- shall support the procedure in subclause 6.3.12.2.3; and
- shall support the procedure in subclause 6.3.13.2.3.

6 Procedures

6.1 Introduction

This clause specifies procedures enabling a configuration management client (CMC) and an MCS server to have the MCS 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 24.482 [6].

6.2.3 MCS server procedures

The MCS server shall send the HTTP request as specified for the HTTP client in the network entity in annex A of 3GPP TS 24.482 [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 24.482 [6].

The CMS shall be configured with an authorized MCS server list, containing public service identities of MCS servers of the MCS provider of the CMS.

When handling an HTTP request, the CMS shall determine the identity of the sender of the HTTP request as specified in 3GPP TS 24.482 [6], and shall use the identity of the sender of the HTTP request as an authenticated identity when performing the authorization.

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*" of OMA OMA-TS-XDM_Core-V2_1 [2] and subclause 6.3.13.2.2 for subscribing to configuration management documents.

6.3.1.2 Configuration management server procedures

A CMS shall support subclause 6.2.1 "*Document Management*", and subclause 6.2.4 "*Access Permissions*" of OMA OMA-TS-XDM_Core-V2_1 [2] and subclause 6.3.13.3 for accepting subscriptions to configuration management documents.

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 23.280 [8A].

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, and shall send the XML document to the network according to procedures specified in IETF RFC 4825 [14] "*Create or Replace a Document*". The CMC shall set the Request-URI of the HTTP PUT request to the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] and include the "auid" as per the appropriate application usage in clause 7.

6.3.2.3 Configuration management server (CMS) procedures

A CMS shall support receiving XML documents of the application usages according to procedures specified in IETF RFC 4825 [14] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an XML document and include the "auid" as per the appropriate application usage in clause 7.

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 IETF RFC 4825 [14] "*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. The CMC shall set the Request-URI of the HTTP GET request to the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] and include the "auid" as per the appropriate application usage in clause 7.

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 MCS server procedures

In order to retrieve a configuration management document via the CSC-5 reference point, an MCS Server shall perform the procedures in subclause 6.3.3.2.1 specified for GC. The MCS server shall set the Request-URI of the HTTP PUT request to identify the XML document based on configuration and include the "auid" as per the appropriate application usage.

6.3.3.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from a CMC and an MCS Server according to procedures specified in IETF RFC 4825 [14] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an XML document and include the "auid" as per with the "auid" parameter set to 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, and shall send the XML document to the network according to procedures specified in IETF RFC 4825 [14] "*Create or Replace a Document*". The CMC shall set the Request-URI of the HTTP PUT request to the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] and include the "auid" as per the appropriate application usage.

6.3.4.3 Configuration management server procedures

A CMS shall support receiving an XML document of the application usages according to the procedures specified in IETF RFC 4825 [14] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an XML document and include the "auid" as per to 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 of the HTTP DELETE request set to the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] along with the "auid" as per the appropriate application usage for the XML document to be deleted to the network according to procedures specified in IETF RFC 4825 [14] "*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 IETF RFC 4825 [14] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an XML document using the "auid" as per 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 IETF RFC 4825 [14] "*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. The CMC shall construct the Request-URI of the HTTP PUT request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path along with the "auid" as per the appropriate application usage.

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 IETF RFC 4825 [14] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an element of XML document using the "auid" as per 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 IETF RFC 4825 [14] "*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. The CMC shall construct the Request-URI of the HTTP DELETE request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path and include the "auid" as per the appropriate application usage.

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 IETF RFC 4825 [14] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an element of XML document along with the "auid" as per 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 IETF RFC 4825 [14] "*Fetch 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. The CMC shall construct the Request-URI of the HTTP GET request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path along with the "auid" as per the appropriate application usage.

6.3.8.2.3 MCS 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. The MCPTT server shall set the Request-URI of the HTTP PUT request to identify the XML document based on configuration with the "auid" as per the appropriate application usage.

6.3.8.3 Configuration management server procedures

A CMS shall support handling an HTTP GET request from CMC according to procedures specified in IETF RFC 4825 [14] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an element of XML document with the "auid" as per 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 IETF RFC 4825 [14] "*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. The CMC shall construct the Request-URI of the HTTP PUT request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path along with the "auid" per the appropriate application usage.

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 IETF RFC 4825 [14] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an attribute of XML document with the "auid" per the appropriate application usage in clause 7.

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 IETF RFC 4825 [14] "*Delete an Attribute*".

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. The CMC shall construct the Request-URI of the HTTP DELETE request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path along with the "auid" per the appropriate application usage.

6.3.10.3 Configuration management server procedures

A CMS shall support handling an HTTP DELETE request from CMC according to procedures specified in IETF RFC 4825 [14] "*DELETE Handling*" where the Request-URI of the HTTP DELETE request identifies an attribute of XML document along with the "auid" per the appropriate application usage in clause 7.

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 IETF RFC 4825 [14] "*Fetch 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. The CMC shall construct the Request-URI of the HTTP GET request using the "CMSXCAPRootURI" configured as per 3GPP TS 24.483 [4] as the root of the relative path along with the "auid" per the appropriate application usage .

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. The MCPTT sserver shall set the Request-URI of the HTTP GET request to identify the XML document based on configuration with the "auid" per the appropriate application usage.

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 IETF RFC 4825 [14] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an attribute of XML document with the "auid" per the appropriate application usage in clause 7.

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 IETF RFC 4825 [14] "*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. The CMC shall construct the Request-URI of the HTTP GET request to identify a namespace binding of the XML document along with the "auid" per the appropriate application usage .

6.3.12.2.3 MCS 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. The MCPTT server shall set the Request-URI of the HTTP GET request to identify a namespace binding of the XML document with the "auid" per the appropriate application usage.

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 IETF RFC 4825 [14] "*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

This procedure enables the CMC to subscribe to notification of changes of one or more configuration management documents defined.

This procedure enables the MCS server to subscribe to notification of changes of the MCPTT service configuration document.

6.3.13.2.2 Configuration management client procedures

In order to subscribe to Configuration management document, a CMC shall send an initial SIP SUBSCRIBE request to the network according to the UE originating procedures specified in 3GPP TS 24.229 [22] and IETF RFC 5875 [11]. In the initial SIP SUBSCRIBE request, the CMC:

- a) if direct subscription is used, shall set the Request URI to a SIP URI containing:

- 1) the base URI being equal to the "CMSXCAPRootURI" configured in the CMC as per 3GPP TS 24.483 [4];
and
 - 2) the "auid" parameter set to the appropriate application usage identifying a configuration management document;
- b) if subscription to multiple documents simultaneously using the subscription proxy function is used:
- 1) shall include an application/resource-lists+xml MIME body. In the application/resource-lists+xml MIME body, the CMC shall include one <entry> element for each document or element to be subscribed to, such that the "uri" attribute of the <entry> element contains a relative path reference:
 - A) with the base URI being equal to the "CMSXCAPRootURI" configured in the CMC as per 3GPP TS 24.483 [4]; and
 - B) with the "auid" parameter set to the appropriate application usage identifying a configuration management document;
 - 2) shall set the Request-URI to the configured public service identity for performing subscription proxy function of the CMS;
- c) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-access-token> element set to the value of the access token received during authentication procedure as described in 3GPP TS 24.482 [6];
- d) if identity hiding is required:
- 1) shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [9] for MCPTT client on the application/vnd.3gpp.mcptt-info+xml MIME body and on the application/resource-lists+xml MIME body; and
 - 2) shall include an application/mikey MIME body with the CSK as specified in 3GPP TS 24.379 [9];
- e) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [22]), in a P-Preferred-Service header field according to IETF RFC 6050 [23]; and
- f) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field.

Upon receiving a SIP NOTIFY request associated with a subscription created as result of the sent initial SIP SUBSCRIBE request:

- 1) if identity hiding is required, the CMC shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [9] for MC client; and
- 2) shall handle the SIP NOTIFY request according to IETF RFC 5875 [11].

In order to re-subscribe to notification of changes of a modified list of one or more configuration management documents; a CMC shall send a SIP re-SUBSCRIBE request to the network according to the UE originating procedures specified in 3GPP TS 24.229 [22] and IETF RFC 5875 [11]. In the SIP re-SUBSCRIBE request, the CMC:

- a) if direct subscription is used, shall set the Request URI to a SIP URI containing:
 - 1) the base URI being equal to the "CMSXCAPRootURI" configured in the CMC as per 3GPP TS 24.483 [4];
and
 - 2) the "auid" parameter set to the appropriate application usage identifying a configuration management document as described in clause 7;
- b) if subscription to multiple documents simultaneously using the subscription proxy function is used:
 - 1) shall include an application/resource-lists+xml MIME body. In the application/resource-lists+xml MIME body, the CMC shall include one <entry> element for each document or element to be subscribed to, such that the "uri" attribute of the <entry> element contains a relative path reference:
 - A) with the base URI being equal to the "CMSXCAPRootURI" configured in the CMC as per 3GPP TS 24.483 [4]; and

- B) with the "auid" parameter set to the appropriate application usage identifying a configuration management document as described in clause 7;
- c) if identity hiding is required, shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [9] for MC client on the application/vnd.3gpp.mcptt-info+xml MIME body and on the application/resource-lists+xml MIME body using the CSK included in the initial SIP SUBSCRIBE request; and
- d) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field.

6.3.13.2.3 MCS server procedures

In order to subscribe to an MCS service configuration document, an MCS server shall send an initial SIP SUBSCRIBE request to the network according to the originating AS procedures specified in 3GPP TS 24.229 [22] and IETF RFC 5875 [11]. In the initial SIP SUBSCRIBE request, MCPTT server:

- a) shall set the Request URI to a SIP URI containing:
 - 1) the base URI being equal to the XCAP root URI configured in the MCS server; and
 - 2) the "auid" parameter set to the application usage identifying the MCS service configuration document;
- b) shall include a P-Asserted-Identity header field containing the public service identity of the MCS server;
- c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [22]), in a P-Asserted-Service header field according to IETF RFC 6050 [23]; and
- d) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field.

Upon receiving a SIP NOTIFY request associated with a subscription created as result of the sent initial SIP SUBSCRIBE request, the MCS server shall handle the SIP NOTIFY request according to IETF RFC 5875 [11].

In order to re-subscribe to notification of changes to an MCS service configuration document, an MCS server shall send a SIP re-SUBSCRIBE request to the network according to the originating AS procedures specified in 3GPP TS 24.229 [22] and IETF RFC 5875 [11]. In the SIP re-SUBSCRIBE request, MCS server:

- a) shall set the Request URI to a SIP URI containing:
 - 1) the base URI being equal to the XCAP root URI configured in the MCS server; and
 - 2) the "auid" parameter set to the application usage identifying an MCS service configuration document; and
- b) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field.

6.3.13.3 Configuration management server procedures

6.3.13.3.1 General

The CMS procedures consist of:

- a) procedures for CMS performing the subscription proxy function; and
- b) procedures for CMS storing configuration management documents.

The CMS shall be configured with own public service identity for performing subscription proxy function of the CMS.

The CMS shall be configured with own public service identity for accessing documents.

6.3.13.3.2 Procedures for CMS performing the subscription function

6.3.13.3.2.1 General

The procedures for the CMS performing the subscription function.

6.3.13.3.2.2 CMC originated subscription proxy procedure

Upon reception of an initial SIP SUBSCRIBE request:

- a) with the Event header field set to xcap-diff;
- b) with the Request-URI set to own public service identity for performing subscription proxy function of the CMS;
- c) with a P-Asserted-Identity header field not containing an identity listed in the authorized MCS server list specified in subclause 6.2.4;
- d) with an application/vnd.3gpp.mcptt-info+xml MIME body containing the <mcptt-access-token> element;
- e) with an application/resource-lists+xml MIME body; and
- f) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24 229 [12]), in a P-Asserted-Service header field according to IETF RFC 6050 [23];

the CMS:

- a) if an <EncryptedData> XML tag is included in the application/vnd.3gpp.mcptt-info+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/vnd.3gpp.mcptt-info+xml MIME body;
- b) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body;
- c) shall identify the originating MCPTT ID from <mcptt-access-token> element received in the application/vnd.3gpp.mcpttinfo+xml MIME body and shall use the originating MCPTT ID as an authenticated identity when performing the authorization;
- d) if the authenticated identity is not authorized to subscribe to notification of changes of any resource in the application/resource-lists+xml MIME body, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps;
- e) act as a notifier according to IETF RFC 5875 [11]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the initial SIP SUBSCRIBE request contains an "auid" parameter set to an application usage identifying a configuration management document as described in clause 7;

shall return the XCAP URI identifying the configuration management document in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

Upon sending a SIP NOTIFY request associated with a subscription created as result of the received initial SIP SUBSCRIBE request, if the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, the CMS shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [9] for MCPTT server.

Upon reception of a SIP re-SUBSCRIBE request:

- a) with the Event header field set to xcap-diff; and
- b) with an application/resource-lists+xml MIME body;

the CMS:

- a) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body of the received SIP re-SUBSCRIBE request and the CSK was received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body; and
- b) act as a notifier according to IETF RFC 5875 [11]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the SIP re-SUBSCRIBE request contains an "auid" parameter set to an application usage identifying a configuration management document:

and for which there is no related subscription established according to the subclause 6.3.13.3.2.3, shall return the XCAP URI identifying the configuration management document in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

6.3.13.3.2.3 CMC originated subscription procedure

Upon reception of an initial SIP SUBSCRIBE request:

- a) with the Event header field set to xcap-diff;
- b) with the Request-URI having the base URI equal to the XCAP root URI of the CMS;
- c) with a P-Asserted-Identity header field containing an identity listed in the authorized MCS server list specified in subclause 6.2.4; and
- d) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24 229 [12]), in a P-Asserted-Service header field according to IETF RFC 6050 [23];

the CMS shall act as a notifier according to IETF RFC 5875 [11].

Upon reception of a SIP re-SUBSCRIBE request with the Event header field set to xcap-diff, the CMS:

- a) if the <mcptt-calling-user-id> element is included in the application/vnd.3gpp.mcptt-info+xml MIME body:
 - 1) shall use the <mcptt-calling-user-id> element value as an authenticated identity when performing the authorization; and
 - 2) if the authenticated identity is not authorized to subscribe to notification of changes of any document, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps;
- b) if the authenticated identity is not authorized to subscribe to notification of changes of any document, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps; and
- c) shall act as a notifier according to IETF RFC 5875 [11].

