ETSI TS 124 282 V16.6.0 (2021-01)

LTE;
Mission Critical Data (MCData) signalling control;
Protocol specification
(3GPP TS 24.282 version 16.6.0 Release 16)

Reference
RTS/TSGC-0124282vg60

Keywords
LTE

ETSI

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

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

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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the signalling control protocols needed to support Mission Critical Data (MCData) communications as specified by 3GPP TS 23.282 [2]. The present document specifies both on-network and off-network protocols.

The present document utilises the common functional architecture to support mission critical services as specified in 3GPP TS 23.280 [3], in support of MCData communications.

The MCData service can be used for public safety applications and also for general commercial applications e.g. utility companies and railways.

The present document is applicable to User Equipment (UE) supporting the MCData client functionality, and to application servers supporting the 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] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2";

[3] 3GPP TS 23.280:" Common functional architecture to support mission critical services; Stage 2";

[4] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[5] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[6] IETF RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[7] IETF RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[8] IETF RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)".

[9] IETF RFC 4826 (May 2007): "Extensible Markup Language (XML) Formats for Representing Resource Lists".

[10] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification".

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

[12] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management Protocol specification".

[13] IETF RFC 4483 (May 2006): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.

[14] IETF RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[15] 3GPP TS 24.582: "Mission Critical Data (MCData) media plane control Protocol specification";

[16] IETF RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[17] IETF RFC 4975 (September 2007): "The Message Session Relay Protocol (MSRP)".

[18] IETF RFC 5366 (October 2008): "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)".

[19] IETF RFC 6135 (February 2011): "An Alternative Connection Model for the Message Session Relay Protocol (MSRP) ".

[20] IETF RFC 6714 (August 2012): "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[21] IETF RFC 6086 (January 2011): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

[22] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[23] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[24] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management Protocol specification.

[25] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to Proximity-services (ProSe) Function Protocol aspects; Stage 3".

[26] 3GPP TS 33.180: "Security of the Mission Critical Service".

[27] void

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

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

[30] IETF RFC 4648 (October 2006): "The Base16, Base32, and Base64 Data Encodings".

[31] 3GPP TS 23.003: "Numbering, addressing and identification".

[32] IETF RFC 2045 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[33] IETF RFC 2392 (August 1998): "Content-ID and Message-ID Uniform Resource Locators".

[34] IETF RFC 3903 (October 2004): "Session Initiation Protocol (SIP) Extension for Event State Publication".

[35] IETF RFC 4354 (January 2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".

[36] IETF RFC 6665 (July 2012): "SIP-Specific Event Notification".

[37] 3GPP TS 29.283: "Diameter Data Management Applications".

[38] IETF RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

[39] IETF RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[40] IETF RFC 3863 (August 2004): "Presence Information Data Format (PIDF)".

[41] IETF RFC 4661 (September 2006): "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering".

[42] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[43] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[44] IETF RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[45] IETF RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".

[46] IETF RFC 3986 (January 2005): "Uniform Resource Identifier (URI): Generic Syntax".

[47] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[48] 3GPP TS 29.582: "Mission Critical Data (MCData) signalling control interworking with LMR systems; Protocol specification".

[49] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[50] IETF RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer Answer Protocols".

[51] IETF RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) Refer Method".

[52] IETF RFC 7647 (September 2015): "Clarifications for the use of REFER with RFC6665".

[53] IETF RFC 4488 (May 2006): "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription".

[54] IETF RFC 4538 (June 2006): "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)".

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

[56] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[57] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point; Stage 3".

[58] Void.

[59] IETF RFC 5761 (April 2010): "Multiplexing RTP Data and Control Packets on a Single Port".

[60] IETF RFC 5795 (March 2010): "The RObust Header Compression (ROHC) Framework".

[61] IETF RFC 3095 (July 2001): "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed".

[62] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[63] 3GPP TS 23.203: "Policy and charging control architecture".

[64] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[65] 3GPP TS 29.199-09: "Open Service Access (OSA); Parlay X web services; Part 9: Terminal location".

[66] OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C: "RESTful Network API for Network Message Storage".

[67] IETF RFC 8101 (March 2017): "IANA Registration of New Session Initiation Protocol (SIP) Resource-Priority Namespace for Mission Critical Push To Talk Service".

[68] 3GPP TS 22.280: "Mission Critical Services Common Requirements (MCCoRe); Stage 1".

[69] IETF RFC 5547: "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer".

[70] IETF RFC 1738: "Uniform Resource Locators (URL)".

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

[72] IETF RFC 5888 (June 2010): "The Session Description Protocol (SDP) Grouping Framework".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

An MCData user is affiliated to an MCData group: The MCData user has expressed interest in an MCData group it is a member of, and both the MCData server serving the MCData user and the MCData server owning the MCData group have authorized the MCData user's interest in the MCData group communication.

An MCData user is affiliated to an MCData group at an MCData client: The MCData user is affiliated to the MCData group, the MCData client has a registered IP address for an IMPU related to the MCData ID, and the MCData server serving the MCData user has authorised the MCData user's interest in the MCData group at the MCData client.

Affiliation status: Applies for an MCData user to an MCData group and has one of the following states:

a) the "not-affiliated" state indicating that the MCData user is not interested in the MCData group and the MCData user is not affiliated to the MCData group;

b) the "affiliating" state indicating that the MCData user is interested in the MCData group but the MCData user is not affiliated to the MCData group yet;

c) the "affiliated" state indicating that the MCData user is affiliated to the MCData group and there was no indication that MCData user is no longer interested in the MCData group; and

d) the "deaffiliating" state indicating that the MCData user is no longer interested in the MCData group but the MCData user is still affiliated to the MCData group.

Group identity: An MCData group identity or a temporary MCData group identity.

MCData client ID: is a globally unique identification of a specific MCData client instance. MCData client ID is a UUID URN as specified in IETF RFC 4122 [14].

MCData emergency alert: A notification from the MCData client to the MCData service that the MCData user has an emergency condition.

MCData emergency alert state: MCData client internal perspective of the state of an MCData emergency alert.

MCData emergency group state: MCData client internal perspective of the in-progress emergency state of an MCData group maintained by the controlling MCData function.

MCData emergency group communication: An urgent MCData group communication that highlights a situation of potential death or serious injury.

MCData emergency group communication state: MCData client internal perspective of the state of an MCData emergency group communication.

Functional alias status: Applies for the status of a functional alias for an MCData user and has one of the following states:

a) the "not-activated" state indicating that the MCData user has not activated the functional alias;

b) the "activating" state indicating that the MCData user is interested in using the functional alias but the functional alias is not yet activated for the MCData user;

c) the "activated" state indicating that the MCData user has activated the functional alias; and

d) the "deactivating" state indicating that the MCData user is no longer interested in using the functional alias but the functional alias is still activated for the MCData user.

For the purpose of the present document, the following terms and definitions given in 3GPP TS 33.180 [26] apply:

Client Server Key (CSK)
Multicast Signalling Key (MuSiK)
Multicast Signalling Key Identifier (MuSiK-ID)
MBMS subchannel control key (MSCCK)
MBMS subchannel control key identifier (MSCCK-ID)
Private Call Key (PCK)
Signalling Protection Key (SPK)
XML Protection Key (XPK)

For the purpose of the present document, the following terms and definitions given in 3GPP TS 22.280 [68] apply:

Functional alias

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].

CSK	Client-Server Key
IMPU	P Multimedia Public User identity
MBMS	Multimedia Broadcast and Multicast Service
MC	Mission Critical
MCS	Mission Critical Service
MCData	Mission Critical Data
MCData group ID	MCData group Identity
MDEA	MCData Emergency Alert
MDEG	MCData Emergency Group
MDEGC	MCData Emergency Group Communication
MDES	MCData Emergency State
MIME	Multipurpose Internet Mail Extensions
MONP	MC service Off-Network Protocol
QCI	QoS Class Identifier
RTP	Real-time Transport Protocol
SAI	Service Area Identifier
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPK	Signalling Protection Key
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UUID	Universally Unique IDentifier
XPK	XML Protection Key

4 General

4.1 MCData overview

The MCData service supports communication between a pair of users (i.e. one-to-one communication) and several users (i.e. group communication), where each user has the ability to:

- share data using Short Data Service (SDS);
- share files using File Distribution (FD) service; and
- exchange Data using IP Connectivity service.

SDS is provided in both, on-network and off-network while FD and IP Connectivity is provided only in on-network in this release of the present document.

The present document provides the signalling control protocol enhancements to support the MCData architectural procedures specified in 3GPP TS 23.282 [2].

For on-network communications, the present document makes use of the existing IMS procedures specified in 3GPP TS 24.229 [5].

The on-network procedures in this document allow an MCData user to:

- send a standalone SDS using signalling control plane;
- send a standalone SDS using media plane;
- initiate a SDS session;
- send a file using HTTP;
- send a file using media plane;
- establish an IP Connectivity session to exchange Data;
- access the MCData message store; and
- use a functional alias to identify the MCData user.

For off-network, the present document utilises the procedures for ProSe direct discovery for Public Ssafety and the procedures for one-to-one ProSe direct communication for Public Safety and one-to-many ProSe direct communication for Public Safety, as specified in 3GPP TS 24.334 [25], and allows an MCData user to:

- send a standalone SDS using signalling control plane.

The MCData procedures provided by the present document refer to:

- the media plane procedures defined in 3GPP TS 24.582 [15];
- the group management procedures defined in 3GPP TS 24.481 [11];
- the identity management procedures defined in 3GPP TS 24.482 [24]; and
- the security procedures defined in 3GPP TS 33.180 [26].

The MCData procedures provided by the present document access the configuration parameters provided by 3GPP TS 24.483 [42] and 3GPP TS 24.484 [12].

The following procedures are provided within this document:

- common procedures are specified in clause 6;
- procedures for registration in the IM CN subsystem and service authorisation are specified in clause 7;
- procedures for affiliation are specified in clause 8;
- procedures for on-network and off-network SDS are specified in clause 9;
- procedures for on-network FD are specified in clause 10;
- procedures for transmission and reception control are specified in clause 11;
- procedures for dispositions and notifications are specified in clause 12;

- procedures for communication release are specified in clause 13;
- procedures for location reporting are specified in clause 17;
- procedure for using MBMS transmission are specified in clause 19;
- procedures for establishing an IP Connectivity session are specified in clause 20;
- procedures for the MCData message store are specified in clause 21; and
- procedures for the use of functional alias are specified in clause 22.

The MCData UE primarily obtains access to the MCData service via E-UTRAN, using the procedures defined in 3GPP TS 24.301 [43].

4.2 Identity, URI and address assignments

4.2.1 Public Service identities

In order to support MCData, the following URI and address assignments are assumed:

1) the participating MCData function is configured to be reachable using:
   a) the public service identity of the participating MCData function serving the MCData user.

4.2.2 MCData session identity

The MCData session identity is a SIP URI, which identifies the MCData session between:

- the MCData client and the participating MCData function; and
- the participating MCData function and the controlling MCData function.

The MCData session identity shall be a GRUU as defined in IETF RFC 5627 [44] assigned by the MCData server as per 3GPP TS 24.229 [5].

The MCData session identity identifies the MCData session in such a way that e.g.:

- the IM CN subsystem is able to route an initial SIP request to the controlling MCData function.

The controlling MCData function allocates a unique MCData session identity hosted at the controlling MCData function for the MCData session at the time of session establishment.

When protection of sensitive application data is required by the MCData operator, the MCData session identity cannot contain identity information that is classified as sensitive such as the MCData ID or the MCData Group ID, as specified in subclause 4.6.

The controlling MCData function sends the MCData session identity towards the MCData client during MCData session establishment by including it in the Contact header field of the final SIP response to a session initiation request.

The participating MCData function allocates a unique MCData session identity hosted at the participating MCData function for the MCData session when it receives a MCData session identity in the Contact header field of a SIP request or a SIP response from the controlling MCData function and includes it in the Contact header field of the SIP request or SIP response sent towards the MCData client. The participating MCData function maintains a mapping of the MCData session identities it sends to the MCData client to the corresponding MCData session identities received from the controlling MCData function.

The MCData client can cache the MCData session identity until a time when it is no longer needed.

4.2.3 MCData client ID

MCData client ID is described in subclause 4.8 of the present document.

4.3 Pre-established sessions

When establishing a pre-established session, the MCData client negotiates the media parameters, including establishing IP addresses and ports using interactive connectivity establishment (ICE) as specified in IETF RFC 5245 [50] with the participating MCData function, prior to using the pre-established session for establishing MCData communication with other MCData users. The procedures for establishing, modifying and releasing a pre-established session are defined in clause 18.

The pre-established session can later be used in MCData communication. This avoids the need to negotiate media parameters (including evaluating ICE candidates) and reserving bearer resources during the MCData communication establishment that results in delayed MCData communication establishment.

4.4 Emergency Alerts

MCData emergency alerts can be initiated or cancelled as described in the procedures of clause 16 which include:

- MCData emergency alert initiation, on-network;
- MCData emergency alert cancellation, on-network;
- MCData emergency alert initiation, off-network; and
- MCData emergency alert cancellation, off-network.

MCData emergency alerts are initiated to a target MCData group, and, if successful and not already affiliated to that group, will result in the initiator being implicitly affiliated to that MCData group.

Key aspects of MCData emergency alerts include:

- **MCData emergency alert (MDEA) state:** the MCData client maintains the internal MCData emergency alert state (MDEA, see subclause G.4.1). The initial setting is "MDEA 1: no-alert".
- **Authorisations for emergency alerts:** MCData users need to be authorised to initiate MCData emergency alerts and additionally need to be authorised to cancel MCData emergency alerts initiated by them or by others. The parameters related to these authorisations are specified in 3GPP TS 24.483 [42] and 3GPP TS 24.484 [12].

4.5 MCData Protocol

Subclauses 15 describes the TLV based message formats used in MCData communications. Each message consist of a series of information elements. Annex I of 3GPP TS 24.379 [10] describes the standard format of the messages and the encoding rules for each type of information element.

4.6 Protection of sensitive XML application data

In certain deployments, for example, in the case that the MCData operator uses the underlying SIP core infrastructure from the carrier operator, the MCData operator can prevent certain sensitive application data from being visible in the clear to the SIP layer. The following data are classed as sensitive application data:

- MCData ID;
- MCData group ID;
- user location information;
- alert indicator;
- access token (containing the MCData ID);
- MCData client ID; and
- functional alias.

The above data is transported as XML content in SIP messages. in XML elements or XML attributes.

Data is transported in attributes in the following circumstances in the procedures in the present document:

- an MCData ID, an MCData Group ID, and an MCData client ID in an XML document published in SIP PUBLISH request for affiliation according to IETF RFC 3856 [39];
- an MCData ID or an MCData Group ID in XML document notified in a SIP NOTIFY request for affiliation according to IETF RFC 3856 [39];
- an MCData ID in application/resource-lists+xml document included in a SIP MESSAGE or SIP INVITE request for one-to-one SDS or one-to-one FD, according to IETF RFC 5366 [18];
- an MCData ID and functional alias in an XML document published in SIP PUBLISH request for functional alias management according to IETF RFC 3856 [39]; and
- an MCData ID and functional alias in an XML document notified in a SIP NOTIFY request for functional alias management according to IETF RFC 3856 [39].

3GPP TS 33.180 [26] describes a method to provide confidentiality protection of sensitive application data in elements by using XML encryption (i.e. xmlenc) and in attributes by using an attribute confidentiality protection scheme described in subclause 6.6.2.3 of the present document. Integrity protection can also be provided by using XML signatures (i.e. xmlsig).

Protection of the data relies on a shared XML protection key (XPK) used to encrypt and sign data:

- between the MCData client and the MCData server, the XPK is a client-server key (CSK); and
- between MCData servers, the XPK is a signalling protection key (SPK).

The CSK (XPK) and a key-id CSK-ID (XPK-ID) are generated from keying material provided by the key management server. Identity based public key encryption based on MIKEY-SAKKE is used to transport the CSK between SIP end-points. The encrypted CSK is transported from the MCData client to the MCData server when the MCData client performs service authorisation as described in clause 7 and is also used during service authorisation to protect the access token.

The SPK (XPK) and a key-id SPK-ID (XPK-ID) are directly provisioned in the MCData servers.

Configuration in the MCData client and MCData server is used to determine whether one or both of confidentiality protection and integrity protection are required.

The following four examples give a brief overview of the how confidentiality and integrity protection is applied to application data in this specification.