6.3.13.3.2.4 MCS server originated subscription procedure

Upon reception of an initial SIP SUBSCRIBE request:

- a) with the Event header field set to xcap-diff;
- b) with the Request-URI having the base URI equal to the XCAP root URI of the CMS;
- c) with a P-Asserted-Identity header field containing an identity listed in the authorized MCS server list specified in subclause 6.2.4; and
- d) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24 229 [12]), in a P-Asserted-Service header field according to IETF RFC 6050 [23];

the CMS shall act as a notifier according to IETF RFC 5875 [11].

Upon reception of a SIP re-SUBSCRIBE request:

- a) with the Event header field set to xcap-diff; and
- b) with an application/resource-lists+xml MIME body;

the CMS:

- a) shall use URI of the P-Asserted-Identity header field as an authenticated identity when performing the authorization;
- b) if the authenticated identity is not authorized to subscribe to notification of changes of any document or element in the application/resource-lists+xml MIME body, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps; and
- c) shall act as a notifier according to IETF RFC 5875 [11].

7 Common 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 MCS UE initial configuration document;

7.2 MCS UE initial configuration document

7.2.1 General

The MCS UE initial configuration document is specified in this subclause. The MCS UE initial configuration document content is based on requirements of Annex A.6 of 3GPP TS 23.280 [8A], and structure and procedures of OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCS UE initial configuration an MCS 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 MCS UE initial configuration document may apply to all MC UEs of a mission critical organization or apply to specific MC UEs identified by the optional <mcptt-UE-id> element. If there is no <mcptt-UE-id> element then by default the MC UE initial configuration document applies to all MC UEs of the mission critical organization. If the MC UE is to be configured with a specific MCS UE initial configuration document that document is identified by comparing the instance ID of the MC UE with the criteria in the <mcptt-UE-id> element.

The MCS UE initial configuration document acts as a template for the device management server coresident in the CMS to generate the MCS UE initial configuration managed object. The MCS UE initial configuration document that acts as a template is referred to as a "master MCS UE configuration document".

The master MCS UE initial configuration document name is assigned by an MCS administrator when the document is created and is stored in the user directory of that MCS administrator. The master MCS UE initial configuration document does not directly apply to a specific MC UE, but instead acts as template that the CMS uses to generate MCS UE initial configuration managed objects of MC UEs identified by elements of the <MCPTT-UE-id> element. For MCS UE initial configuration documents that correspond to a specific MC UE, the name of the MCS UE initial configuration document is created from a value defined by the corresponding element that identifies the MCS UE within the <MCPTT-UE-id> element. For a master MCS UE initial configuration documents that does not contain a <MCPTT-UE-id> element, the name of the MCS UE initial configuration document is "DEFAULT-MCPTT-UE.xml".

NOTE: For historical reasons some of the elements in the MCS UE initial configuration document uses the terminology "MCPTT", however this document is common to all MCS with some MCPTT specific elements. Not all elements that contain the terminology "MCPTT" are just MCPTT specific.

7.2.2 Coding

7.2.2.1 Structure

The MCS 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 <mcptt-UE-id> element;
- 3) may include a <name> element;
- 4) may include a <Default-user-profile> element;
- 5) may include an <on-network> element;
- 6) may include an <off-network> element; and
- 7) 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-auth-endpoint> element;
 - b) an <idms-token-endpoint> element;
 - c) a <gms> element;
 - d) a <cms> element; and
 - e) a <kms> element;
- 4) shall contain a <GMS-URI> element;
- 5) shall contain a <group-creation-XUI> element;
- 6) shall contain a <GMS-XCAP-root-URI> element; and
- 7) shall contain a <CMS-XCAP-root-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:

- 1) may contain a list of <Instance-ID-URN> elements; and
- 2) may contain a list of <IMEI-range> elements.

The <IMEI-range> element:

- 1) shall contain a <TAC> element;
- 2) may contain a list of <SNR> elements; and
- 3) may contain <SNR-range> element.

The <SNR-range> element:

- 1) shall contain a <Low-SNR> element; and
- 2) shall contain a <High-SNR> element.

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

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:mcpttiup="urn:3gpp:mcptt:mcpttUEinitConfig:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:mcptt:mcpttUEinitConfig: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="mcptt-UE-initial-configuration">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="mcptt-UE-id" type="mcpttiup:MCPTTUEIDType"/>
        <xs:element name="name" type="mcpttiup:NameType"/>
        <xs:element name="Default-user-profile" type="mcpttiup:UserProfileType"/>
        <xs:element name="on-network" type="mcpttiup:On-networkType"/>
        <xs:element name="off-network" type="mcpttiup:Off-networkType"/>
        <xs:element name="anyExt" type="mcpttiup:anyExtType"/>
        <xs:any namespace="##other" processContents="lax"/>
      </xs:choice>
      <xs:attribute name="domain" type="xs:anyURI" use="required"/>
      <xs:attribute name="XUI-URI" type="xs:anyURI"/>
      <xs:attribute name="Instance-ID-URN" type="xs:anyURI"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>

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

```

<xs:complexType name="MCPTTUEIDType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="Instance-ID-URN" type="xs:anyURI" />
    <xs:element name="IMEI-range" type="mcpttiup:IMEI-rangeType"/>
    <xs:element name="anyExt" type="mcpttiup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>

<xs:complexType name="IMEI-rangeType">
  <xs:sequence>
    <xs:element name="TAC" type="mcpttiup:tacType" />
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="SNR" type="mcpttiup:snrType" />
      <xs:element name="SNR-range" type="mcpttiup:SNR-rangeType" />
    </xs:choice>
    <xs:element name="anyExt" type="mcpttiup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>

<xs:complexType name="SNR-rangeType">
  <xs:sequence>
    <xs:element name="Low-SNR" type="mcpttiup:snrType" />
    <xs:element name="High-SNR" type="mcpttiup:snrType" />
    <xs:element name="anyExt" type="mcpttiup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>

<xs:simpleType name="tac-baseType">
  <xs:restriction base="xs:decimal">
    <xs:totalDigits value="8" />
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="tacType">
  <xs:simpleContent>
    <xs:extension base="tac-baseType">
      <xs:attributeGroup ref="IndexType" />
      <xs:anyAttribute namespace="##any" processContents="lax" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="snr-baseType">
  <xs:restriction base="xs:decimal">
    <xs:totalDigits value="6" />
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="snrType">
  <xs:simpleContent>
    <xs:extension base="snr-baseType">
      <xs:attributeGroup ref="IndexType" />
      <xs:anyAttribute namespace="##any" processContents="lax" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="UserProfileType">
  <xs:attribute name="User-ID" type="xs:anyURI" use="required" />
  <xs:attribute name="user-profile-index" type="xs:unsignedByte" use="required" />
  <xs:attributeGroup ref="IndexType" />
  <xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>

<xs:complexType name="VPLMType">
  <xs:sequence>
    <xs:element name="service" type="ServiceType" />
  </xs:sequence>

```

```

    <xs:attribute name="PLMN" type="xs:string" use="required"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="ServiceType">
    <xs:sequence>
      <xs:element name="MCPTT-to-con-ref" type="xs:string"/>
      <xs:element name="MC-common-core-to-con-ref" type="xs:string"/>
      <xs:element name="MC-ID-to-con-ref" type="xs:string"/>
      <xs:element name="anyExt" type="mcpttiup:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="On-networkType">
    <xs:sequence>
      <xs:element name="Timers">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="T100" type="xs:unsignedByte"/>
            <xs:element name="T101" type="xs:unsignedByte"/>
            <xs:element name="T103" type="xs:unsignedByte"/>
            <xs:element name="T104" type="xs:unsignedByte"/>
            <xs:element name="T132" type="xs:unsignedByte"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="HPLM">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="service" type="ServiceType"/>
            <xs:element name="VPLM" type="VPLMType" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="PLMN" type="xs:string" use="required"/>
        </xs:complexType>
      </xs:element>
      <xs:element name="App-Server-Info">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="idms-auth-endpoint" type="xs:anyURI"/>
            <xs:element name="idms-token-endpoint" type="xs:anyURI"/>
            <xs:element name="gms" type="xs:anyURI"/>
            <xs:element name="cms" type="xs:anyURI"/>
            <xs:element name="kms" type="xs:anyURI"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="GMS-URI" type="xs:anyURI"/>
      <xs:element name="group-creation-XUI" type="xs:anyURI"/>
      <xs:element name="GMS-XCAP-root-URI" type="xs:anyURI"/>
      <xs:element name="CMS-XCAP-root-URI" type="xs:anyURI"/>
      <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attributeGroup ref="IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="Off-networkType">
    <xs:sequence>
      <xs:element name="Timers">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="TFG1" type="xs:unsignedShort"/>
            <xs:element name="TFG2" type="xs:unsignedShort"/>
            <xs:element name="TFG3" type="xs:unsignedShort"/>
            <xs:element name="TFG4" type="xs:unsignedByte"/>
            <xs:element name="TFG5" type="xs:unsignedByte"/>
            <xs:element name="TFG11" type="xs:unsignedShort"/>
            <xs:element name="TFG12" type="xs:unsignedShort"/>
            <xs:element name="TFP1" type="xs:unsignedShort"/>
            <xs:element name="TFP2" type="xs:unsignedByte"/>
            <xs:element name="TFP3" type="xs:unsignedShort"/>
            <xs:element name="TFP4" type="xs:unsignedShort"/>
            <xs:element name="TFP5" type="xs:unsignedShort"/>
            <xs:element name="TFP6" type="xs:unsignedShort"/>
            <xs:element name="TFP7" type="xs:unsignedByte"/>
            <xs:element name="TFB1" type="xs:unsignedShort"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>

```

```

    <xs:element name="TFB2" type="xs:unsignedByte" />
    <xs:element name="TFB3" type="xs:unsignedByte" />
    <xs:element name="T201" type="xs:unsignedShort" />
    <xs:element name="T203" type="xs:unsignedByte" />
    <xs:element name="T204" type="xs:unsignedByte" />
    <xs:element name="T205" type="xs:unsignedByte" />
    <xs:element name="T230" type="xs:unsignedByte" />
    <xs:element name="T233" type="xs:unsignedByte" />
    <xs:element name="TFE1" type="xs:unsignedShort" />
    <xs:element name="TFE2" type="xs:unsignedByte" />
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Counters">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="CFP1" type="xs:unsignedByte" />
      <xs:element name="CFP3" type="xs:unsignedByte" />
      <xs:element name="CFP4" type="xs:unsignedByte" />
      <xs:element name="CFP6" type="xs:unsignedByte" />
      <xs:element name="CFG11" type="xs:unsignedByte" />
      <xs:element name="CFG12" type="xs:unsignedByte" />
      <xs:element name="C201" type="xs:unsignedByte" />
      <xs:element name="C204" type="xs:unsignedByte" />
      <xs:element name="C205" type="xs:unsignedByte" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="anyExt" type="anyExtType" minOccurs="0" />
<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
<xs:attributeGroup ref="IndexType" />
<xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>

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

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

```

7.2.2.4 Default Document Namespace

The default document namespace used in evaluating URIs shall be "urn:3gpp:ns:mcpttUEinitConfig:1.0".

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 7.2.2.2, 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 MCS UE initial configuration document shall conform to the XML Schema described in subclause 7.2.2.3.

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 an <Instance-ID-URN> element of the <mcptt-UE-id> element does not conform to a valid Instance ID as specified in 3GPP TS 23.003 [16], 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 Instance ID URN" and contain the non-conformant <Instance-ID-URN> element.

If the <TAC> element of an <IMEI-range> element does not conform to a valid 8 digit Type Allocation Code as specified in 3GPP TS 23.003 [16], 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 Type Allocation Code" and contain the non-conformant <TAC> element.

If a <SNR> element of an <IMEI--range> element does not conform to a valid 6 digit Serial Number as specified in 3GPP TS 23.003 [16], 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 Serial Number" and contain the non-conformant <SNR> element.

If a <Low-SNR> element or a <High-SNR> element of a <SNR-range> element does not conform to a valid 6 digit Serial Number as specified in 3GPP TS 23.003 [16], 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 Serial Number range" and contain the non-conformant <Low-SNR> or <High-SNR> element.

If the "User-ID" attribute of the <Default-user-profile> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 the "User-ID" attribute of the <Default-user-profile> element does not contain an "XUI-URI" attribute of a MCS user profile configuration document, 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 "No MCS User Profile configuration document exists for the user identified by the User ID URI".

If the "user-profile-index" attribute of the <Default-user-profile> element does not contain an "user-profile-index" attribute of a MCPTT user profile configuration document, 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 "The user profile index does not identify a MCS User Profile configuration document identified of the user identified by the User ID URI".

NOTE: If the MCS administrator includes a <Default-user-profile> element in the MCS UE initial configuration document, at least one instance of a MCS user profile configuration document needs to first be created on the configuration management server, containing the "XUI-URI" attribute and "user-profile-index" attribute that are included in the <Default-user-profile> element.

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-auth-endpoint> element of the <AppServerInfo> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 <idms-token-endpoint> element of the <AppServerInfo> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 IETF RFC 3986 [21], 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 IETF RFC 3986 [21], 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 IETF RFC 3986 [21], 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 IETF RFC 3986 [21], 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 <group-creation-XUI> element of the <on-network> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 creation XUI".

If the <GMS-XCAP-root-URI> element of the <on-network> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 XCAP root URI".

If the <CMS-XCAP-root-URI> element of the <on-network> element does not conform to a valid URI as specified in IETF RFC 3986 [21], 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 CMS XCAP root 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 [16] 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 does not conform to the syntax of a valid PLMN code as defined in 3GPP TS 23.003 [16] 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 65535;
- g) the <TFG12> element contains an integer value between 0 and 65535;
- 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 65535;
- 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 65535;
- 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.

The creator of the MCS UE initial configuration document may include an <mcptt-UE-id> element in the version of the MCS UE initial configuration document that is uploaded to the CMS and may also appear in the MCS UE initial configuration document when downloaded by the MCS administrator. The <mcptt-UE-id> element does not appear in the MCS UE initial configuration managed object specified in 3GPP TS 24.483 [4] that is configured to the MC UE.. If an <mcptt-UE-id> element is included then the MCS UE initial configuration document and corresponding MCS UE initial configuration management object applies only to the MC UE(s) identified by the <mcptt-UE-id> element. If no <mcptt-UE-id> element is included then the MCS UE initial configuration document and corresponding MCS UE initial configuration management object applies to all the MC UEs of the domain.

If one or more optional <Instance-ID-URN> elements is included in the <mcptt-UE-id> element then the MCS UE initial configuration document applies to the MC UE with an instance ID equal to the instance ID contained in the <Instance-ID-URN> element.

The <TAC> element of the <IMEI-range> element contains the Type Allocation Code of the MC UE.

The optional <SNR> element of the <IMEI-range> element contains the individual serial number uniquely identifying MC UE within the Type Allocation Code contained in the <TAC> element that the MCS UE initial configuration document applies to.

If an optional <SNR-range> element is included within the <IMEI-range> element then the MCS UE initial configuration document applies to all MC UEs within the Type Allocation Code contained in the <TAC> element with the serial number equal or greater than the serial number contained in the <Low-SNR> element and less than or equal to the serial number contained in the <High-SNR> element.

If no <SNR> element nor <SNR-range> element is included within the <IMEI-range> element then the MCS UE initial configuration document applies to all the MC UE(s) with the Type Allocation Code contained within the <TAC> element of the <IMEI-range> element.

If no <mcptt-UE-id> element is included then the MCS UE initial configuration document applies to all MC UEs of the mission critical organization identified in the "domain" attribute.

The <name> element of the <mcptt-UE-initial-configuration> element contains the user displayable name of the MCS UE initial configuration document and corresponds to the "Name" element of subclause 8.2.3 in 3GPP TS 24.483 [4].

The "User-ID" attribute of the <Default-user-profile> element contains the XUI contained in the "XUI-URI" attribute of the MCPTT user profile that is intended to be used as default MCS user profile and corresponds to the "UserID" element of subclause 8.2.6 in 3GPP TS 24.483 [4].

The "user-profile-index" attribute of the <Default-user-profile> element contains an indicator for a particular MCS user profile document when multiple MCS user profiles are defined for that MC user and is of type "unsignedByte" and matches a value in a "user-profile-index" attribute of the MC user profile that is intended to be used as default MCS user profile. and corresponds to the "UserProfileIndex" element of subclause 8.2.7 in 3GPP TS 24.483 [4]

The <on-network> element contains MCS UE initial configuration data for on-network operation only.

The <off-network> element contains MC UE initial configuration data for off-network operation 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 8.2.11 in 3GPP TS 24.483 [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 8.2.12 in 3GPP TS 24.483 [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 8.2.13 in 3GPP TS 24.483 [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 8.2.14 in 3GPP TS 24.483 [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 8.2.15 in 3GPP TS 24.483 [4].
- 2) the "PLMN" attribute of the <HPLMN> element contains the PLMN code of the HPLMN as defined in 3GPP TS 23.003 [16] and corresponds to the "PLMN" element of subclause 8.2.18 in 3GPP TS 24.483 [4];
- 3) the "PLMN" attribute of the <VPLMN> element contains the PLMN code of a VPLMN as defined in 3GPP TS 23.003 [16] and corresponds to the "PLMN" element of subclause 8.2.30 in 3GPP TS 24.483 [4];
- 4) the <AppServerInfo> element:
 - a) the <idms-auth-endpoint> element contains the URI used to contact the identity management server and corresponds to the "IDMSAuthEndpoint" element of subclause 8.2.41 in 3GPP TS 24.483 [4];
 - b) the <idms-token-endpoint> element contains the URI used to contact the identity management server and corresponds to the "IDMSTokenEndpoint" element of subclause 8.2.41A in 3GPP TS 24.483 [4];
 - c) the <gms> element contains the URI used to contact the group management server and corresponds to the "GMS" element of subclause 8.2.42 in 3GPP TS 24.483 [4];
 - d) the <cms> element contains the URI used to contact the configuration management server and corresponds to the "CMS" element of subclause 8.2.43 in 3GPP TS 24.483 [4]; and
 - e) the <kms> element contains the URI used to contact the key management server and corresponds to the "KMS" element of subclause 8.2.44 in 3GPP TS 24.483 [4];
- 5) the <GMS-URI> element contains the group management service URI information to enable hiding of MCS identities, the group management service URI information contains the public service identity for performing subscription proxy function of the GMS and corresponds to the "GMSURI" element of subclause 8.2.9 in 3GPP TS 24.483 [4];
- 6) the <group-creation-XUI> element contains the group management server XCAP Root URI information and corresponds to the "GroupCreationXUI" element of subclause 8.2.9A in 3GPP TS 24.483 [4];
- 7) the <GMS-XCAP-root-URI> element contains the group management server XCAP Root URI and corresponds to the "GMSXCAPRootURI" element of subclause 8.2.9B in 3GPP TS 24.483 [4]; and
- 8) the <CMS-XCAP-root-URI> element contains the configuration management server XCAP Root URI and corresponds to the "CMSXCAPRootURI" element of subclause 8.2.9C in 3GPP TS 24.483 [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 8.2.47 in 3GPP TS 24.483 [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 8.2.48 in 3GPP TS 24.483 [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 8.2.49 in 3GPP TS 24.483 [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 8.2.50 in 3GPP TS 24.483 [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 8.2.51 in 3GPP TS 24.483 [4];
- f) the <TFG11> element contains the timer value in milliseconds for MCPTT emergency end retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG11" element of subclause 8.2.52 in 3GPP TS 24.483 [4];
- g) the <TFG12> element contains the timer value in milliseconds for MCPTT imminent peril end retransmission as specified in 3GPP TS 24.379 [9] and corresponds to the "TFG12" element of subclause 8.2.53 in 3GPP TS 24.483 [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 8.2.54 in 3GPP TS 24.483 [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 8.2.55 in 3GPP TS 24.483 [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 8.2.56 in 3GPP TS 24.483 [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 8.2.57 in 3GPP TS 24.483 [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 8.2.58 in 3GPP TS 24.483 [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 8.2.59 in 3GPP TS 24.483 [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 8.2.60 in 3GPP TS 24.483 [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 8.2.61 in 3GPP TS 24.483 [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 8.2.62 in 3GPP TS 24.483 [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 8.2.63 in 3GPP TS 24.483 [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 8.2.64 in 3GPP TS 24.483 [4];
- s) the <T201> element contains the timer value in milliseconds for floor request as specified in 3GPP TS 24.380 [10] and corresponds to the "T201" element of subclause 8.2.65 in 3GPP TS 24.483 [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 8.2.66 in 3GPP TS 24.483 [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 8.2.67 in 3GPP TS 24.483 [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 8.2.68 in 3GPP TS 24.483 [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 8.2.69 in 3GPP TS 24.483 [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 8.2.70 in 3GPP TS 24.483 [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 8.2.71 in 3GPP TS 24.483 [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 8.2.72 in 3GPP TS 24.483 [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 8.2.74 in 3GPP TS 24.483 [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 8.2.75 in 3GPP TS 24.483 [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 8.2.76 in 3GPP TS 24.483 [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 8.2.77 in 3GPP TS 24.483 [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 8.2.78 in 3GPP TS 24.483 [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 8.2.79 in 3GPP TS 24.483 [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 8.2.80 in 3GPP TS 24.483 [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 8.2.81 in 3GPP TS 24.483 [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 8.2.82 in 3GPP TS 24.483 [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 MCS 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 MCS UE initial configuration document application usage shall support subscription to changes as specified in subclause 6.3.13.3 .

MCS UE initial configuration documents are kept as XDM collections. Therefore, it is possible to subscribe to all MCST UE initial configuration documents of a MC user according to XCAP URI construction convention of a trailing '/', as specified in IETF RFC 5875 [11].

8 MCPTT configuration management documents

8.1 Introduction

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

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

8.2 MCPTT UE configuration document

8.2.1 General

The MCPTT UE configuration document is specified in this subclause. The MCPTT UE configuration document content is based on requirements of Annex A.2 of 3GPP TS 23.379 [8], in accordance with OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. The usage of an MCPTT UE configuration document 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 8.2.2.3. An MCPTT UE configuration document may apply to all MCPTT UEs of a mission critical organization or apply to specific MCPTT UEs identified in the <mcptt-UE-id> element. If there is no <mcptt-UE-id> element in the MCPTT UE configuration document, then by default the MCPTT UE configuration document applies to all MCPTT UEs of the mission critical organization that are not specifically identified in the <mcptt-UE-id> element of another MCPTT UE initial configuration document of the mission critical organization. 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.

MCPTT UE configuration documents of a MCPTT user are contained as "XDM collections" in the user's directory of the "Users Tree", in accordance with OMA OMA-TS-XDM_Core-V2_1-20120403-A [2]. A MCPTT UE configuration document corresponding to a specific MCPTT UE the MCPTT user has used to authenticate and is authorised to use the MCPTT service with is placed in the user directory of the MCPTT user.

The MCPTT UE configuration document acts as a template for the CMS to generate UE configuration documents that are downloaded to specific MCPTT UEs. The MCPTT UE configuration document that acts as a template is referred to as a "master MCPTT UE configuration document". The master MCPTT UE configuration document name is assigned by an MCPTT system administrator when the document is created and is stored in the users tree of that MCPTT system administrator. The master MCPTT UE configuration document does not directly apply to a specific MCPTT UE, but instead acts as template that the CMS uses to populate the MCPTT UE configuration documents of MCPTT UEs identified by elements of the <MCPTT-UE-id> element. For MCPTT UE configuration documents that correspond to a specific MCPTT UE, the name of the MCPTT UE configuration document is created from a value defined by the corresponding element that identifies the MCPTT UE within the <MCPTT-UE-id> element. For a master MCPTT UE configuration documents that does not contain a <MCPTT-UE-id> element, the name of the MCPTT UE configuration document stored in the user directory is "DEFAULT-MCPTT-UE.xml".

8.2.2 Coding

8.2.2.1 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 <mcptt-UE-id> element;
- 3) may include a <name> element;
- 4) shall include a <common> element;
- 5) shall include an <on-network> element; and
- 6) 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) may contain a list of <Relayed-MCPTT-Group> elements containing:
 - a) a <MCPTT-Group-ID> element; and
 - b) a <Relay-Service-Code> element.

NOTE: When the <Relay-Service> element is set to "false" a list of <Relayed-MCPTT-Group> elements is not needed.

The <mcptt-UE-id> element:

- 1) may contain a list of <Instance-ID-URN> elements; and
- 2) may contain a list of <IMEI-range> elements.

The <IMEI-range> element:

- 1) shall contain a <TAC> element;
- 2) may contain a list of <SNR> elements; and
- 3) may contain <SNR-range> element.

The <SNR-range> element:

- 1) shall contain a <Low-SNR> element; and
- 2) shall contain a <High-SNR> element.

8.2.2.2 Application Unique ID

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

8.2.2.3 XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:mcpttuep="urn:3gpp:mcptt:mcpttUEConfig:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:mcptt:mcpttUEConfig: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="mcptt-UE-configuration">
    <xs:complexType>
      <xs:sequence>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:element name="mcptt-UE-id" type="mcpttuep:MCPTTUEIDType"/>
          <xs:element name="name" type="mcpttuep:NameType"/>
          <xs:element name="anyExt" type="mcpttuep:anyExtType"/>
          <xs:any namespace="##other" processContents="lax"/>
        </xs:choice>
        <xs:element name="common" type="mcpttuep:CommonType"/>
        <xs:element name="on-network" type="mcpttuep:On-networkType"/>
        <xs:element name="anyExt" type="mcpttuep:anyExtType"/>
        <xs:any namespace="##other" processContents="lax"/>
      </xs:sequence>
      <xs:attribute name="domain" type="xs:anyURI" use="required"/>
      <xs:attribute name="XUI-URI" type="xs:anyURI"/>
      <xs:attribute name="Instance-ID-URN" type="xs:anyURI"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>

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

  <xs:complexType name="MCPTTUEIDType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="Instance-ID-URN" type="xs:anyURI"/>
      <xs:element name="IMEI-range" type="mcpttuep:IMEI-rangeType"/>
      <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:attributeGroup ref="IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="IMEI-rangeType">
    <xs:sequence>
      <xs:element name="TAC" type="tacType"/>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="SNR" type="mcpttuep:snrType"/>
        <xs:element name="SNR-range" type="mcpttuep:SNR-rangeType"/>
      </xs:choice>
      <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attributeGroup ref="IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

```

```

</xs:complexType>

<xs:complexType name="SNR-rangeType">
  <xs:sequence>
    <xs:element name="Low-SNR" type="mcpttuep:snrType"/>
    <xs:element name="High-SNR" type="mcpttuep:snrType"/>
    <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:simpleType name="tac-baseType">
  <xs:restriction base="xs:decimal">
    <xs:totalDigits value="8"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="tacType">
  <xs:simpleContent>
    <xs:extension base="tac-baseType">
      <xs:attributeGroup ref="IndexType"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="snr-baseType">
  <xs:restriction base="xs:decimal">
    <xs:totalDigits value="6"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="snrType">
  <xs:simpleContent>
    <xs:extension base="snr-baseType">
      <xs:attributeGroup ref="IndexType"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="CommonType">
  <xs:sequence>
    <xs:element name="private-call">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="Max-Simul-Call-N10" type="xs:positiveInteger"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="MCPTT-Group-Call">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="Max-Simul-Call-N4" type="xs:positiveInteger"/>
          <xs:element name="Max-Simul-Trans-N5" type="xs:positiveInteger"/>
          <xs:element name="Prioritized-MCPTT-Group">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="MCPTT-Group-Priority" maxOccurs="unbounded">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="MCPTT-Group-ID" type="xs:anyURI"/>
                      <xs:element name="group-priority-hierarchy" type="xs:nonNegativeInteger"/>
                    </xs:sequence>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attributeGroup ref="IndexType"/>

```