EXAMPLE 1: Pseudo code showing how confidentiality protection is represented in the procedures in the document for sensitive data sent by the originating client.

```
IF configuration is set for confidentiality protection of sensitive data
THEN
    Encrypt data element using the CSK (XPK;
    Include in an <EncryptedData> element of the XML MIME body:
      (1) the encryption method;
      (2) the key-id (XPK-ID);
      (3) the cipher data;
    Encrypt URIs in attribute using the CSK (XPK) by following subclause 6.6.2.3;
ELSE
    include application data into XML MIME body in clear text;
ENDIF;
```

EXAMPLE 2: Pseudo code showing how integrity protection is represented in the procedures in the present document for data sent by the originating client.

```
IF configuration is set for integrity protection of application data
THEN
    Use a method to hash the content;
    Generate a signature for the hashed content using the CSK (XPK;
    Include within a <Signature> XML element of the XML MIME body:
       (1) a cannonicalisation method to be applied to the signed information;
```

```
          (2) the signature method used for generating the signature;
          (3) a reference to the content to be signed;
          (4) the hashing method used;
          (5) the hashed content;
          (6) the key-id (XPK-ID);
          (7) the signature value;
   ENDIF;
```

EXAMPLE 3: Pseudo code showing how confidentiality protection is represented in the procedures in the present document at the server side when receiving encrypted content.

```
   IF configuration is set for confidentiality protection of sensitive data
   THEN
       Check that the XML content contains the <EncryptedData> element;
       Check that the XML document contains a URI with the domain name for MC Services
confidentiality protection;
       Return an error if the <EncryptedData> element or domain name for MC Services confidentiality
protection are not found;
       Otherwise:
          (1) obtain the CSK (XPK) using the CSK-ID (XPK-ID) in the received XML body;
          (2) for encrypted data in elements, decrypt the data elements using the CSK;
          (3) for encrypted URIs in attributes, decrypt the URIs using the CSK;
   ENDIF;
```

EXAMPLE 4: Pseudo code showing how integrity protection is represented in the procedures in the present document at the server side when receiving signed content.

```
   IF configuration is set for integrity protection of application data
   THEN
      Check that the XML content contains the <Signature> element;
      Return an error if the <Signature> element is not found;
      Otherwise:
          (1) obtain the CSK (XPK) using the CSK-ID (XPK-ID) in the received XML body;
          (2) verify the signature of the content using the CSK;
      Return an error if the validation of the signature fails;
      IF validation of the signature passes
      THEN
         decrypt any data found in <EncryptedData> elements;
         decrypt any encrypted URIs found in attributes;
      ENDIF;
   ENDIF;
```

The content can be re-encrypted and signed again using the SPK between MCData servers.

The following examples show the difference between normal and encrypted data content. In this example consider the MCData client initiating a group standalone SDS message using the signalling control plane.

EXAMPLE 5: <mcdata-info> MIME body represented with data elements in the clear:

```
   Content-Type: application/vnd.3gpp.mcdata-info+xml
   <?xml version="1.0"?>
   <mcdata-info>
     <mcdata-Params>
       <request-type>group-sds</request-type>
       <mcdata-request-uri type="Normal">
         <mcdataURI>sip:group123@mcdataoperator1.com></mcdataURI>
       </mcdata-request-uri>
     </mcdata-Params>
   </mcdata-info>
```

EXAMPLE 6: <mcdata-info> MIME body represented with the <mcdata-request-uri> encrypted:

```
   Content-Type: application/vnd.3gpp.mcdata-info+xml
   <?xml version="1.0"?>
   <mcdata-info>
     <mcdata-Params>
       <request-type>group-sds</request-type>
       <mcdata-request-uri type="Encrypted">
         <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
          Type='http://www.w3.org/2001/04/xmlenc#Content'>
           <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
           <ds:KeyInfo>
             <ds:KeyName>base64XpkId</KeyName>
```

```
            </ds:KeyInfo>
            <CipherData>
              <CipherValue>A23B45C5657689090</CipherValue>
            </CipherData>
          </EncryptedData>
        </mcdata-request-uri>
      </mcdata-Params>
    </mcdata-info>
```

EXAMPLE 7: pidf+xml MIME body represented with clear URIs in attributes:

```
Content-Type: application/pidf+xml
<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:somebody@mcdata.org">
  <tuple id="acD4rhU87bK">
    <status>
      <affiliation group="sip:thegroup@mcdata.org"/>
    </status>
  </tuple>
</presence>
```

EXAMPLE 8: pidf+xml MIME body represented with encrypted URIs in attributes:

```
Content-Type: application/pidf+xml
<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:c4Hrt45XG8IohRFT67vfdr3V;iv=45RtfVgHY23k8Ihy;xpk-id=b7UJv9;alg=128-aes-
gcm@mc1-encryption.3gppnetwork.org">
  <tuple id="acD4rhU87bK">
    <status>
      <affiliation group="sip:98yudFG45tx_89TYGedb4ujF ;iv=FGD567kjhfH7d4-D;key-id=eV9kl7;alg=128-
aes-gcm@mc1-encryption.3gppnetwork.org"/>
    </status>
  </tuple>
</presence>
```

4.7 Protection of TLV signalling and media content

The protection of TLV signalling and media content is based on 3GPP MCData security solution as defined in 3GPP TS 33.180 [26].

For different security requirements of different information elements of a MCData message, the information elements of MCData messages are bifurcated in the following components:

- **MCData Data signalling payload**: information elements necessary for identification and management of the MCData messages e.g. conversation identifiers, session identifiers, transaction identifiers, disposition requests, etc. This payload is confidentiality and integrity protected between the MCData Client and the MCData server.
- **MCData Data payload**: the actual user payload for MCData user or application consumption. This payload is end-to-end confidentiality and integrity protected.

An SDS message can be sent over both, signalling plane and media plane. When an SDS message is sent using signalling plane, the body included in the SIP MESSAGE request, which carries MCData Data signalling payload, is protected between each entity separately if protection is applied. On the other hand the body included in the SIP MESSAGE request which carries the MCData Data payload is end-to-end protected. The procedures for the protection of the SDS messages over the signalling plane are specified in this document. Protection of SDS message over media control plane is specified in 3GPP TS 24.582 [15].

For FD using HTTP and FD using media plane, the MCData Data signalling payload sent over the signalling plane is protected between each entity separately if protection is applied. The procedure for the protection of the file is specified in 3GPP TS 24.582 [15].

The ciphering algorithm indicated in the Key Download procedure by the MCData server shall be used to protect the MCData signalling fields (i.e. MCData signaling parameters, Data signaling payload and end-to-end security parameters).

4.7A Signalling security when using MBMS

Signalling security is established between the participating MCData function and the MCData client.

The protection of MBMS subchannel control messages on the general purpose MBMS subchannels can be done with MSCCKs (each identified by a corresponding MSCCK-ID), distributed during MBMS bearer announcement (see subclause 19.2.2). Each general purpose MBMS subchannel is associated with an MSCCK and a corresponding MSCCK-ID. There can be multiple general purpose MBMS subchannels deployed, each associated with its own MSCCK and corresponding MSCCK-ID. The (MSCCK-ID, MSCCK) pair is provided for each general purpose MBMS subchannel separately.

According to 3GPP TS 33.180 [26] subclause 8.2, the MCData Payload Protection Key (DPPK) referenced in subclause 6.6 is a Multicast Signalling Keys (MuSiK), (identified by a corresponding (MuSiK-ID)), distributed via MuSiK download messages. The MSCCK and MuSiKs can be distributed independently of each other and in any order and can also be used independently. Signalling supports initial keying, as well as repeated re-keying and un-keying for both MSCCK and MuSiKs.

The MuSiK download message contains an embedded MIME payload which is the MIKEY payload containing the MuSiK and MuSiK-ID, as well as an embedded XML payload potentially containing an explicit list of MCData group ids to which the key applies. Both payloads are protected as described in 3GPP TS 33.180 [26], as they are transferred between the participating MCData function and the MCData client. Within the XML payload, the list of MCData group ids is protected as application sensitive data (see subclause 4.8). Within the MIKEY payload, the MuSiK is encrypted using the MCData ID of the served MCData client. The payload is signed using a key associated to the identity of the participating MCData function.

To distribute MuSiK, the participating MCData function uses the I_MESSAGE format from subclause 5.2.4 of 3GPP TS 33.180 [26], which includes associated parameters. The participating function sets the Status associated parameter to values defined in subclause E.6.9 of 3GPP TS 33.180 [26], namely "Not-revoked" when keying or rekeying and "Revoked" when unkeying, respectively. Upon receipt, the MCData client validates the signature and, if valid, the MCData client first examines the Status attribute and either marks the associated security functions as "not in use" or stores the MuSiK and the MuSiK-ID, and then replies with a success code; otherwise, the MCData client can reply with a failure code. If a success code is not received from the MCData client in response to the MuSiK download message, the participating MCData function starts using only unicast towards the respective MCData client for the listed groups.

The security context is initiated when the MBMS bearer is announced to the MCData clients. The procedure involves the participating MCData function creating an MBMS subchannel control key (MSCCK) and a corresponding key identifier (MSCCK-ID) associated with the MBMS bearer when the MBMS bearer is activated, and then transferring the MSCCK and the MSCCK-ID associated with the MBMS bearer to served MCData clients using SIP signalling. The MSCCK is encrypted using the MCData ID of the served MCData client and domain-specific material provided from the KMS.