```

    <xs:anyAttribute namespace="##any" processContents="lax" />
  </xs:complexType>

  <xs:complexType name="On-networkType">
    <xs:sequence>
      <xs:element name="IPv6Preferred" type="xs:boolean" />
      <xs:element name="Relay-Service" type="xs:boolean" />
      <xs:element name="Relayed-MCPTT-Group" type="mcpttuep:Relayed-MCPTT-GroupType" />
      <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0" />
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attributeGroup ref="IndexType" />
    <xs:anyAttribute namespace="##any" processContents="lax" />
  </xs:complexType>

  <xs:complexType name="Relayed-MCPTT-GroupType">
    <xs:sequence>
      <xs:element name="MCPTT-Group-ID" type="xs:anyURI" />
      <xs:element name="Relay-Service-Code" type="xs:string" />
      <xs:element name="anyExt" type="mcpttuep:anyExtType" minOccurs="0" />
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>

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

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

```

8.2.2.4 Default Document Namespace

The default document namespace used in evaluating URIs shall be "urn:3gpp:ns:mcpttUEConfig:1.0".

8.2.2.5 MIME type

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

8.2.2.6 Validation Constraints

If the AUID value of the document URI or node URI in the Request-URI is other than that specified in subclause 8.2.2.2, 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 8.2.2.3.

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".

If an <Instance-ID-URN> element of the <mcptt-UE-id> element does not conform to a valid Instance ID as specified in 3GPP TS 23.003 [16], 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 Instance ID URN" and contain the non-conformant <Instance-ID-URN> element.

If the <TAC> element of an <IMEI-range> element does not conform to a valid 8 digit Type Allocation Code as specified in 3GPP TS 23.003 [16], 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 Type Allocation Code" and contain the non-conformant <TAC> element.

If a <SNR> element of an <IMEI-range> element does not conform to a valid 6 digit Serial Number as specified in 3GPP TS 23.003 [16], 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 Serial Number" and contain the non-conformant <SNR> element.

If a <Low-SNR> element or a <High-SNR> element of a <SNR-range> element does not conform to a valid 6 digit Serial Number as specified in 3GPP TS 23.003 [16], 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 Serial Number range" and contain the non-conformant <Low-SNR> or <High-SNR> element.

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".

8.2.2.7 Data Semantics

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

The <name> element of the <mcptt-UE-configuration> element contains the user displayable name of the MCPTT UE configuration document and corresponds to the "Name" element of subclause 4.2.3 in 3GPP TS 24.483 [4].

The creator of the MCPTT UE configuration document may include an <mcptt-UE-id> element in the version of the MCPTT UE configuration document that is uploaded to the CMS and may also appear in the MCPTT UE configuration document when downloaded by the MCPTT system administrator. The <mcptt-UE-id> element does not appear in the MCPTT UE configuration document that is configured to the MCPTT UE. If an <mcptt-UE-id> element is included then the MCPTT UE configuration document applies only to the MCPTT UE(s) identified by the <mcptt-UE-id> element. If no <mcptt-UE-id> element is included then the MCPTT UE configuration document t applies to all the MCPTT UEs of the domain.

If one or more optional <Instance-ID-URN> elements is included in the <mcptt-UE-id> element then the MCPTT UE configuration document applies to the MCPTT UE with an instance ID equal to the instance ID contained in the <Instance-ID-URN> element.

The <TAC> element of the <IMEI-range> element contains the Type Allocation Code of the MCPTT UE.

The optional <SNR> element of the <IMEI-range> element contains the individual serial number uniquely identifying MCPTT UE within the Type Allocation Code contained in the <TAC> element that the MCPTT UE initial configuration document applies to.

If an optional <SNR-range> element is included within the <IMEI-range> element then the MCPTT UE configuration document applies to all MCPTT UEs within the Type Allocation Code contained in the <TAC> element with the serial number equal or greater than the serial number contained in the <Low-SNR> element and less than or equal to the serial number contained in the <High-SNR> element.

If no <SNR> element nor <SNR-range> element is included within the <IMEI-range> element then the MCPTT UE configuration document applies to all the MCPTT UE(s) with the Type Allocation Code contained within the <TAC> element of the <IMEI-range> element.

If no <mcptt-UE-id> element is included then the MCPTT UE configuration document applies to all MCPTT UEs of the mission critical organization identified in the "domain" attribute.

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

The <on-network> element contains MCPTT UE configuration data for on-network operation 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 24.483 [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 24.483 [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 24.483 [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 24.483 [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 24.483 [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 24.483 [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 "RelayService" element of subclause 4.2.16 in 3GPP TS 24.483 [4];
- 2) an <IPv6Preferred> element which corresponds to the "IPv6Preferred" element of subclause 4.2.17 in 3GPP TS 24.483 [4],
 - a) if the UE has both IPv4 and IPv6 host configuration::
 - i) if IPv6Preferred is set to true then the UE shall use IPv6 for all on-network signalling and media; otherwise
 - ii) if IPv6Preferred is set to false then the UE shall use IPv4 for all on-network signalling and media;
 - b) if the UE has only IPv4 host configuration then the UE shall use IPv4 for all on-network signalling and media; and
 - c) if the UE has only IPv6 host configuration then the UE shall use IPv6 for all on-network signalling and media; and
- 3) the <Relayed-MCPTT-Groups> element of the <Relay-Service> element which corresponds to the "RelayedMCPTTGroup" element of subclause 4.2.18 in 3GPP TS 24.483 [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 24.483 [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 24.483 [4].

8.2.2.8 Naming Conventions

The present document defines no naming conventions.

8.2.2.9 Global documents

The present document requires no global documents.

8.2.2.10 Resource interdependencies

There are no resource interdependencies.

8.2.2.11 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".

8.2.2.12 Subscription to Changes

The MCPTT UE configuration document application usage shall support subscription to changes as specified in subclause 6.3.13.3.

MCPTT UE configuration documents are kept as XDM collections. Therefore, it is possible to subscribe to all MCPTT UE configuration documents of a MCPTT user according to XCAP URI construction convention of a trailing '/', as specified in IETF RFC 5875 [11].

8.3 MCPTT user profile configuration document

8.3.1 General

The MCPTT user profile configuration document is specified in this subclause. The MCPTT user profile configuration document content is based on requirements of Annex A.3 of 3GPP TS 23.379 [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 8.3.2.

MCPTT user profile documents are "XDM collections" in the user's directory in the "Users Tree", in accordance with OMA OMA-TS-XDM_Core-V2_1-20120403-A [2].

The name of the MCPTT user profile document matches the value of the <ProfileName> element in the MCPTT user profile document.

8.3.2 Coding

8.3.2.1 Structure

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

The <mcptt-user-profile> document:

- 1) shall include an "XUI-URI" attribute;
- 2) may include a <Name> element;
- 3) shall include one <Status> element;
- 4) shall include a "user-profile-index" attribute;
- 5) may include any other attribute for the purposes of extensibility;
- 6) may include one <ProfileName> element;
- 7) may include a <Pre-selected-indication> element;
- 8) shall include one or more <Common> elements, each of which:
 - a) shall have an "index" attribute;
 - b) shall include one <UserAlias> element containing one or more <alias-entry> elements
 - c) shall include one <MCPTTUserID> element that contains an <entry> element;
 - d) shall include one <PrivateCall> element. The <PrivateCall> element contains:
 - i) a <PrivateCallList> element that contains:
 - A) a <PrivateCallURI> element that contains one or more <entry> elements; and
 - B) a <PrivateCallProSeUser> element that contains one or more <ProSeUserID-entry> elements; and
 - ii) one <EmergencyCall> element containing one <MCPTTPrivateRecipient> element that contains:
 - A) an <entry> element; and
 - B) a <ProSeUserID-entry> element;
 - e) shall contain one <MCPTT-group-call> element containing:
 - i) one <MaxSimultaneousCallsN6> element;
 - ii) one <EmergencyCall> element containing one <MCPTTGroupInitiation>element that contains an <entry> element;

- iii) one <ImminentPerilCall> element containing one <MCPTTGroupInitiation> element that contains an <entry> element;
 - iv) one <EmergencyAlert> element containing an <entry> element; and
 - v) one <Priority> element;
 - f) may contain one <ParticipantType> element; and
 - g) shall contain one <MissionCriticalOrganization> element indicating the name of the mission critical organization the MCPTT User belongs to;
- 9) shall include zero or more <OffNetwork> elements each of which:
- a) shall contain an "index" attribute; and
 - b) shall include one or more <MCPTTGroupInfo> elements, each containing one or more <entry> elements.;
- 10) shall include zero or more <OnNetwork> elements each of which:
- a) shall have an "index" attribute;
 - b) shall include one or more <MCPTTGroupInfo> elements, each containing one or more <entry> elements;
 - c) shall include one <MaxAffiliationsN2> element;
 - d) may include one or more <ImplicitAffiliations> elements, each containing one or more <entry> elements;
 - e) shall include one <MaxSimultaneousTransmissionsN7> element; and
 - f) shall include one <PrivateEmergencyAlert> element containing an <entry> element;
- 11) 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-presence-status> element;
 - ii) an <allow-request-presence> element;
 - iii) an <allow-query-availability-for-private-calls> element;
 - iv) an <allow-enable-disable-user> element;
 - v) an <allow-enable-disable-UE> element;
 - vi) an <allow-create-delete-user-alias> element;
 - vii) an <allow-private-call> element;
 - viii) an <allow-manual-commencement> element;
 - ix) an <allow-automatic-commencement> element;
 - x) an <allow-force-auto-answer> element;
 - xi) an <allow-failure-restriction> element;
 - xii) an <allow-emergency-group-call> element;
 - xiii) an <allow-emergency-private-call> element;
 - xiv) an <allow-cancel-group-emergency> element;
 - xv) an <allow-cancel-private-emergency-call> element;

- xvi) an <allow-imminent-peril-call> element;
- xvii) an <allow-cancel-imminent-peril> element;
- xviii) an <allow-activate-emergency-alert> element;
- xix) an <allow-cancel-emergency-alert> element;
- xx) an <allow-offnetwork> element;
- xxi) an <allow-imminent-peril-change> element;
- xxii) an <allow-private-call-media-protection> element;
- xxiii) an <allow-private-call-floor-control-protection> element;
- xxiv) an <allow-request-affiliated-groups> element;
- xxv) an <allow-request-to-affiliate-other-users> element;
- xxvi) an <allow-recommend-to-affiliate-other-users> element;
- xxvii) an <allow-private-call-to-any-user> element;
- xxviii) an <allow-regroup> element;
- xxix) an <allow-private-call-participation> element;
- xxx) an <allow-override-of-transmission> element;
- xxxi) an <allow-manual-off-network-switch> element;
- xxxii) an <allow-listen-both-overriding-and-overridden> element;
- xxxiii) an <allow-transmit-during-override> element;
- xxxiv) an <allow-off-network-group-call-change-to-emergency> element;
- xxxv) an <allow-revoke-transmit> element;
- xxxvi) an <allow-create-group-broadcast-group> element;
- xxxvii) an <allow-create-user-broadcast-group> element; and
- xxxviii) an <anyExt> element which may contain:
 - A) an <allow-request-private-call-call-back> element; and
 - B) an <allow-cancel-private-call-call-back> element; and

12) may include any other element for the purposes of extensibility.

The <entry> elements:

- 1) shall contain a <uri-entry> element;
- 2) shall contain an "index" attribute;
- 3) may contain a <display-name> element; and
- 4) may contain an "entry-info" attribute.

The <ProSeUserID-entry> elements:

- 1) shall contain a <DiscoveryGroupID> element ;
- 2) shall contain an <User-Info-ID> element; and
- 3) shall contain an "index" attribute.

8.3.2.2 Application Unique ID

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

8.3.2.3 XML Schema

The MCPTT user profile configuration document shall be composed according to the following XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:mcpttup="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"/>
  <!-- This import brings in common policy namespace from RFC 4745 -->
  <xs:import namespace="urn:ietf:params:xml:ns:common-policy"
    schemaLocation="http://www.iana.org/assignments/xml-registry/schema/common-policy.xsd"/>

  <xs:element name="mcptt-user-profile">
    <xs:complexType>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="Name" type="mcpttup:NameType"/>
        <xs:element name="Status" type="xs:boolean"/>
        <xs:element name="ProfileName" type="mcpttup:NameType"/>
        <xs:element name="Pre-selected-indication" type="mcpttup:emptyType"/>
        <xs:element name="Common" type="mcpttup:CommonType"/>
        <xs:element name="OffNetwork" type="mcpttup:OffNetworkType"/>
        <xs:element name="OnNetwork" type="mcpttup:OnNetworkType"/>
        <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
        <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:unsignedByte" use="required"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="NameType">
    <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="mcpttup:UserAliasType"/>
      <xs:element name="MCPTTUserID" type="mcpttup:EntryType"/>
      <xs:element name="PrivateCall" type="mcpttup:MCPTTPrivateCallType"/>
      <xs:element name="MCPTT-group-call" type="mcpttup:MCPTTGroupCallType"/>
      <xs:element name="MissionCriticalOrganization" type="xs:string"/>
      <xs:element name="ParticipantType" type="xs:string"/>
      <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:attributeGroup ref="IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="MCPTTPrivateCallType">
    <xs:sequence>
      <xs:element name="PrivateCallList" type="mcpttup:PrivateCallListEntryType"/>
      <xs:element name="EmergencyCall" type="mcpttup:EmergencyCallType" minOccurs="0"/>
      <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="PrivateCallListEntryType">
    <xs:choice minOccurs="1" maxOccurs="unbounded">
      <xs:element name="PrivateCallURI" type="mcpttup:EntryType"/>
    </xs:choice>
  </xs:complexType>
```

```

    <xs:element name="PrivateCallProSeUser" type="mcpttup:ProSeUserEntryType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

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

<xs:complexType name="EntryType">
  <xs:sequence>
    <xs:element name="uri-entry" type="xs:anyURI"/>
    <xs:element name="display-name" type="mcpttup:DisplayNameElementType" minOccurs="0"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:sequence>
  <xs:attribute name="entry-info" type="mcpttup:EntryInfoTypeList"/>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="ProSeUserEntryType">
  <xs:sequence>
    <xs:element name="DiscoveryGroupID" type="xs:hexBinary" minOccurs="0"/>
    <xs:element name="User-Info-ID" type="xs:hexBinary"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:sequence>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:simpleType name="EntryInfoTypeList">
  <xs:restriction base="xs:normalizedString">
    <xs:enumeration value="UseCurrentlySelectedGroup"/>
    <xs:enumeration value="DedicatedGroup"/>
    <xs:enumeration value="UsePreConfigured"/>
    <xs:enumeration value="LocallyDetermined"/>
  </xs:restriction>
</xs:simpleType>

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

```



```

<xs:complexType name="MCPTTGroupCallType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MaxSimultaneousCallsN6" type="xs:positiveInteger"/>
    <xs:element name="EmergencyCall" type="mcpttup:EmergencyCallType"/>
    <xs:element name="ImminentPerilCall" type="mcpttup:ImminentPerilCallType"/>
    <xs:element name="EmergencyAlert" type="mcpttup:EmergencyAlertType"/>
    <xs:element name="Priority" type="xs:unsignedShort"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="EmergencyCallType">
  <xs:sequence>
    <xs:choice>
      <xs:element name="MCPTTGroupInitiation" type="mcpttup:MCPTTGroupInitiationEntryType"/>
      <xs:element name="MCPTTPrivateRecipient" type="mcpttup:MCPTTPrivateRecipientEntryType"/>
      <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="ImminentPerilCallType">
  <xs:sequence>
    <xs:element name="MCPTTGroupInitiation" type="mcpttup:MCPTTGroupInitiationEntryType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="EmergencyAlertType">
  <xs:sequence>
    <xs:element name="entry" type="mcpttup:EntryType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="MCPTTGroupInitiationEntryType">
  <xs:choice>
    <xs:element name="entry" type="mcpttup:EntryType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="MCPTTPrivateRecipientEntryType">
  <xs:choice>
    <xs:element name="entry" type="mcpttup:EntryType"/>
    <xs:element name="ProSeUserID-entry" type="mcpttup:ProSeUserEntryType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="OffNetworkType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MCPTTGroupInfo" type="ListEntryType"/>
    <xs:element name="User-Info-ID" type="xs:hexBinary"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="OnNetworkType">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="MCPTTGroupInfo" type="mcpttup:ListEntryType"/>
    <xs:element name="MaxAffiliationsN2" type="xs:nonNegativeInteger"/>
    <xs:element name="MaxSimultaneousTransmissionsN7" type="xs:nonNegativeInteger"/>
  </xs:choice>

```

```

    <xs:element name="ImplicitAffiliations" type="mcpttup:ListEntryType"/>
    <xs:element name="PrivateEmergencyAlert" type="mcpttup:EmergencyAlertType"/>
    <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"/>
  </xs:choice>
  <xs:attributeGroup ref="IndexType"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:element name="allow-presence-status" type="xs:boolean"/>
<xs:element name="allow-request-presence" type="xs:boolean"/>
<xs:element name="allow-query-availability-for-private-calls" type="xs:boolean"/>
<xs:element name="allow-enable-disable-user" type="xs:boolean"/>
<xs:element name="allow-enable-disable-UE" type="xs:boolean"/>
<xs:element name="allow-force-delete-user-alias" type="xs:boolean"/>
<xs:element name="allow-private-call" type="xs:boolean"/>
<xs:element name="allow-manual-commencement" type="xs:boolean"/>
<xs:element name="allow-automatic-commencement" type="xs:boolean"/>
<xs:element name="allow-force-auto-answer" type="xs:boolean"/>
<xs:element name="allow-failure-restriction" type="xs:boolean"/>
<xs:element name="allow-emergency-group-call" type="xs:boolean"/>
<xs:element name="allow-emergency-private-call" type="xs:boolean"/>
<xs:element name="allow-cancel-group-emergency" type="xs:boolean"/>
<xs:element name="allow-cancel-private-emergency-call" type="xs:boolean"/>
<xs:element name="allow-imminent-peril-call" type="xs:boolean"/>
<xs:element name="allow-cancel-imminent-peril" type="xs:boolean"/>
<xs:element name="allow-activate-emergency-alert" type="xs:boolean"/>
<xs:element name="allow-cancel-emergency-alert" type="xs:boolean"/>
<xs:element name="allow-offnetwork" type="xs:boolean"/>
<xs:element name="allow-imminent-peril-change" type="xs:boolean"/>
<xs:element name="allow-private-call-media-protection" type="xs:boolean"/>
<xs:element name="allow-private-call-floor-control-protection" type="xs:boolean"/>
<xs:element name="allow-request-affiliated-groups" type="xs:boolean"/>
<xs:element name="allow-request-to-affiliate-other-users" type="xs:boolean"/>
<xs:element name="allow-recommend-to-affiliate-other-users" type="xs:boolean"/>
<xs:element name="allow-private-call-to-any-user" type="xs:boolean"/>
<xs:element name="allow-regroup" type="xs:boolean"/>
<xs:element name="allow-private-call-participation" type="xs:boolean"/>
<xs:element name="allow-override-of-transmission" type="xs:boolean"/>
<xs:element name="allow-manual-off-network-switch" type="xs:boolean"/>
<xs:element name="allow-listen-both-overriding-and-overridden" type="xs:boolean"/>
<xs:element name="allow-transmit-during-override" type="xs:boolean"/>
<xs:element name="allow-off-network-group-call-change-to-emergency" type="xs:boolean"/>
<xs:element name="allow-revoke-transmit" type="xs:boolean"/>
<xs:element name="allow-create-group-broadcast-group" type="xs:boolean"/>
<xs:element name="allow-create-user-broadcast-group" type="xs:boolean"/>
<xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>

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

<!-- empty complex type -->
<xs:complexType name="emptyType"/>

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

</xs:schema>

```

8.3.2.4 Default Document Namespace

The default document namespace used in evaluating .URIs shall be "urn:3gpp:mcptt:user-profile:1.0".

8.3.2.5 MIME type

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

8.3.2.6 Validation Constraints

The MCPTT user profile configuration document shall conform to the XML Schema described in subclause 8.3.2.3 "*XML Schema*", with the clarifications given in this subclause.

The value of the "XUI-URI" attribute of the <mcptt-user-profile> element shall be the same as the XUI value of the Document URI for the MCPTT 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 value of the <Priority> element of the <MCPTT-group-call> element shall be within the range of 0 to 255. 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 "Priority value out of range".

The value of the <DiscoveryGroupID> shall be 3 octets expressed in hexadecimal format. 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 "Invalid Discovery Group ID".

The value of the <User-Info-ID> shall be 6 octets expressed in hexadecimal format. 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 "Invalid User Info ID".

If more than one MCPTT user profile document is specified for the MCPTT user in the "XDM collections" in the user's directory, then only one MCPTT user profile document shall contain the <Pre-selected-indication> element. If there is only one MCPTT user profile specified for the MCPTT user in the user's directory, then it is optional to include the <Pre-selected-indication> element. If a MCPTT user profile document containing the <Pre-selected-indication> element already exists for the MCPTT user in the "XDM collections" 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 "Pre-selected User Profile Indication already exists in:" including the contents of the <Profile-Name> element of the MCPTT user profile document that already contains the <Pre-selected-indication> element.

8.3.2.7 Data Semantics

The <Name> element is of type "token", and corresponds to the "Name" element of subclause 5.2.3 in 3GPP TS 24.483 [4].

The <alias-entry> element of the <UserAlias> element is of type "token" and indicates an alphanumeric alias of the MCPTT user, and corresponds to the leaf nodes of the "UserAlias" element of subclause 5.2.8 in 3GPP TS 24.483 [4].

The <uri-entry> element is of type "anyURI" and when it appears within:

- the <MCPTTUserID> element contains the MCPTT user identity (MCPTT ID) of the MCPTT user, and corresponds to the "MCPTTUserID" element of subclause 5.2.7 in 3GPP TS 24.483 [4];
- the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element of the <MCPTT-group-call> element, indicates the MCPTT group used on initiation of an MCPTT emergency group call and corresponds to the "GroupID" element of the "MCPTTGroupInitiation" element of subclause 5.2.34B in 3GPP TS 24.483 [4];
- the <entry> element of the <MCPTTPrivateRecipient> of the <EmergencyCall> element of the <PrivateCall> element indicates the recipient MCPTT user for an MCPTT emergency private call and corresponds to the "ID" element of subclause 5.2.29B in 3GPP TS 24.483 [4];
- the <entry> element of the <MCPTTGroupInitiation> element of the <ImminentPerilCall> element of the <MCPTT-group-call> element, indicates the MCPTT group used on initiation of an MCPTT imminent peril group call and corresponds to the "GroupID" element of subclause 5.2.39B in 3GPP TS 24.483 [4];
- the <entry> element of the <EmergencyAlert> element of the <MCPTT-group-call> element, indicates the MCPTT group recipient for an MCPTT emergency Alert and corresponds to the "ID" element of subclause 5.2.43B in 3GPP TS 24.483 [4];
- the <entry> element of the <EmergencyAlert> element of the <PrivateEmergencyAlert> element indicates the MCPTT user recipient for an on-network MCPTT emergency private alert and corresponds to the "ID" element of subclause 5.2.48J4 in 3GPP TS 24.483 [4];

- the <PrivateCallURI> of the <PrivateCall> list element indicates an MCPTT ID of an MCPTT user that the MCPTT user is authorised to initiate a private call to and corresponds to the "MCPTTID" element of subclause 5.2.17 in 3GPP TS 24.483 [4];
- the <entry> element of the <ImplicitAffiliations> list element indicates an MCPTT group ID of an MCPTT group that the MCPTT user is implicitly affiliated with and corresponds to the "MCPTTGroupID" element of subclause 5.2.48C4 in 3GPP TS 24.483 [4]; and
- the <entry> element of the <MCPTTGroupInfo> list element of the <OnNetwork> element indicates an MCPTT group ID of an MCPTT group that the MCPTT user is authorised to affiliate with during on-network operation and corresponds to the "MCPTTGroupID" element of subclause 5.2.48B4 in 3GPP TS 24.483 [4].

The <DiscoveryGroupID> element is of type "hexBinary" and is used as the Discovery Group ID in the ProSe discovery procedures as specified in 3GPP TS 23.303 [18] and 3GPP TS 23.334 [19]. When it appears within:

- the <MCPTTPrivateRecipient> element of the <EmergencyCall> element it identifies the Discovery Group ID that the MCPTT UE uses to initiate an off-network MCPTT emergency private call and corresponds to the "DiscoveryGroupID" element of subclause 5.2.29C in 3GPP TS 24.483 [4]; and
- the <PrivateCallProSeUser> element of the <PrivateCallList> element it identifies the Discovery Group ID that the MCPTT UE uses to initiate a private call during off-network operation and corresponds to the "DiscoveryGroupID" element of subclause 5.2.18 in 3GPP TS 24.483 [4].

The <display-name> element is of type "string", contains a human readable name and when it appears within:

- the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element of the <MCPTT-group-call> element, indicates the name of the MCPTT group used on initiation of an MCPTT emergency group call and corresponds to the "DisplayName" element of the "MCPTTGroupInitiation" element of subclause 5.2.34C in 3GPP TS 24.483 [4];
- the <entry> element of the <MCPTTPrivateRecipient> of the <EmergencyCall> element of the <PrivateCall> element indicates the name of the recipient MCPTT user for an MCPTT emergency private call and corresponds to the "DisplayName" element of subclause 5.2.29E in 3GPP TS 24.483 [4];
- the <entry> element of the <MCPTTGroupInitiation> element of the <ImminentPerilCall> element of the <MCPTT-group-call> element, indicates the name of the MCPTT group used on initiation of an MCPTT imminent peril group call and corresponds to the "DisplayName" element of subclause 5.2.39C in 3GPP TS 24.483 [4];
- the <entry> element of the <EmergencyAlert> element of the <MCPTT-group-call> element, indicates the name of the MCPTT group recipient for an MCPTT emergency Alert and corresponds to the "DisplayName" element of subclause 5.2.43D in 3GPP TS 24.483 [4];
- the <entry> element of the <EmergencyAlert> element of the <PrivateEmergencyAlert> element indicates the name of the MCPTT user recipient for an on-network MCPTT emergency private alert and corresponds to the "DisplayName" element of subclause 5.2.48J5 in 3GPP TS 24.483 [4];
- the <PrivateCallURI> of the <PrivateCallList> element indicates the name of an MCPTT ID of an MCPTT user that the MCPTT user is authorised to initiate a private call to and corresponds to the "DisplayName" element of subclause 5.2.19A in 3GPP TS 24.483 [4];
- the <MCPTTGroupInfo> list element of the <OnNetwork> element indicates the name of an MCPTT group ID of an MCPTT group that the MCPTT user is authorised to affiliate with during on-network operation and corresponds to the "DisplayName" element of subclause 5.2.48B5 in 3GPP TS 24.483 [4]; and
- the <ImplicitAffiliations> list element indicates the name of of an MCPTT group that the MCPTT user is implicitly affiliated with and corresponds to the "DisplayName" element of subclause 5.2.48C5 in 3GPP TS 24.483 [4]; and
- the <MCPTTGroupInfo> list element of the <OffNetwork> element indicates the name of an off-network MCPTT group that the MCPTT user is authorised to join during off-network operation and corresponds to the "DisplayName" element of subclause 5.2.53A in 3GPP TS 24.483 [4].

The "index" attribute is of type "token" and is included within some elements for uniqueness purposes, and does not appear in the user profile configuration managed object specified in 3GPP TS 24.483 [4].

The <Status> element is of type "Boolean" and indicates whether this particular MCPTT user profile is enabled or disabled and corresponds to the "Status" element of subclause 5.2.59 in 3GPP TS 24.483 [4]. When set to "true" this MCPTT user profile is enabled. When set to "false" this MCPTT user profile is disabled.

The "user-profile-index" is of type "unsignedByte" and indicates the particular MCPTT user profile configuration document in the collection and corresponds to the "MCPTTUserProfileIndex" element of subclause 5.2.7A in 3GPP TS 24.483 [4].