The MSCCK and the MSCCK-ID associated with the MBMS bearer are distributed within a MIKEY payload within the SDP describing the general purpose MBMS subchannel of the MBMS bearer. This payload is called a MIKEY-SAKKE I_MESSAGE, as defined in IETF RFC 6509 [55], which ensures the confidentiality, integrity and authenticity of the payload. The encoding of the MIKEY payload in the SDP is described in IETF RFC 4567 [45] using an "a=key-mgmt" attribute. The payload is signed using a key associated to the identity of the participating MCData function. To distribute MSCCK, the participating MCData function uses the I_MESSAGE format from subclause 5.2.4 of 3GPP TS 33.180 [26], which includes associated parameters.

The participating function sets the Status associated parameter to values defined in subclause E.6.9 of 3GPP TS 33.180 [26], namely "Not-revoked" when keying or rekeying and "Revoked" when unkeying, respectively. Upon receipt, the MCData client validates the signature and, if the signature is found valid and the I_MESSAGE contains a Status attribute, the MCData client first examines the Status attribute and either marks the associated security functions as "not in use" or extracts and stores the encapsulated MSCCK and the corresponding MSCCK-ID. The decrypted key is used as described in 3GPP TS 33.180 [26]. With the MSCCK successfully shared between the participating MCData function and the served UEs, the participating MCData function is able to securely send MBMS subchannel control messages to the MCData clients.

4.8 MCData client ID

The MCData client assigns the MCData client ID when the MCData client is used for the first time. The MCData client generates the MCData client ID as specified in subclause 4.2 of IETF RFC 4122 [25].

The MCData client preserves the MCData client ID:

- while the MCData client is SIP registered as specified in 3GPP TS 24.229 [5];
- while the MCData client is not SIP registered as specified in 3GPP TS 24.229 [5] and the UE serving the MCData client is switched on;
- while the UE serving the MCData client is switched off; and
- while the UE serving the MCData client is power-cycled.

NOTE: MCData client ID is not preserved when the UE is reset to factory settings.

4.9 Warning Header Field

4.9.1 General

The MCData server can include a free text string in a SIP response to a SIP request. When the MCData server includes a text string in a response to a SIP MESSAGE or SIP INVITE request the text string is included in a Warning header field as specified in IETF RFC 3261 [24]. The MCData server includes the Warning code set to 399 (miscellaneous warning) and includes the host name set to the host name of the MCData server.

EXAMPLE: Warning: 399 "200 user not authorised to transmit data "

4.9.2 Warning texts

The text string included in a Warning header field consists of an explanatory text preceded by a 3-digit text code, according to the following format in Table 4.4.2-1.

Table 4.9.2-1 ABNF for the Warning text

```
warn-text      =/  DQUOTE mcdata-warn-code SP mcdata-warn-text DQUOTE
mcdata-warn-code = DIGIT DIGIT DIGIT
mcdata-warn-text = *( qdtext | quoted-pair )
```

Table 4.4.2-2 defines the warning texts that are defined for the Warning header field when a Warning header field is included in a response to a SIP INVITE request as specified in subclause 4.4.1.

Table 4.9.2-2: Warning texts defined for the Warning header field

Code	Explanatory text	Description
101	service authorisation failed	The service authorisation of the MCData ID against the IMPU failed at the MCData server.
102	too many simultaneous affiliations	The MCData user already has N2 maximum number of simultaneous affiliations.
104	isfocus not assigned	A controlling MCData function has not been assigned to the MCData session.
113	group document does not exist	The group document requested from the group management server does not exist.
114	unable to retrieve group document	The group document exists on the group management server but the MCData server was unable to retrieve it.
115	group is disabled	The group has the <disabled> element set to "true" in the group management server.
116	user is not part of the MCData group	The group exists on the group management server but the requesting user is not part of this group.
120	user is not affiliated to this group	The MCData user is not affiliated to the group.
136	authentication of the MIKEY-SAKKE I_MESSAGE failed	Security context establishment failed.
139	integrity protection check failed	The integrity protection of an XML MIME body failed.
140	unable to decrypt XML content	The XML content cannot be decrypted.
141	user unknown to the participating function	The participating function is unable to associate the public user identity with an MCData ID.
142	unable to determine the controlling function	The participating function is unable to determine the controlling function for the group call or private call.
145	unable to determine called party	The participating function was unable to determine the called party from the information received in the SIP request.
198	no users are affiliated to this group	No users in the group are affiliated.
199	expected MIME bodies not in the request"	The expected MIME bodies were not received in the SIP request.
200	user not authorised to transmit data	The MCData user is not authorised to transmit data.
201	user not authorised to transmit data on this group identity	The MCData user is not authorised to transmit data on the group identity included in the request.
202	user not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request	The MCData user is not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request
203	message too large to send over signalling control plane	The MCData client sent data that is greater than the size that can be handled by the signalling control plane.
204	unable to determine targeted user for one-to-one SDS	The MCData server is unable to determine the targeted user for one-to-one SDS.
205	unable to determine targeted user for one-to-one FD	The MCData server is unable to determine the targeted user for one-to-one FD.
206	short data service not allowed for this group	SDS is not allowed on the group indicated in the SDS request.
207	SDS services not supported for this group	SDS services not supported for this group
208	user not authorised for MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request	The MCData user is not authorised for group MCData communications due to exceeding the maximum amount of data that can be sent in a single request.
209	one FD SIGNALLING PAYLOAD or FD HTTP TERMINATION message only must be present in FD request	Only one FD SIGNALLING PAYLOAD or FD HTTP TERMINATION message must be present in FD request
210	Only one File URL must be present in the FD request	Only one File URL must be present in the FD request.
211	payload for an FD request is not FILEURL	The payload in the FD request did not contain a FILEURL

212	file referenced by file URL does not exist	The MCData server was unable to locate the file referenced by the file URL.
213	file distribution not allowed for this group	FD is not allowed on the group indicated in the FD request.
214	FD services not supported for this group	FD services not supported for this group
215	request to transmit is queued by the server	The MCData request was queued by the server for later transmission.
216	unable to correlate the disposition notification	The MCData server was unable to correlate the disposition notification to a MCData message.
217	user not authorised for SDS communications on this group identity due to message size	The size of the message exceeded the maximum data allowed for SDS communications on this group identity
218	user not authorised for one-to-one SDS communications due to message size	The size of the message exceeded the maximum data allowed for one-to-one SDS communications.
219	user not authorised for FD communications on this group identity due to file size	The size of the file exceeded the maximum data allowed for FD communications on this group identity
220	user not authorised for FD communications due to file size	The size of the file exceeded the maximum data allowed for one-to-one FD communications.
221	user not authorised to initiate one-to-one SDS session	The MCData user is not authorised to initiate a one-to-one SDS session.
222	user not authorised to initiate group SDS session on this group identity	The MCData user is not authorised to initiate a SDS session on the group identity included in the request.
223	No Conversation ID or Message ID present	Conversation ID and Message ID required to identify transmission
224	No Transmission available	No transmission identified with given Conversation ID, Message Id and file URL
225	User not authorized to initiate pre-established session	The MCData user is not authorised to initiate a pre-established MCData session.
226	function not allowed due to pre-established session not supported	Pre-established session is not supported by MCData participating function
227	unable to determine targeted user for one-to-one IP Connectivity	The MCData server is unable to determine the targeted user for one-to-one IP Connectivity.
228	maximum number of service authorizations reached	The number of maximum simultaneous service authorizations for the MCData user has been reached.
229	one-to-one MCData communication not authorised to the targeted user"	The user is not authorised to initiate one-to-one MCData communication to this targeted user".
230	one-to-one MCData communication not authorised from this originating user"	The user is not authorised to receive one-to-one MCData communication from this originating user".

4.10 MCData emergency groups and emergency group communications

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

MCData emergency groups and emergency group communications as defined by 3GPP TS 23.282 [2] are supported by the procedures in this specification. There are a number of state variables used to manage MCData emergencies, including:

- **MCData emergency state:** in accordance with 3GPP TS 23.282 [2], indicates (see subclause G.4.2) that the MCData user is in a life-threatening situation. This MCData client state variable is changed via action by the MCData user of the device or by an authorised MCData user. While the MCData emergency state is set on the client, all communications originated by the client will be MCData emergency communications, assuming the MCData user is authorised for MCData emergency communications.

- **in-progress emergency group state:** in accordance with 3GPP TS 23.282 [2], this state variable (see subclause G.4.3) indicates whether or not there is an MCData emergency group communication ongoing on the specified group. This state is managed by the controlling MCData function. All group communications originated on this MCData group when in an in-progress emergency state are MCData emergency group communications until this state is cancelled, regardless of the originator being (or not) in an MCData emergency state.

- **MCData emergency group (MDEG) state:** this is an internal state (see subclause G.4.4) managed by the MCData client which tracks the in-progress emergency state of the group (see 3GPP TS 23.282 [2]) managed by the controlling MCData function. Ideally, the MCData client would not need to track the in-progress emergency group state, but doing so enables the MCData client to request MCData emergency-level priority earlier than otherwise possible. For example, if the MCData user wishes to join an MCData emergency group communication and is not in MCData emergency state itself, the MCData client should have emergency level priority. If it has knowledge of the in-progress emergency state of the group, it can request priority by including a Resource-Priority header field set to the MCPTT namespace specified in IETF RFC 8101 [67], and appropriate priority level in the SIP INVITE request (or SIP re-INVITE request).

- **MCData emergency group communication (MDEGC) state**: this is an internal state (see subclause G.4.5) corresponding to an ongoing group communication. The state is managed by the MCData client, which in conjunction with the MCData emergency alert state (see subclause 4.4), aids in managing the MCData emergency state and related actions.

5 Functional entities

5.1 Introduction

This clause associates the functional entities with the MCData roles described in the stage 2 architecture document (see 3GPP TS 23.282 [2]).

5.2 MCData client

To be compliant with the procedures in the present document, an MCData client shall:

- act as the user agent for all MCData application transactions (e.g. initiation of a group standalone SDS message); and

- support handling of the MCData client ID as described in subclause 4.8.

To be compliant with the on-network procedures in the present document, an MCData client shall:

- support the MCData client on-network procedures defined in 3GPP TS 23.282 [2];

- support the GCS UE procedures defined in 3GPP TS 23.468 [56] for unicast delivery, MBMS delivery and service continuity;

- support the on-network MCData message formats specified in clause 15 for the short data service (SDS) and the file distribution service (FD);

- act as a SIP UA as defined in 3GPP TS 24.229 [5];

- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [5] and:

  a) subclause 9.2.3 and subclause 9.2.4 for short data service; and

  b) subclause 10.2.5 for file distribution.

- for registration and service authorisation, implement the procedures specified in subclause 7.2;

- for affiliation, implement the procedures specified in subclause 9.2;

- for short data service (SDS) functionality implement the MCData client procedures specified in:

a) subclause 9.2; and

b) clause 6 of 3GPP TS 24.582 [15];

- for file distribution (FD) functionality implement the MCData client procedures specified in:

a) subclause 10.2; and

b) clause 7 of 3GPP TS 24.582 [15];

- for transmission and reception control functionality implement the MCData client procedures specified in clause 11;
- for disposition notification functionality implement the MCData client procedures specified in subclause 12.2;
- for communication release functionality implement the MCData client procedures specified in subclause 13.2; and
- for functional alias management, implement the procedures specified in subclause 22.2.1.

To be compliant with the off-network procedures in the present document, an MCData client shall:

- support the off-network procedures defined in 3GPP TS 23.282 [2];
- support the off-network MCData message formats specified in clause 15;
- implement the procedures for ProSe direct discovery for public safety use as specified in 3GPP TS 24.334 [25];
- implement the procedures for one-to-one ProSe direct communication for Public Safety use as specified in 3GPP TS 24.334 [25]; and
- for short data service (SDS) functionality implement the MCData client procedures specified in subclause 9.3.

To be compliant with the on-network and off-network procedures in the present document requiring end-to-end security key distribution, an MCData client shall support the procedures specified in 3GPP TS 33.180 [26].

To be compliant with the procedures for confidentiality protection of XML elements in the present document, the MCData client shall implement the procedures specified in subclause 6.5.2.

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the MCData client shall implement the procedures specified in subclause 6.5.3.

5.3 MCData server

5.3.0 General

An MCData server can perform the controlling role for short data service and file distribution as defined in 3GPP TS 23.282 [2].

An MCData server can perform the participating role for short data service and file distribution as defined in 3GPP TS 23.282 [2].

An MCData server performing the participating role can serve an originating MCData user.

An MCData server performing the participating role can serve a terminating MCData user.

The same MCData server can perform the participating role and controlling role for the same group short data service transaction or group file distribution transaction.

When referring to the procedures in the present document for the MCData server acting in a participating role for the served user, the term, "participating MCData function" is used.

When referring to the procedures in the present document for the MCData server acting in a controlling role for the served user, the term "controlling MCData function" is used.

To be compliant with the procedures in the present document, an MCData server shall:

- support the MCData server procedures defined in 3GPP TS 23.282 [2];
- support the GCS AS procedures defined in 3GPP TS 23.468 [56] for unicast delivery, MBMS delivery and service continuity;
- implement the role of an AS performing 3rd party call control acting as a routing B2BUA as defined in 3GPP TS 24.229 [5];
- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [5] and:
  a) subclause 9.2.3 and subclause 9.2.4 for short data service; and
  b) subclause 10.2.5 for file distribution.
- for registration and service authorisation, implement the procedures specified in subclause 7.3;
- for affiliation, implement the procedures specified in subclause 9.2.2;
- for short data service (SDS) functionality implement the MCData server procedures specified in:
  a) subclause 9.2; and
  b) clause 6 of 3GPP TS 24.582 [15];
- for file distribution (FD) functionality implement the MCData server procedures specified in:
  a) subclause 10.2; and
  b) clause 7 of 3GPP TS 24.582 [15];
- for transmission and reception control functionality implement the MCData server procedures specified in clause 11;
- for disposition notification functionality implement the MCData server procedures specified in clause 12.2;
- for communication release functionality implement the MCData server procedures specified in clause 13.2; and
- for functional alias management, implement the procedures specified in subclause 22.2.2.

To be compliant with the procedures in the present document requiring the distribution of keying material between MCData clients as specified in 3GPP TS 33.180 [26], an MCData server shall ensure that the keying material is copied from the incoming MCData messages into the outgoing MCData messages.

To be compliant with the procedures for confidentiality protection of XML elements in the present document, the MCData server shall implement the procedures specified in subclause 6.5.2.

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the MCData server shall implement the procedures specified in subclause 6.5.3.

5.3.1 SIP failure case

When initiating a SIP failure response to any received SIP request, depending on operator policy, the MCData server may insert a SIP Response-Source header field in accordance with the procedures in subclause 5.7.1.0 of 3GPP TS 24.229 [5], where the "role" header field parameter is set to "pf-mcdata-server" or "cf-mcdata-server" depending on the current role endorsed by the MCData server.

5.3.2 Management of MBMS bearers

When providing services over MBMS, an MCData server acting in the participating MCData function role shall:

- allocate TMGIs and activate MBMS bearers in MBMS service areas to be used for MCData media plane transmissions via multicast, per 3GPP TS 23.468 [56] and 3GPP TS 29.468 [57];

- deactivate MBMS bearers and deallocate TMGIs when no longer necessary, per 3GPP TS 23.468 [56] and 3GPP TS 29.468 [57];
- handle MBMS bearers related notifications per 3GPP TS 23.468 [56] and 3GPP TS 29.468 [57]; and
- adjust the priority / pre-emption characteristics of MBMS bearers, as appropriate, in response to relevant events, using procedures specified in per 3GPP TS 23.468 [56] and 3GPP TS 29.468 [57].

6 Common procedures

6.1 Introduction

This clause describes the common procedures for each functional entity.

6.2 MCData client procedures

6.2.1 Distinction of requests at the MCData client

6.2.1.1 SIP MESSAGE request

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

The MCData client needs to distinguish between the following SIP MESSAGE request for originations and terminations:

- SIP MESSAGE request routed to the MCData client containing a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml" and includes an XML body containing a Location root element containing a Configuration element. Such requests are known as "SIP MESSAGE request for location report configuration";
- SIP MESSAGE request routed to the MCData client containing a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml" and includes an XML body containing a Location root element containing a Request element. Such requests are known as "SIP MESSAGE request for location report request";
- SIP MESSAGE request routed to the MCData client containing a Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and including an <alert-ind> element set to a value of "true" or "false" and/or an <emergency-ind> element set to a value of "true" or "false". Such requests are known as "SIP MESSAGE request for emergency notification";
- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for standalone SDS for terminating MCData client";
- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for FD using HTTP for terminating MCData client";
- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an SDS NOTIFICATION message Such requests are known as "SIP MESSAGE request for SDS disposition notification for terminating MCData client"; and

- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an FD NOTIFICATION message Such requests are known as "SIP MESSAGE request for FD disposition notification for terminating MCData client";

- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-info+xml MIME body containing a <request-type> element in of the SIP MESSAGE request contains the value "msf-disc-res". Such requests are known as "SIP MESSAGE request for absolute URI discovery response"; and

- SIP MESSAGE request routed to the MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an DEFERRED DATA RESPONSE message. Such requests are known as "SIP MESSAGE response for the list of deferred group communications request".