The <ProfileName> element is of type "token" and specifies the name of the MCPTT user profile configuration document in the MCPTT user profile XDM collection and corresponds to the "MCPTTUserProfileName" element of subclause 5.2.7B in 3GPP TS 24.483 [4].

The <Pre-selected-indication> element is of type "mcpttup:emptyType". Presence of the <Pre-selected-indication> element indicates that this particular MCPTT user profile is designated to be the pre-selected MCPTT user profile as defined in 3GPP TS 23.379 [8], and corresponds to the "PreSelectedIndication" element of subclause 5.2.7C in 3GPP TS 24.483 [4]. Absence of the <Pre-selected-indication> element indicates that this MCPTT user profile is not designated as the pre-selected MCPTT user profile within the collection of MCPTT user profiles for the MCPTT user or is the only MCPTT user profile within the collection and is the pre-selected MCPTT user profile by default.

The "XUI-URI" attribute is of type "anyURI" that contains the XUI of the MCPTT user for whom this MCPTT user profile configuration document is intended and does not appear in the user profile configuration managed object specified in 3GPP TS 24.483 [4].

The <ParticipantType> element of the <Common> element is of type "token" and indicates the functional category of the MCPTT user (e.g., first responder, second responder, dispatch, dispatch supervisor). The <ParticipantType> element corresponds to the "ParticipantType" element of subclause 5.2.10 in 3GPP TS 24.483 [4].

The <MaxAffiliationsN2> element is of type "nonNegativeInteger", and indicates to the MCPTT server the maximum number of MCPTT groups that the MCPTT user is authorised to affiliate with.

The <MaxSimultaneousCallsN6> element of the <MCPTT-group-call> element is of type "positiveInteger" and indicates the maximum number of simultaneously received MCPTT group calls, and corresponds to the "MaxSimultaneousCallsN6" element of subclause 5.2.31 in 3GPP TS 24.483 [4].

The <MaxSimultaneousTransmissionsN7> element is of type "positiveInteger", and indicates to the MCPTT server the maximum number of simultaneous transmissions received in one MCPTT group call for override.

The <Priority> element of the <MCPTT-group-call> element is of a type "nonNegativeInteger", indicates the priority of the MCPTT user for initiating and receiving MCPTT calls and corresponds to the "Priority" element of subclause 5.2.44 in 3GPP TS 24.483 [4].

The <User-Info-ID> element is of type "hexBinary". When the <User-Info-ID> element appears within:

- the <ProSeUserID-entry> element of the <MCPTTPrivateRecipient> of the <EmergencyCall> element indicates the ProSe "User Info ID" as defined in 3GPP TS 23.303 [18] and 3GPP TS 24.334 [19] of the recipient MCPTT user for an MCPTT emergency private call and corresponds to the "UserInfoID" element of subclause 5.2.29D in 3GPP TS 24.483 [4];
- the <PrivateCallProSeUser> element of the <PrivateCallList> element, indicates a ProSe "User Info ID" as defined in 3GPP TS 23.303 [18] and 3GPP TS 24.334 [19] of another MCPTT user that the MCPTT user is authorised to initiate a private call to and corresponds to the "UserInfoID" element of subclause 5.2.19 in 3GPP TS 24.483 [4]; and
- the <OffNetwork> element, indicates the ProSe "User Info ID" as defined in 3GPP TS 23.303 [18] and 3GPP TS 24.334 [19] of the MCPTT UE for off-network operation and corresponds to the "UserInfoID" element of subclause 5.2.58 in 3GPP TS 24.483 [4].

The "entry-info" attribute is of type "string" and when it appears within:

- the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element of the <MCPTT-group-call> element, it corresponds to the "Usage" element of subclause 5.2.34D in 3GPP TS 24.483 [4] and indicates to use as the destination address for an emergency group call:
 - a) the MCPTT user currently selected MCPTT group if the "entry-info" attribute has the value of 'UseCurrentlySelectedGroup'; or

- b) the value in the <uri-entry> element within the <entry> element of the <MCPTTGroupInitiation> element for an on-network emergency group call, if the "entry-info" attribute has the value of 'DedicatedGroup' or if the "entry-info" attribute has the value of 'UseCurrentlySelectedGroup' and the MCPTT user has no currently selected MCPTT group;
- the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element of the <PrivateCall> element, it corresponds to the "Usage" element of subclause 5.2.29F in 3GPP TS 24.483 [4] and indicates to use as the destination address for an emergency private call:
 - a) an MCPTT ID of an MCPTT user that is selected by the MCPTT user if the "entry-info" attribute has the value of 'LocallyDetermined';
 - b) the value in the <uri-entry> element within the <entry> element of the <MCPTTPrivateRecipient> for an on-network emergency private call, if the "entry-info" attribute has the value of 'UsePreConfigured'; or
 - c) the value in the <User-Info-ID> element within the <ProSeUserID-entry> element of the <MCPTTPrivateRecipient> for an off-network emergency private call, if the "entry-info" attribute has the value of 'UsePreConfigured';
- the <entry> element of the <MCPTTGroupInitiation> element of the <ImminentPerilCall> element of the <MCPTT-group-call> element, it corresponds to the "Usage" element of subclause 5.2.39D in 3GPP TS 24.483 [4] and indicates to use as the destination for the MCPTT imminent peril group call:
 - a) the MCPTT user currently selected MCPTT group if the "entry-info" attribute has the value of 'UseCurrentlySelectedGroup'; or
 - b) the value in the <uri-entry> element within the <entry> element of the <MCPTTGroupInitiation> for an on-network imminent peril call, if the "entry-info" attribute has the value of:
 - i) 'DedicatedGroup'; or
 - ii) 'UseCurrentlySelectedGroup' and the MCPTT user has no currently selected MCPTT group; and
- the <entry> element within the <EmergencyAlert> element, it corresponds to the "Usage" element of subclause 5.2.43E in 3GPP TS 24.483 [4] and indicates to use as the destination address for a group emergency alert:
 - a) the MCPTT user currently selected MCPTT group if the "entry-info" attribute has the value of 'UseCurrentlySelectedGroup';
 - b) the value in the <uri-entry> element within the <entry> element of the <EmergencyAlert> element for an on-network group emergency alert, if the "entry-info" attribute has the value of:
 - i) 'DedicatedGroup'; or
 - ii) 'UseCurrentlySelectedGroup' and the MCPTT user has no currently selected MCPTT group.
- the <entry> element within the <PrivateEmergencyAlert> element, it corresponds to the "Usage" element of subclause 5.2.48J6 in 3GPP TS 24.483 [4] and indicates to use as the destination address for on-network private emergency alert:
 - a) the MCPTT ID of an MCPTT user that is selected by the MCPTT user if the "entry-info" attribute has the value of 'LocallyDetermined'; and
 - b) the value in the <uri-entry> element within the <entry> element of the <PrivateEmergencyAlert> element, if the "entry-info" attribute has the value of:
 - i) 'UsePreConfigured'; or
 - ii) 'LocallyDetermined' and the MCPTT user has no currently selected MCPTT user.

The <allow-presence-status> element is of type Boolean, as specified in table 8.3.2.7-1, and corresponds to the "AllowedPresenceStatus" element of subclause 5.2.48E in 3GPP TS 24.483 [4].

Table 8.3.2.7-1: Values of <allow-presence-status>

"true"	indicates to the MCPTT user that their presence on the network is available.
"false"	indicates to the MCPTT user that their presence on the network is not available

The <allow-request-presence> element is of type Boolean, as specified in table 8.3.2.7-2, and corresponds to the "AllowedPresence" element of subclause 5.2.48F in 3GPP TS 24.483 [4].

Table 8.3.2.7-2: Values of <allow-request-presence>

"true"	indicates that the MCPTT user is locally authorised to request whether a particular MCPTT User is present on the network.
"false"	indicates that the MCPTT user is not locally authorised to request whether a particular MCPTT User is present on the network.

The <allow-query-availability-for-private-calls> element is of type Boolean, as specified in table 8.3.2.7-3, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-3: Values of <allow-query-availability-for-private-calls>

"true"	indicates that the MCPTT user is locally authorised to query the availability of other MCPTT users to participate in a private call.
"false"	indicates that the MCPTT user is not locally authorised to query the availability of other MCPTT users to participate in a private call.

The <allow-enable-disable-user> element is of type Boolean, as specified in table 8.3.2.7-4, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-4: Values of <allow-enable-disable-user>

"true"	indicates that the MCPTT user is locally authorised to enable/disable other MCPTT users from receiving MCPTT service.
"false"	indicates that the MCPTT user is not locally authorised to enable/disable other MCPTT users from receiving MCPTT service.

The <allow-enable-disable-UE> element is of type Boolean, as specified in table 8.3.2.7-5, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-5: Values of <allow-enable-disable-UE>

"true"	indicates that the MCPTT user is locally authorised to enable/disable other MCPTT UEs from receiving MCPTT service.
"false"	indicates that the MCPTT user is not locally authorised to enable/disable other MCPTT UEs from receiving MCPTT service.

The <allow-create-delete-user-alias> element is of type Boolean, as specified in table 8.3.2.7-6, and corresponds to the "AuthorisedAlias" element of subclause 5.2.9 in 3GPP TS 24.483 [4].

Table 8.3.2.7-6: Values of <allow-create-delete-user-alias>

"true"	indicates that the MCPTT user is locally authorised to create or delete aliases of an MCPTT user and its associated user profiles.
"false"	indicates that the MCPTT user is not locally authorised to create or delete aliases of an MCPTT user and its associated user profiles.

The <allow-private-call> element is of type Boolean, as specified in table 8.3.2.7-7, and corresponds to the "Authorised" element of subclause 5.2.13 in 3GPP TS 24.483 [4].

Table 8.3.2.7-7: Values of <allow-private-call>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call request using the procedures defined in 3GPP TS 24.379 [9]. The recipient must be a MCPTT user identified in a <entry> element of the <PrivateCall> element, which corresponds to leaf nodes of "UserList" in subclause 5.2.16 in 3GPP TS 24.483 [4].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, to reject private call request using the procedures defined in 3GPP TS 24.379 [9]. 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 8.3.2.7-8, and corresponds to the "ManualCommence" element of subclause 5.2.20 in 3GPP TS 24.483 [4].

Table 8.3.2.7-8: Values of <allow-manual-commencement>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call with manual commencement using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request a private call with manual commencement using the procedures defined in 3GPP TS 24.379 [9].

The <allow-automatic-commencement> element is of type Boolean, as specified in table 8.3.2.7-9, corresponds to the "AutoCommence" element of subclause 5.2.21 in 3GPP TS 24.483 [4].

Table 8.3.2.7-9: Values of <allow-automatic-commencement>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call with automatic commencement using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request a private call with automatic commencement using the procedures defined in 3GPP TS 24.379 [9].

The <allow-force-auto-answer> element is of type Boolean, as specified in table 8.3.2.7-10, and corresponds to the "AutoAnswer" element of subclause 5.2.22 in 3GPP TS 24.483 [4].

Table 8.3.2.7-10: Values of <allow-force-auto-answer>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call and force automatic commencement using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request a private call and force automatic commencement using the procedures defined in 3GPP TS 24.379 [9].

The <allow-failure-restriction> element is of type Boolean, as specified in table 8.3.2.7-11, and corresponds to the "FailRestrict" element of subclause 5.2.23 in 3GPP TS 24.483 [4].

Table 8.3.2.7-11: Values of <allow-failure-restriction>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to restrict the notification of a call failure reason for a private call (with or without floor control) using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to restrict the notification of a call failure reason for a private call (with or without floor control) using the procedures defined in 3GPP TS 24.379 [9].

The <allow-emergency-group-call> element is of type Boolean, as specified in table 8.3.2.7-12, and corresponds to the "Enabled" element of subclause 5.2.33 in 3GPP TS 24.483 [4].

Table 8.3.2.7-12: Values of <allow-emergency-group-call>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request an emergency group call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request an emergency group call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-emergency-private-call> element is of type Boolean, as specified in table 8.3.2.7-13, and corresponds to the "Authorised" element of subclause 5.2.27 in 3GPP TS 24.483 [4].

Table 8.3.2.7-13: Values of <allow-emergency-private-call>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request an emergency private call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request an emergency private call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-cancel-group-emergency> element is of type Boolean, as specified in table 8.3.2.7-14, and corresponds to the "CancelMCPTTGroup" element of subclause 5.2.35 in 3GPP TS 24.483 [4].

Table 8.3.2.7-14: Values of <allow-cancel-group-emergency>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to cancel an emergency group call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to cancel an emergency group call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-cancel-private-emergency-call> element is of type Boolean, as specified in table 8.3.2.7-15, and corresponds to the "CancelPriority" element of subclause 5.2.28 in 3GPP TS 24.483 [4].

Table 8.3.2.7-15: Values of <allow-cancel-private-emergency-call>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to cancel an emergency priority in an emergency private call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to cancel an emergency priority in an emergency private call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-imminent-peril-call> element is of type Boolean, as specified in table 8.3.2.7-16, and corresponds to the "Authorised" element of subclause 5.2.37 in 3GPP TS 24.483 [4].

Table 8.3.2.7-16: Values of <allow-imminent-peril-call>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request an imminent peril group call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request an imminent peril group call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-cancel-imminent-peril> element is of type Boolean, as specified in table 8.3.2.7-17, and corresponds to the "Cancel" element of subclause 5.2.38 in 3GPP TS 24.483 [4].

Table 8.3.2.7-17: Values of <allow-cancel-imminent-peril>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to cancel an imminent peril group call using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to cancel an imminent peril group call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-activate-emergency-alert> element is of type Boolean, as specified in table 8.3.2.7-18, and corresponds to the "Authorised" element of subclause 5.2.41 in 3GPP TS 24.483 [4].

Table 8.3.2.7-18: Values of <allow-activate-emergency-alert>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to activate an emergency alert using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to activate an emergency alert using the procedures defined in 3GPP TS 24.379 [9].

The <allow-cancel-emergency-alert> element is of type Boolean, as specified in table 8.3.2.7-19, and corresponds to the "Cancel" element of subclause 5.2.42 in 3GPP TS 24.483 [4].