6.2.1.2 SIP INVITE request

The MCData client needs to distinguish between the following SIP INVITE requests for terminations:

- SIP INVITE request routed to the terminating MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds" or "group-sds" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "initial SIP INVITE request for standalone SDS over media plane for terminating MCData client";

- SIP INVITE request routed to the terminating MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds-session" or "group-sds-session" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "initial SIP INVITE request for SDS session for terminating MCData client";

- SIP INVITE request routed to the terminating MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-fd" or "group-fd" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "initial SIP INVITE request for file distribution for terminating MCData client"; and

- SIP INVITE request routed to the terminating MCData client with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-ipconn" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "initial SIP INVITE request for IP Connectivity session for terminating MCData client".

6.2.2 MCData conversation items

6.2.2.1 Generating an SDS Message

In order to generate an SDS message, the MCData client:

1) shall generate an SDS SIGNALLING PAYLOAD message as specified in subclause 15.1.2;

2) shall generate a DATA PAYLOAD message as specified in subclause 15.1.4;

3) shall include in the SIP request, the SDS SIGNALLING PAYLOAD message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

4) shall include in the SIP request, the DATA PAYLOAD message in an application/vnd.3gpp.mcdata-payload MIME body as specified in subclause E.2.

When generating an SDS SIGNALLING PAYLOAD message as specified in subclause 15.1.2, the MCData client:

1) shall set the Date and time IE to the current time as specified in subclause 15.2.8;

2) if the SDS message starts a new conversation, shall set the Conversation ID IE to a newly generated Conversation ID value as specified in subclause 15.2.9;

3) if the SDS message continues an existing unfinished conversation, shall set the Conversation ID IE to the Conversation ID value of the existing conversation as specified in subclause 15.2.9;

4) shall set the Message ID IE to a newly generated Message ID value as specified in subclause 15.2.10;

5) if the SDS message is in reply to a previously received SDS message, shall include the InReplyTo message ID IE with the Message ID value in the previously received SDS message;

6) if the SDS message is for user consumption, shall not include an Application ID IE as specified in subclause 15.2.7and shall not include an Extended application ID IE as specified in subclause 15.2.24;

7) if the SDS message is intended for an application on the terminating MCData client, shall include:

   a) an Application ID IE with a Application ID value representing the intended application as specified in subclause 15.2.7; or

   b) an Extended application ID IE with an Extended application ID value representing the intended application as specified in subclause 15.2.24;

NOTE: The value chosen for the Application ID value is decided by the mission critical organisation.

8) if only a delivery disposition notification is required shall include a SDS disposition request type IE set to "DELIVERY" as specified in subclause 15.2.3;

9) if only a read disposition notification is required shall include a SDS disposition request type IE set to "READ" as specified in subclause 15.2.3;

10) if both a delivery and read disposition notification is required shall include a SDS disposition request type IE set to "DELIVERY AND READ" as specified in subclause 15.2.3; and

11) may set the User location IE to the current location of the UE as specified in subclause 15.2.25.

When generating an DATA PAYLOAD message for SDS as specified in subclause 15.1.4, the MCData client:

1) shall set the Number of payloads IE to the number of Payload IEs that needs to be encoded, as specified in subclause 15.2.12;

2) if end-to-end security is required for a one-to-one communication, shall include the Security parameters and Payload IE with security parameters as described in 3GPP TS 33.180 [26]. Otherwise, if end-to-end security is not required for a one-to-one communication, shall include the Payload IE as specified in subclause 15.1.4; and

3) for each Payload IE included:

   a) if the payload is text, shall set the Payload content type as "TEXT" as specified in subclause 15.2.13;

   b) if the payload is binary data, shall set the Payload content type as "BINARY" as specified in subclause 15.2.13;

   c) if the payload is hyperlinks, shall set the Payload content type as "HYPERLINKS" as specified in subclause 15.2.13;

   d) if the payload is location, shall set the Payload content type as "LOCATION" as specified in subclause 15.2.13;

e) if payload is enhanced status for a group, shall set the Payload content type as “ENHANCED STATUS” as specified in subclase 15.2.13; and

f) shall include the data to be sent in the Payload data.

6.2.2.2 Generating an FD Message for FD using HTTP

In order to generate an FD message, the MCData client:

1) shall generate an FD SIGNALLING PAYLOAD message as specified in subclause 15.1.3; and

2) shall include in the SIP request, the FD SIGNALLING PAYLOAD message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an FD SIGNALLING PAYLOAD message as specified in subclause 15.1.3, the MCData client:

1) shall set the Date and time IE to the current time as specified in subclause 15.2.8;

2) if the FD message starts a new conversation, shall set the Conversation ID IE to a newly generated Conversation ID value as specified in subclause 15.2.9;

3) if the FD message continues an existing unfinished conversation, shall set the Conversation ID IE to the Conversation ID value of the existing conversation as specified in subclause 15.2.9;

4) shall set the Message ID IE to a newly generated Message ID value as specified in subclause 15.2.10;

5) if the FD message is in reply to a previously received MCData message, shall include the InReplyTo message ID IE with the Message ID value in the previously received MCData message;

6) if the FD message is for user consumption, shall not include an Application ID IE as specified in subclause 15.2.7 and shall not include an Extended application ID IE as specified in subclause 15.2.24;

7) if the FD message is intended for an application on the terminating MCData client, shall include:

   a) an Application ID IE with a Application ID value representing the intended application as specified in subclause 15.2.7; or

   b) an Extended application ID IE with an Extended application ID value representing the intended application as specified in subclause 15.2.24;

NOTE: The value and field chosen for coding the identity of the application are coordinated by the mission critical organisation.

8) may include an FD disposition request type IE set to "FILE DOWNLOAD COMPLETE UPDATE" as specified in subclause 15.2.4;

9) if requiring mandatory download at the recipient side, shall include a Mandatory download IE as specified in subclause 15.2.16 set to the value of "MANDATORY DOWNLOAD";

10) shall include a Payload IE with:

   a) the Payload content type set to "FILEURL" as specified in subclause 15.2.13; and

   b) the URL of the file in the Payload data as as specified in subclause 15.2.13; and

11) may include a Metadata IE with the required file description information and file availability information, as specified in subclause 15.2.17.

6.2.2.3 Generating an FD Message for FD using media plane

In order to generate an FD message, the MCData client:

1) shall generate an FD SIGNALLING PAYLOAD message as specified in subclause 15.1.3; and

2) shall include in the SIP request, the FD SIGNALLING PAYLOAD message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an FD SIGNALLING PAYLOAD message as specified in subclause 15.1.3, the MCData client:

1) shall set the Date and time IE to the current time as specified in subclause 15.2.8;

2) if the filestarts a new conversation, shall set the Conversation ID IE to a newly generated Conversation ID value as specified in subclause 15.2.9;

3) if the filecontinues an existing conversation, shall set the Conversation ID IE to the Conversation ID value of the existing conversation as specified in subclause 15.2.9;

4) shall set the Message ID IE to a newly generated Message ID value as specified in subclause 15.2.10;

5) if the fileis in reply to a previously received SDS message or file, shall include the InReplyTo message ID IE with the Message ID value in the previously received SDS message or file;

6) if the file is for user consumption, shall not include an Application ID IE as specified in subclause 15.2.7 and shall not include an Extended application ID IE as specified in subclause 15.2.24;

7) if the file is intended for an application on the terminating MCData client, shall include:

   a) an Application ID IE with a Application ID value representing the intended application as specified in subclause 15.2.7; or

   b) an Extended application ID IE with an Extended application ID value representing the intended application as specified in subclause 15.2.24;

NOTE: The value and field chosen for coding the identity of the application are coordinated by the mission critical organisation.

8) if a file download complete notification is required shall include a FD disposition request type IE set to "FILE DOWNLOAD COMPLETED UPDATE" as specified in subclause 15.2.4; and

9) shall include and set the Mandatory download IE to "MANDATORY DOWNLOAD" as described in subclause 15.2.16.

6.2.2.4 Client generating message to terminate FD over HTTP

In order to generate an message to terminate FD using HTTP, the MCData client:

1) shall generate an FD HTTP TERMINATION message as specified in subclause 15.1.13; and

2) shall include in the SIP request, the FD HTTP TERMINATION message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an FD HTTP TERMINATION message as specified in subclause 15.1.13, the MCData client:

1) shall set the Conversation ID IE to a value identifying the conversation, as specified in subclause 15.2.9;

2) shall set the Message ID IE to a value identifying the message as specified in subclause 15.2.10;

3) may set:

   a) the Application ID IE to the stored value if applicable; or

   b) the Extended Application ID IE to the stored value if applicable;

4) shall include a Payload IE with:

   a) shall set the Payload content type set to "FILEURL" as specified in subclause 15.2.13; and

   b) shall set the URL of the file same as of FD transmission; and

5) Shall set the Termination information type IE set to "TERMINATION REQUEST" as specified in subclause 15.2.22.

6.2.3 Disposition Notifications

6.2.3.1 Generating an SDS Notification

In order to generate an SDS notification, the MCData client:

1) shall generate an SDS NOTIFICATION message as specified in subclause 15.1.5; and

2) shall include in the SIP request, the SDS NOTIFICATION message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an SDS NOTIFICATION message as specified in subclause 15.1.5, the MCData client:

1) if sending a delivered notification, shall set the SDS disposition notification type IE as "DELIVERED" as specified in subclause 15.2.5;

2) if sending a read notification, shall set the SDS disposition notification type IE as "READ" as specified in subclause 15.2.5;

3) if sending a delivered and read notification, shall set the SDS disposition notification type IE as "DELIVERED AND READ" as specified in subclause 15.2.5;

4) if the SDS message could not be delivered to the user or application (e.g. due to lack of storage), shall set the SDS disposition notification type IE as "UNDELIVERED" as specified in subclause 15.2.5;

5) shall set the Date and time IE to the current time to as specified in subclause 15.2.8;

6) shall set the Conversation ID to the value of the Conversation ID that was received in the SDS message as specified in subclause 15.2.9;

7) shall set the Message ID to the value of the Message ID that was received in the SDS message as specified in subclause 15.2.10;

8) if the SDS message was destined for the user, shall not include an Application ID IE (as specified in subclause 15.2.7) and shall not include an Extended application ID IE (as specified in subclause 15.2.24); and

9) if the SDS message was destined for an application, shall include:

   a) an Application ID IE set to the value of the Application ID that was included in the SDS message as specified in subclause 15.2.3; or

   b) an Extended application ID IE set to the value of the Extended application ID that was included in the SDS message as specified in subclause 15.2.24.

6.2.3.2 Generating an FD Notification

In order to generate an FD notification, the MCData client:

1) shall generate an FD NOTIFICATION message as specified in subclause 15.1.6; and

2) shall include in the SIP request, the FD NOTIFICATION message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an FD NOTIFICATION message as specified in subclause 15.1.6, the MCData client:

1) if sending a file download accept notification, shall set the FD disposition notification type IE as "FILE DOWNLOAD REQUEST ACCEPTED" as specified in subclause 15.2.6;

2) if sending a file download reject notification, shall set the FD disposition notification type IE as "FILE DOWNLOAD REQUEST REJECTED" as specified in subclause 15.2.6;

3) if sending a file download deferred notification, shall set the FD disposition notification type IE as "FILE DOWNLOAD REQUEST DEFERRED" as specified in subclause 15.2.6;

4) shall set the Conversation ID to the value of the Conversation ID that was received in the FD message as specified in subclause 15.2.9;

5) shall set the Date and time IE to the current time as specified in subclause 15.2.8; and

6) if sending a file download completed notification:

   a) shall set the FD disposition notification type IE as "FILE DOWNLOAD COMPLETED" as specified in subclause 15.2.6;

   b) shall set the Message ID to the value of the Message ID that was received in the FD message as specified in subclause 15.2.10;

   c) if the FD message was destined for the user, shall not include an Application ID IE as specified in subclause 15.2.7 and shall not include a Extended application ID IE as specified in subclause 15.2.24; and

   d) if the FD message was destined for an application, shall include:

      i) an Application ID IE set to the value of the Application ID that was included in the FD message as specified in subclause 15.2.3; or

      ii) an Extended application ID IE set to the value of the Extended application ID that was included in the FD message as specified in subclause 15.2.24.

6.2.4 Sending SIP requests and receiving SIP responses

6.2.4.1 Generating a SIP MESSAGE request towards the originating participating MCData function

This subclause is referenced from other procedures.

In a SIP MESSAGE request, the MCData client:

1) when sending SDS messages or SDS disposition notifications:

   a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

   b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8]; and

   c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

2) when sending FD messages, FD disposition notifications or FD media storage function discovery messages:

   a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

   b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8]; and

   c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

3) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [5]; and

4) shall set the Request-URI to the public service identity identifying the participating MCData function serving the MCData user.

6.2.5 Location information

6.2.5.1 Location information for location reporting

This procedure is initiated by the MCData client when it is including location report information as part of a SIP request for a specified location trigger.

The MCData client:

1) shall include an application/vnd.3gpp.location-info+xml MIME body as specified in Annex D.4 with a <Report> element included in the <location-info> root element; and

2) shall include in the <Report> element the specific location information configured for the specified location trigger.

6.3 MCData server procedures

6.3.1 Distinction of requests at the MCData server

6.3.1.1 SIP MESSAGE request

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

The MCData server needs to distinguish between the following SIP MESSAGE request for originations and terminations:

- SIP MESSAGE requests routed to the participating MCData function as a result of processing initial filter criteria at the S-CSCF in accordance with the origination procedures as specified in 3GPP TS 24.229 [5] with the Request-URI set to the MBMS public service identity of the participating MCData function. Such requests are known as "SIP MESSAGE request for an MBMS listening status update";

- SIP MESSAGE request routed to the participating MCData function containing a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml" and includes an XML body containing a Location root element containing a Report element. Such requests are known as "SIP MESSAGE request for location reporting";

- SIP MESSAGE request routed to the MCData client containing a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml" and includes an XML body containing a Location root element containing a Configuration element. Such requests are known as "SIP MESSAGE request for location report configuration";

- SIP MESSAGE request routed to the MCData client containing a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml" and includes an XML body containing a Location root element containing a Request element. Such requests are known as "SIP MESSAGE request for location report request";

- SIP MESSAGE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for standalone SDS for originating participating MCData function";

- SIP MESSAGE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-info+xml MIME body containing a <request-type> element containing the value "msf-disc-req". Such requests are known as "SIP MESSAGE request for absolute URI discovery request for participating MCData function";

- SIP MESSAGE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-info+xml MIME body containing a <request-type> element containing the value "msf-disc-res". Such requests are known as "SIP MESSAGE request for absolute URI discovery response for participating MCData function";

- SIP MESSAGE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-info+xml MIME body containing a <request-type> element containing the value "msf-disc-req". Such requests are known as "SIP MESSAGE request for absolute URI discovery request for controlling MCData function";

- SIP MESSAGE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for FD using HTTP for originating participating MCData function";

- SIP MESSAGE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an FD NETWORK NOTIFICATION message. Such requests are known as "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function";

- SIP MESSAGE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for standalone SDS for terminating participating MCData function";

- SIP MESSAGE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for FD using HTTP for terminating participating MCData function";

- SIP MESSAGE request routed to an MCData server with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an SDS NOTIFICATION message Such requests are known as "SIP MESSAGE request for SDS disposition notification for MCData server";

- SIP MESSAGE request routed to an MCData server with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an FD NOTIFICATION message. Such requests are known as "SIP MESSAGE request for FD disposition notification for MCData server";

- SIP MESSAGE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for standalone SDS for controlling MCData function";

- SIP MESSAGE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for FD using HTTP for controlling MCData function";

- SIP MESSAGE requests routed to the controlling MCData function with the Request-URI set to the public service identity of the controlling MCData function and containing a Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and including an XML body containing a <mcdatainfo> root element

containing a <mcdata-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for controlling MCData function";

- SIP MESSAGE requests routed to the originating participating MCData function with the Request-URI set to the public service identity of the participating MCData function and containing a Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and including an XML body containing a <mcdatainfo> root element containing a <mcdata-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for originating participating MCData function";

- SIP MESSAGE requests routed to the terminating participating MCData function with the Request-URI set to the public service identity of the terminating participating MCData function and containing a Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and including an XML body containing a <mcdatainfo> root element containing a <mcdata-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for terminating participating MCData function";

- SIP MESSAGE requests routed to the terminating participating MCData function with the Request-URI set to the public service identity of the terminating participating MCData function and containing an "application/vnd.3gpp.mcdata-info+xml" MIME body with an <alert-ind-rcvd> element present. Such requests are known as "SIP MESSAGE requests indicating delivery of emergency notification"; and

- SIP MESSAGE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field, and with an application/vnd.3gpp.mcdata-signalling MIME body containing an DEFERRED DATA REQUEST message. Such requests are known as "SIP MESSAGE request for list of deferred group communications".

If a SIP MESSAGE request is received at an MCData server that is not in accordance with the SIP MESSAGE requests listed above, then the MCData server shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response.