Table 8.3.2.7-19: Values of <allow-cancel-emergency-alert>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to cancel an emergency alert using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to cancel an emergency alert using the procedures defined in 3GPP TS 24.379 [9].

The <allow-offnetwork> element is of type Boolean, as specified in table 8.3.2.7-20, and corresponds to the "Authorised" element of subclause 5.2.50 in 3GPP TS 24.483 [4].

Table 8.3.2.7-20: Values of <allow-offnetwork>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised for off-network operation using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised for off-network operation using the procedures defined in 3GPP TS 24.379 [9].

The <allow-imminent-peril-change> element is of type Boolean, as specified in table 8.3.2.7-21, and corresponds to the "ImminentPerilCallChange" element of subclause 5.2.57 in 3GPP TS 24.483 [4].

Table 8.3.2.7-21: Values of <allow-imminent-peril-change>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to change an off-network MCPTT group call in-progress to an off-network imminent peril group call using the procedures defined in 3GPP TS 24.379 [9]. The default value for the <allow-private-call-media-protection> element is "true"
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to change an off-network MCPTT group call in-progress to an off-network imminent peril group call using the procedures defined in 3GPP TS 24.379 [9].

The <allow-private-call-media-protection> element is of type Boolean, as specified in table 8.3.2.7-22, and corresponds to the "AllowedMediaProtection" element of subclause 5.2.24 in 3GPP TS 24.483 [4].

Table 8.3.2.7-22: Values of <allow-private-call-media-protection>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to protect the confidentiality and integrity of media for on-network and off-network private calls. The default value for the <allow-private-call-floor-control-protection> element is "true".
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised 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 8.3.2.7-23, and corresponds to the "AllowedFloorControlProtection" element of subclause 5.2.25 in 3GPP 24.483 [4];

Table 8.3.2.7-23: Values of <allow-private-call-floor-control-protection>

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

The <allow-request-affiliated-groups> element is of type Boolean, as specified in table 8.3.2.7-24, and does not appear in the user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-24: Values of <allow-request-affiliated-groups>

"true"	Instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request the list of MCPTT groups to which a specified MCPTT user is affiliated.
"false"	Instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request the list of MCPTT groups to which the a specified MCPTT user is affiliated.

The <allow-request-to-affiliate-other-users> element is of type Boolean, as specified in table 8.3.2.7-25, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-25: Values of <allow-request-to-affiliate-other-users>

"true"	Instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request specified MCPTT user(s) to be affiliated to/deaffiliated from specified MCPTT group(s).
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request specified MCPTT user(s) to be affiliated to/deaffiliated from specified MCPTT group(s).

The <allow-recommend-to-affiliate-other-users> element is of type Boolean, as specified in table 8.3.2.7-26, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-26: Values of <allow-recommend-to-affiliate-other-users>

"true"	Instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to recommend to specified MCPTT user(s) to affiliate to specified MCPTT group(s).
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to recommend to specified MCPTT user(s) to affiliate to specified MCPTT group(s).

The <allow-private-call-to-any-user> element is of type Boolean, as specified in table 8.3.2.7-27, and corresponds to the "AuthorisedAny" element of subclause 5.2.14 in 3GPP TS 24.483 [4].

Table 8.3.2.7-27: Values of <allow-private-call-to-any-user>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call request using the procedures defined in 3GPP TS 24.379 [9]. The recipient is not constrained to MCPTT users identified in <entry> elements of the <PrivateCall> element i.e., to any MCPTT users.
"false"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, to reject private call requests using the procedures defined in 3GPP TS 24.379 [9]. This shall be the default value taken in the absence of the element;

The <allow-regroup> element is of type Boolean, as specified in table 8.3.2.7-28, and corresponds to the "AllowedRegroup" element of subclause 5.2.48D in 3GPP TS 24.483 [4].

Table 8.3.2.7-28: Values of <allow-regroup>

"true"	instructs the MCPTT server performing the originating participating MCPTT function for the MCPTT user, that the MCPTT user is locally authorised to send a dynamic regrouping request according to the procedures defined in 3GPP TS 24.481 [5].
"false"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is not locally authorised to send a dynamic regrouping request according to the procedures defined in 3GPP TS 24.481 [5].

The <allow-private-call-participation> element is of type Boolean, as specified in table 8.3.2.7-29, and corresponds to the "EnabledParticipation" element of subclause 5.2.48G in 3GPP TS 24.483 [4].

Table 8.3.2.7-29: Values of <allow-private-call-participation>

"true"	instructs the MCPTT server performing the terminating participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to participate in private calls that they are invited to using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the terminating participating MCPTT function for the MCPTT user, that the MCPTT user to reject private call requests that they are invited to using the procedures defined in 3GPP TS 24.379 [9].

The <allow-override-of-transmission> element is of type Boolean, as specified in table 8.3.2.7-30, and corresponds to the "AllowedTransmission" element of subclause 5.2.48H in 3GPP TS 24.483 [4].

Table 8.3.2.7-30: Values of <allow-override-of-transmission>

"true"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to override transmission in a private call.
"false"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to override transmission in a private call

The <allow-manual-off-network-switch> element is of type Boolean, as specified in table 8.3.2.7-31, and corresponds to the "AllowedManualSwitch" element of subclause 5.2.48I in 3GPP TS 24.483 [4].

Table 8.3.2.7-31: Values of <allow-manual-off-network-switch>

"true"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to manually switch to off-network operation while in on-network operation using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to manually switch to off-network operation while in on-network operation using the procedures defined in 3GPP TS 24.379 [9].

The <allow-listen-both-overriding-and-overridden> element is of type Boolean, as specified in table 8.3.2.7-32, and corresponds to the "AllowedListen" element of subclause 5.2.54 in 3GPP TS 24.483 [4].

Table 8.3.2.7-32: Values of <allow-listen-both-overriding-and-overridden>

"true"	Indicates that the MCPTT user is allowed to listen both overriding and overridden transmissions during off-network operation.
"false"	Indicates that the MCPTT user is not allowed to listen both overriding and overridden transmissions during off-network operation.

The <allow-transmit-during-override> element is of type Boolean, as specified in table 8.3.2.7-33, and corresponds to the "AllowedTransmission" element of subclause 5.2.55 in 3GPP TS 24.483 [4].

Table 8.3.2.7-33: Values of <allow-transmit-during-override>

"true"	Indicates that the MCPTT user is allowed to transmit in case of override (overriding and/or overridden).during off-network operation.
"false"	Indicates that the MCPTT user is not allowed to transmit in case of override (overriding and/or overridden).during off-network operation.

The <allow-off-network-group-call-change-to-emergency> element is of type Boolean, as specified in table 8.3.2.7-34, and corresponds to the "EmergencyCallChange" element of subclause 5.2.56 in 3GPP TS 24.483 [4].

Table 8.3.2.7-34: Values of <allow-off-network-group-call-change-to-emergency>

"true"	Indicates that the MCPTT user is allowed to change an off-network group call in-progress to an off-network MCPTT emergency group call.
"false"	Indicates that the MCPTT user is not allowed to change an off-network group call in-progress to an off-network MCPTT emergency group call.

The <allow-revoke-transmit> element is of type Boolean, as specified in table 8.3.2.7-35, and does not appear in the MCPTT user profile configuration managed object specified in 3GPP TS 24.483 [4].

Table 8.3.2.7-35: Values of <allow-revoke-transmit>

"true"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is authorised to revoke the permission to transmit of another participant.
"false"	instructs the MCPTT server performing the participating MCPTT function for the MCPTT user, that the MCPTT user is not authorised to revoke the permission to transmit of another participant.

The <allow-create-group-broadcast- group> element is of type Boolean, as specified in table 8.3.2.7-36, and corresponds to the "Authorised" element of subclause 5.2.46 in 3GPP TS 24.483 [4].

Table 8.3.2.7-36: Values of <allow-create-group-broadcast- group>

"true"	indicates that the MCPTT user is locally authorised to send a request to create a group-broadcast group according to the procedures of 3GPP TS 24.481 [5].
"false"	Indicates that the MCPTT user is not locally authorised to send a request to create a group-broadcast group according to the procedures of 3GPP TS 24.481 [5].

The <allow-create-user-broadcast-group> element is of type Boolean, as specified in table 8.3.2.7-37, and corresponds to the "Authorised" element of subclause 5.2.48 in 3GPP TS 24.483 [4].

Table 8.3.2.7-37: Values of <allow-create-user-broadcast-group>

"true"	indicates that the MCPTT user is locally authorised to send a request to create a user-broadcast group according to the procedures of 3GPP TS 24.481 [5].
"false"	Indicates that the MCPTT user is not locally authorised to send a request to create a user-broadcast group according to the procedures of 3GPP TS 24.481 [5].

The <allow-request-private-call-call-back> element is of type Boolean, as specified in table 7.4.2.7-38, and corresponds to the "AllowedCallBackRequest" element of subclause 5.2.48P in 3GPP TS 24.483 [4].

Table 7.4.2.7-38: Values of <allow-request-private-call-call-back>

"true"	instructs the MCPTT server performing the controlling MCPTT function for the MCPTT user, that the MCPTT user is authorised to request a private call call-back using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the controlling MCPTT function for the MCPTT user, that the MCPTT user is not authorised to request a private call call-back using the procedures defined in 3GPP TS 24.379 [9].

The <allow-cancel-private-call-call-back > element is of type Boolean, as specified in table 7.4.2.7-39, and corresponds to the "AllowedCallBackCancelRequest" element of subclause 5.2.48Q in 3GPP TS 24.483 [4].

Table 7.4.2.7-39: Values of <allow-cancel-private-call-call-back>

"true"	instructs the MCPTT server performing the controlling MCPTT function for the MCPTT user, that the MCPTT user is authorised to cancel a private call call-back cancel using the procedures defined in 3GPP TS 24.379 [9].
"false"	instructs the MCPTT server performing the controlling MCPTT function for the MCPTT user, that the MCPTT user is not authorised to cancel a private call call-back using the procedures defined in 3GPP TS 24.379 [9].

8.3.2.8 Naming Conventions

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

8.3.2.9 Global documents

The present document requires no global documents.

8.3.2.10 Resource interdependencies

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

8.3.2.11 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*".

8.3.2.12 Subscription to Changes

The User Access Policy Application Usage shall support subscription to changes as specified in subclause 6.3.13.3.

MCPTT user profile configuration documents are kept as XDM collections. Therefore, it is possible to subscribe to all MCPTT user profile configuration documents of a MCPTT user according to XCAP URI construction convention of a trailing '/', as specified in IETF RFC 5875 [11].

8.4 MCPTT service configuration document

8.4.1 General

The MCPTT service configuration document is specified in this subclause. The MCPTT service configuration document content is based on requirements of Annex A.5 of 3GPP TS 23.379 [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 8.4.2.3. Each mission critical organization is configured with an MCPTT service configuration document.

8.4.2 Coding

8.4.2.1 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 a <min-length-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;
- 8) may contain a <signalling-protection> element containing:
- a) a <confidentiality-protection> element; and
 - b) an <integrity-protection> element;
- 9) shall include one <emergency-resource-priority> element containing:
- a) one <resource-priority-namespace> string element containing a namespace defined in draft-holmberg-dispatch-mcptt-rp-namespace [20]; and
 - b) one <resource-priority-priority> string element element containing a priority level in the range specified in draft-holmberg-dispatch-mcptt-rp-namespace [20];
- 10) shall include one <imminent-peril-resource-priority> element containing:
- a) one <resource-priority-namespace> string element containing a namespace defined in draft-holmberg-dispatch-mcptt-rp-namespace [20]; and
 - b) one <resource-priority-priority> string element element containing a priority level in the range specified in draft-holmberg-dispatch-mcptt-rp-namespace [20];
- 11) shall include one <normal-resource-priority> element containing:
- a) one <resource-priority-namespace> string element containing a namespace defined in draft-holmberg-dispatch-mcptt-rp-namespace [20]; and

- b) one <resource-priority-priority> string element element containing a priority level in the range specified in draft-holmberg-dispatch-mcptt-rp-namespace [20]; and

12) may contain a <protection-between-mcptt-servers> element containing:

- a) an <allow-signalling-protection> element; and
- b) an <allow-floor-control-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.

8.4.2.2 Application Unique ID

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

8.4.2.3 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:sequence>
  </xs:complexType>
</xs:schema>
```

```

    <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="min-length-alias" type="xs:unsignedShort" 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="mcpttsc:priorityhierarchyType"
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"/>
    <xs:element name="signalling-protection" type="mcpttsc:signalling-protectionType"
minOccurs="0"/>
    <xs:element name="protection-between-mcptt-servers" type="mcpttsc:server-protectionType"
minOccurs="0"/>
    <xs:element name="emergency-resource-priority" type="mcpttsc:resource-priorityType"/>
    <xs:element name="imminent-peril-resource-priority" type="mcpttsc:resource-priorityType"/>
    <xs:element name="normal-resource-priority" type="mcpttsc:resource-priorityType"/>
    <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="mcpttsc:priorityhierarchyType"
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="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"/>
    <xs:element name="T3-stop-talking-grace" type="xs:duration"/>
    <xs:element name="T7-floor-idle" type="xs:duration"/>
    <xs:element name="T8-floor-revoke" type="xs:duration"/>
    <xs:element name="T11-end-of-RTP-dual" type="xs:duration"/>
    <xs:element name="T12-stop-talking-dual" type="xs:duration"/>
    <xs:element name="T15-conversation" type="xs:duration"/>
    <xs:element name="T16-map-group-to-bearer" type="xs:duration"/>
    <xs:element name="T17-unmap-group-to-bearer" type="xs:duration"/>
    <xs:element name="T20-floor-granted" type="xs:duration"/>
    <xs:element name="T55-connect" type="xs:duration"/>
    <xs:element name="T56-disconnect" type="xs:duration"/>
    <xs:element name="C7-floor-idle" type="xs:unsignedShort"/>
    <xs:element name="C17-unmap-group-to-bearer" type="xs:unsignedShort"/>
    <xs:element name="C20-floor-granted" type="xs:unsignedShort"/>
    <xs:element name="C55-connect" type="xs:unsignedShort"/>
    <xs:element name="C56-disconnect" type="xs:unsignedShort"/>
    <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="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="server-protectionType">
  <xs:sequence>
    <xs:element name="allow-signalling-protection" type="xs:boolean" minOccurs="0"
default="true"/>
    <xs:element name="allow-floor-control-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="resource-priorityType">
  <xs:sequence>
    <xs:element name="resource-priority-namespace" type="xs:string"/>
    <xs:element name="resource-priority-priority" type="xs:string"/>
    <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>

<!-- simple type for priority element -->
<xs:simpleType name="priorityhierarchyType">
  <xs:restriction base="xs:unsignedShort">
    <xs:minInclusive value="4"/>
    <xs:maxInclusive value="256"/>
  </xs:restriction>
</xs:simpleType>

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

```

8.4.2.4 Default Document Namespace

The default document namespace used in evaluating URIs shall be "urn:3gpp:ns:mcpttServiceConfig:1.0".

8.4.2.5 MIME type

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

8.4.2.6 Validation Constraints

If the AUID value of the document URI or node URI in the Request-URI is other than that specified in subclause 8.4.2.2, 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 8.4.2.3.

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 <min-length-alias> element in the <common> element refers to variable N3 defined in Annex A of 3GPP TS 22.179 [3] and contains a value between 0 and 255.

If the <min-length-alias> element of the <common> element contains a value greater than 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 "element value out of range".

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 <min-length-alias>, 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 <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 2: The higher the <default-prose-per-packet-priority> value, the higher the priority given to the signalling or media.

The "resource-priority-namespace" element contained in the "emergency-resource-priority" element shall have an MCPTT namespace value as specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The "resource-priority-priority" element contained in the "emergency-resource-priority" element shall have a value greater than or equal to the value of the "resource-priority-priority" element contained in the "imminent-peril-resource-priority" element and shall be a priority level specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The "resource-priority-namespace" element contained in the "imminent-peril-resource-priority" element shall have an MCPTT namespace value as specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The "resource-priority-priority" element contained in the "imminent-peril-resource-priority" element shall have a value greater than or equal to the value of the "resource-priority-priority" element contained in the "normal-resource-priority" element and shall be a priority level specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The "resource-priority-namespace" element contained in the "normal-resource-priority" element shall have an MCPTT namespace value as specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The "resource-priority-priority" element contained in the "normal-resource-priority" element shall have a value that is a priority level specified in draft-holmberg-dispatch-mcptt-rp-namespace [20].

The values used for the "emergency-resource-priority", "imminent-peril-resource-priority" and "normal-resource-priority" elements need to be carefully agreed to by the MCPTT operator and network operator.

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 3: "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".

8.4.2.7 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 <min-length-alias> element contains the minimum length (N3) of alphanumeric names assigned to MCPTT users by the MCPTT administrator, which corresponds to the "MinLengthAliasID" element as specified in subclause 7.2.9 of 3GPP TS 24.483 [4];
- 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, which corresponds to the "NumLevelGroupHierarchy" element as specified in subclause 7.2.7 of 3GPP TS 24.483 [4]; 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, which corresponds to the "NumLevelUserHierarchy" element as specified in subclause 7.2.8 of 3GPP TS 24.483 [4];

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 1: 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. Absence of the <num-levels-priority-hierarchy> element in the <on-network> element indicates that the lowest possible value is used according to the schema, to represent the priority hierarchy;

NOTE 2: The higher the value from the priority hierarchy assigned to a participant, the higher the priority given to override an active 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;
- 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 of the <fc-timers-counters> element 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 of the <fc-timers-counters> element contains the retransmission interval of the Map Group To Bearer message;
- 20) the <T17-unmap-group-to-bearer> element of the <fc-timers-counters> 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 of the <fc-timers-counters> 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 of the <fc-timers-counters> 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 of the <fc-timers-counters> 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 of the <fc-timers-counters> element contains the maximum number of times the Connect message is retransmitted;
- 28) the <C56-disconnect> element of the <fc-timers-counters> 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 between the MCPTT client and MCPTT server;
- 30) the <integrity-protection> element of the <signalling-protection> element contains a boolean indicating whether integrity protection of MCPTT signalling is enabled or disabled between the MCPTT client and MCPTT server;
- 31) The <emergency-resource-priority> element is of type "resource-priorityType" and indicates how a Resource-Priority header field is to be populated for MCPTT emergency calls;
- 32) The <imminent-peril-resource-priority> element is of type "resource-priorityType" and indicates how a Resource-Priority header field is to be populated for MCPTT Imminent Peril calls;
- 33) The <normal-resource-priority> element is of type "resource-priorityType" and indicates how a Resource-Priority header field is to be populated when downgrading to normal priority from an MCPTT emergency call or MCPTT imminent peril call;
- 34) the <allow-signalling-protection> element of the <protection-between-mcptt-servers> element contains a boolean indicating whether protection of MCPTT signalling is enabled between MCPTT servers; and
- 35) the <allow-floor-control-protection> element of the <protection-between-mcptt-servers> element contains a boolean indicating whether protection of MCPTT floor control signalling is enabled between MCPTT servers.

NOTE 3: The default values of the <confidentiality-protection> element, the <integrity-protection> element, the <allow-signalling-protection> element and the <allow-floor-control-protection> element are "true".

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, which corresponds to the "CancelTimeout" element as specified in subclause 7.2.14 of 3GPP TS 24.483 [4];
- 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, which corresponds to the "MCPTTGroupTimeout" element as specified in subclause 7.2.16 of 3GPP TS 24.483 [4];
- 3) the <hang-time> element of the <private-call> element contains the value of the hang timer for off-network private calls, which corresponds to the "HangTime" element as specified in subclause 7.2.13 of 3GPP TS 24.483 [4];
- 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, which and corresponds to the "MaxDuration" element as specified in subclause 7.2.12 of 3GPP TS 24.483 [4];
- 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, which corresponds to the "NumLevelHierarchy" element as specified in subclause 7.2.17 of 3GPP TS 24.483 [4]. Absence of the <num-levels-priority-hierarchy> element in the <off-network> element indicates that the lowest possible value is used according to the schema to represent the priority hierarchy;

NOTE 4: The higher the value from the priority hierarchy assigned to a participant, the higher the priority given to override an active 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, which corresponds to the "TransmitTimeout" element as specified in subclause 7.2.18 of 3GPP TS 24.483 [4];
- 7) the <time-warning> element of the <transmit-time> element contains the warning time before the off-network transmit time is reached, which corresponds to the "TransmissionWarning" element as specified in subclause 7.2.19 of 3GPP TS 24.483 [4];
- 8) the <hang-time-warning> element contains the warning time before the off-network hang time is reached, which corresponds to the "HangTimeWarning" element as specified in subclause 7.2.20 of 3GPP TS 24.483 [4];
- 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 which corresponds to the "MCPTTPrivateCallSignalling" element as specified in subclause 7.2.22 of 3GPP TS 24.483 [4];
 - b) mcptt private call media which corresponds to the "MCPTTPrivateCallMedia" element as specified in subclause 7.2.23 of 3GPP TS 24.483 [4];
 - c) mcptt emergency private call signalling which corresponds to the "MCPTTEmergencyPrivateCallSignalling" element as specified in subclause 7.2.24 of 3GPP TS 24.483 [4]; and
 - d) mcptt emergency private call media which corresponds to the "MCPTTEmergencyPrivateCallMedia" element as specified in subclause 7.2.25 of 3GPP TS 24.483 [4]; and
- 10) the <allow-log-metadata> element which corresponds to the "LogMetadata" element as specified in subclause 7.2.26 of 3GPP TS 24.483 [4] and 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.

8.4.2.8 Naming Conventions

The present document defines no naming conventions.

8.4.2.9 Global documents

The present document requires no global documents.

8.4.2.10 Resource interdependencies

There are no resource interdependencies.

8.4.2.11 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*".

8.4.2.12 Subscription to Changes

The service configuration document application usage shall support subscription to changes as specified in subclause 6.3.13.3.

9 MCVideo configuration management documents

Editor's Note: [C1-170137, MCImp-MCVIDEO-CT] Text for MCVideo is FFS.

10 MCDATA configuration management documents

Editor's Note: [C1-170137, MCImp-MCDATA-CT] Text for MCDATA is FFS.

Annex A (informative): Signalling flows

No signaling flows are provided in the present document.

Annex B (informative): IANA registration templates

B.1 IANA registration templates for MIME types

B.1.1 application/vnd.3gpp.mcptt-ue-init-config+xml IANA registration template

Editor's note: The MIME type is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

application

Subtype name:

vnd.3gpp.mcptt-ue-init-config+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.484 "Mission Critical Services (MCS) configuration management; Protocol specification" version 13.3.0, available via <http://www.3gpp.org/specs/numbering.htm>.

Applications which use this media type:

Applications supporting the MCPTT UE initial configuration document as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
 - i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
 - ii) Change controller: <MCC name>/<MCC email address>

B.1.2 application/vnd.3gpp.mcptt-ue-config+xml IANA registration template

Editor's note: The MIME type is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

application

Subtype name:

vnd.3gpp.mcptt-ue-config+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.484 "Mission Critical Services (MCS) configuration management; Protocol specification" version 13.3.0, available via <http://www.3gpp.org/specs/numbering.htm>.

Applications which use this media type:

Applications supporting the MCPTT UE configuration document as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none

4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
 - i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
 - ii) Change controller: <MCC name>/<MCC email address>

B.1.3 application/vnd.3gpp.mcptt-user-profile+xml IANA registration template

Editor's note: The MIME type is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

application

Subtype name:

vnd.3gpp.mcptt-user-profile+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.484 "Mission Critical Services (MCS) configuration management; Protocol specification" version 13.3.0, available via <http://www.3gpp.org/specs/numbering.htm>.

Applications which use this media type:

Applications supporting the MCPTT user profile configuration document as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
 - i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
 - ii) Change controller: <MCC name>/<MCC email address>

B.1.4 application/vnd.3gpp.mcptt-service-config+xml IANA registration template

Editor's note: The MIME type is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

application

Subtype name:

vnd.3gpp.mcptt-service-config+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.484 "Mission Critical Services (MCS) configuration management; Protocol specification" version 13.3.0, available via <http://www.3gpp.org/specs/numbering.htm>.

Applications which use this media type:

Applications supporting the MCPTT service configuration document as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
 - i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
 - ii) Change controller: <MCC name>/<MCC email address>

Annex C (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
2016-06	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

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2016-09	CT-73	CP-160564	0015	6	F	User Profile schema definition	13.2.0
2016-09	CT-73	CP-160566	0020	8	F	MCPTT UE ID in UE Initial Configuration and UE configuration documents	13.2.0
2016-09	CT-73	CP-160472	0025	3	F	Resource-Priority header field configuration for MCPTT	13.2.0
2016-09	CT-73	CP-160504	0026		F	Configuring the default user profile	13.2.0
2016-09	CT-73	CP-160504	0027		F	Service configuration document missing corresponding pointers to service configuration MO in TS 24.383	13.2.0
2016-09	CT-73	CP-160504	0028	1	F	Service Config has incorrect specification of "alias" parameter	13.2.0
2016-09	CT-73	CP-160504	0029		F	Service Config missing signalling and floor-control protection configuration between MCPTT servers	13.2.0
2016-09	CT-73	CP-160567	0030	4	F	Additional MCPTT UE initial configuration document elements	13.2.0
2016-09	CT-73	CP-160568	0031	4	F	Alignment of MCPTT UE configuration document with TS 23.179 and TS 24.383	13.2.0
2016-09	CT-73	CP-160504	0032	1	F	Default document namespace correction	13.2.0
2016-09	CT-73	CP-160504	0033	1	F	Completion of CMC, CMS and MCPTT server procedures	13.2.0
2016-09	CT-73	CP-160504	0034	2	F	Correction for the corresponding pointers to MCPTT management objects (MOs) in TS 24.383	13.2.0
2016-09	CT-73	CP-160499	0035	1	F	Addition of Mission Critical Organization to the user profile	13.2.0
2016-10	CT-73					Correct misimplementation of CR0030	24.384 13.2.1
2016-12	CT#74					Change of spec number from 24.384 to 24.484 with wider scope and changed title	24.484 13.2.2
2016-12	CT-74	CP-160734	0039	4	F	Essential corrections required to the user profile definition (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0040	3	F	Service Config validations for <num-levels-priority-hierarchy> are incorrect (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0041	1	F	Identity management endpoint UE initial configuration correction (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0043	1	F	Reference update draft-holmberg-dispatch-mcptt-rp-namespace (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0044	1	F	Correction of validation of VPLMN element (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0045	1	F	Identification of pre-selected MCPTT user profile (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0046		F	Fix the MCPTT UE profile schema (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0047		F	Fix the MCPTT initial UE profile schema (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0048	3	F	Reuse of OMA-TS-XDM_Core (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160734	0049		F	Resolve Editor's Note regarding signaling flows (CR to 24.384)	13.3.0
2016-12	CT-74	CP-160743	0050		F	Correction of the semantics description (CR to 24.384)	14.0.0
2017-03	CT-75	CP-170125	0002	1	B	Scope enhancement for MCVideo and MCdata	14.1.0
2017-03	CT-75	CP-170117	0003		A	Correction of implementation errors	14.1.0
2017-03	CT-75	CP-170125	0004		F	Correct references for release 14	14.1.0
2017-03	CT-75	CP-170125	0005	2	B	Restructure TS 24.484 for MCVideo and MCdata	14.1.0
2017-03	CT-75	CP-170117	0007	1	A	Reference update draft-holmberg-dispatch-mcptt-rp-namespace	14.1.0
2017-03	CT-75	CP-170117	0009		A	Syntax error in Servconf.xsd on element max-duration-with-floor-control	14.1.0
2017-03	CT-75	CP-170117	0014	2	A	Corrections to upper limits	14.1.0
2017-03	CT-75	CP-170125	0015	1	B	Modifications to the MCPTT user profile for private call call-back	14.1.0
2017-03	CT-75	CP-170236	0011	3	A	Issues with MCPTT user profile	14.1.0
2017-03	CT-75	C1-170189	0017		A	Registration forms for MIME types defined by TS 24.484 are missing	14.1.0

History

Document history		
V14.1.0	April 2017	Publication