6.3.1.2 SIP INVITE request

The MCData server needs to distinguish between the following SIP INVITE requests for originations and terminations:

- SIP INVITE requests routed to the participating MCData function with the Request-URI set to a public service identity of the participating MCData function and contain in an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdataInfo> element containing the <mcdata-Params> element with the <anyExt> element an <pre-established-session-ind> element set to a value of "true". Such requests are known as "SIP INVITE request for establishing a pre-established session" in the procedures in the present document;

- SIP INVITE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds" or "group-sds" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for standalone SDS over media plane for originating participating MCData function";

- SIP INVITE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds" or "group-sds" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for standalone SDS over media plane for terminating participating MCData function";

- SIP INVITE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds" or "group-sds" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for controlling MCData function for standalone SDS over media plane";

- SIP INVITE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds-session" or "group-sds-session" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for SDS session for originating participating MCData function";

- SIP INVITE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds-session" or "group-sds-session" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for SDS session for terminating participating MCData function";

- SIP INVITE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-sds-session" or "group-sds-session" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for controlling MCData function for SDS session";

- SIP INVITE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-fd" or "group-fd" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for file distribution for originating participating MCData function";

- SIP INVITE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-fd" or "group-fd" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for file distribution for terminating participating MCData function"; and

- SIP INVITE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-fd" or "group-fd" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for controlling MCData function for file distribution";

- SIP INVITE request routed to the originating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-ipconn" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for IP Connectivity session for originating participating MCData function;.

- SIP INVITE request routed to the terminating participating MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-ipconn" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for IP Connectivity session for terminating participating MCData function"; and

- SIP INVITE request routed to the controlling MCData function with an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in a P-Asserted-Service header field and a <request-type> element set to "one-to-one-ipconn" contained in an application/vnd.3gpp.mcdata-info+xml MIME body. Such requests are known as "SIP INVITE request for controlling MCData function for IP Connectivity session".

6.3.2 Sending SIP requests and receiving SIP responses

6.3.2.1 Generating a SIP MESSAGE request towards the terminating MCData client

This subclause is referenced from other procedures.

The participating MCData function shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] and:

1) shall include in the SIP MESSAGE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP MESSAGE request;

2) shall set the Request-URI of the outgoing SIP MESSAGE request to the public user identity associated to the MCData ID of the terminating MCData user;

3) shall populate the outgoing SIP MESSAGE request MIME bodies as specified in subclause 6.4 and

4) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP MESSAGE request to the P-Asserted-Identity header field of the outgoing SIP MESSAGE request.

6.3.3 Retrieving a group document

This subclause describes how an MCData server accesses a group document from a group management server.

Upon receipt of a SIP request:

1) if the MCData server is not yet subscribed to the group document for the group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request, the MCData server shall subscribe to the "xcap-diff" event-package for the group document of this group identity as specified in 3GPP TS 24.481 [11];

NOTE: As a group document can potentially have a large content, the MCData server can subscribe to the group document indicating support of content-indirection as defined in IETF RFC 4483 [13], by following the procedures in 3GPP TS 24.481 [11].

2) upon receipt of a SIP 404 (Not Found) response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document of the group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request as specified in 3GPP TS 24.481 [11], the MCData server shall send the SIP 404 (Not Found) response with the warning text set to "113 group document does not exist" in a Warning header field as specified in subclause 4.9. Otherwise, continue with the rest of the steps; and

3) upon receipt of any other SIP 4xx, SIP 5xx or SIP 6xx response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document of the group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request as specified in 3GPP TS 24.481 [11], the MCData server shall send the SIP final response with the warning text set to "114 unable to retrieve group document" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

6.3.4 Determining targeted group members for MCData communications

The MCData server shall only send MCData messages to affiliated group members.

The MCData server determines whether a user is affiliated to a group by following the procedures in subclause 6.3.5.

The MCData server performs the affiliation check in subclause 6.3.5 on each entry contained in the <list> element of the group document.

6.3.5 Affiliation check

The MCData server shall determine that the MCData user, with MCData User ID, is affiliated to the MCData group, with MCData Group ID, at the MCData client, with MCData client ID, if the elements, as described in subclause 8.3.3.2, exist with their expected values, as below:

1. an MCData group information entry with MCData group ID same as the MCData group ID under consideration;
2. in the MCData group information entry found in 1, an MCData user information entry with the MCData ID same as the MCData ID under consideration;
3. in the MCData user information entry found in 2, an MCData client information entry with MCData Client ID same as the MCData client ID under consideration; and
4. in the MCData user information entry found in 2, an expiration time, which has not expired.

6.3.6 MCData conversation items

6.3.6.1 Server generating a FD HTTP TERMINATION message for FD over HTTP

In order to generate an terminating response message for FD over HTTP, the MCData server:

1) shall generate an FD HTTP TERMINATION message as specified in subclause 15.1.13; and
2) shall include in the SIP request, the FD HTTP TERMINATION message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1.

When generating an FD HTTP TERMINATION message as specified in subclause 15.1.13, the MCData server:

1) shall set the Conversation ID IE to a value identifying the conversation, as specified in subclause 15.2.9;
2) shall set the Message ID IE to a value identifying the message as specified in subclause 15.2.10;
3) may set the Application ID IE ID to the stored value if applicable;
4) shall include a Payload IE with:
   a) Shall set the Payload content type set to "FILEURL" as specified in subclause 15.2.13; and
   b) Shall set the URL of the file same as payload of FD transmission; and
5) Shall set the Termination information type IE set to "TERMINATION RESPONSE" as specified in subclause 15.2.22.

6.3.7 Procedures referenceable from other procedures

6.3.7.1 Emergency alert and emergency communications procedures

6.3.7.1.1 Sending a SIP re-INVITE request for MCData emergency alert or emergency group communication

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

This clause is referenced from other procedures.

The controlling MCData function shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [5].

The controlling MCData function:

1) shall include an SDP offer with the media parameters as currently established with the terminating MCData client according to 3GPP TS 24.229 [5];

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdata-calling-user-id> element set to the MCData ID of the initiating MCData user;

3) if the in-progress emergency group state of the group is set to a value of "true" the controlling MCData function:

   a) shall include a Resource-Priority header field with the namespace populated with the values for an MCData emergency group communication as specified in subclause 6.3.7.1.4;

   b) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body the <emergency-ind> element set to a value of "true"; and

   c) if the <alert-ind> element is set to "true" in the received SIP re-INVITE request and MCData emergency alerts are authorised for this group and MCData user as determined by the procedures of subclause 6.3.7.2.1, shall populate the application/vnd.3gpp.mcdata-info+xml MIME body and application/vnd.3gpp.mcdata-location-info+xml MIME body as specified in subclause 6.3.7.1.3. Otherwise, shall set the <alert-ind> element to a value of "false" in the application/vnd.3gpp.mcdata-info+xml MIME body;

4) if the in-progress emergency group state of the group is set to a value of "false":

   a) shall include a Resource-Priority header field populated with the values for a normal MCData group communication as specified in subclause 6.3.7.1.4; and

   b) if the received SIP re-INVITE request contained an application/vnd.3gpp.mcdata-info+xml MIME body with the <emergency-ind> element set to a value of "false" and this is an authorised request to cancel an MCData emergency group communication as determined by the procedures of subclause 6.3.7.2.3:

      i) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <emergency-ind> element set to a value of "false"; and

      ii) if the received SIP re-INVITE request contained an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "false" and this is an authorised request to cancel an MCData emergency alert as determined by the procedures of subclause 6.3.7.2.2, shall:

         A) include in the application/vnd.3gpp.mcdata-info+xml MIME body an <alert-ind> element set to a value of "false"; and

         B) if the received SIP request contains an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP re-INVITE request.

6.3.7.1.2 Generating a SIP MESSAGE request for notification of in-progress emergency status change

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

This clause is referenced from other procedures.

This clause describes the procedures for generating a SIP MESSAGE request to notify affiliated but not participating members of an MCData group of the change of status of the in-progress emergency state or emergency alert status of an MCData group. The procedure is initiated by the controlling MCData function when there has been a change of in-progress emergency or the emergency alert status of an MCData group.

The controlling MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

4) shall set the Request-URI to the address of the terminating participating function associated with the MCData ID of the targeted MCData user;

5) shall include a P-Asserted-Identity header field set to the public service identity of controlling MCData function;

6) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7];

7) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-request-uri> element set to the value of the MCData ID of the targeted MCData user; and

8) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body an <mcdata-calling-group-id> element set to the MCData group ID of the MCData group on which the MCData emergency communication or the emergency alert state has changed.

6.3.7.1.3 Populate mcdata-info and location-info MIME bodies for emergency alert

This clause is referenced from other procedures.

This clause describes the procedures for populating the application/vnd.3gpp.mcdata-info+xml and application/vnd.3gpp.mcdata-location-info+xml MIME bodies for an MCData emergency alert. The procedure is initiated by the controlling MCData function when it has received a SIP request initiating an MCData emergency alert and generates a message containing the MCData emergency alert information required by 3GPP TS 23.282 [2].

The controlling MCData function:

1) shall include, if not already present, an application/vnd.3gpp.mcdata-info+xml MIME body as specified in Annex D.1, and set the <alert-ind> element to a value of "true";

2) shall determine the value of the MCData user's Mission Critical Organization from the <MissionCriticalOrganization> element, of the MCData user profile document identified by the MCData ID and profile index associated with MCData user (see the MCData user profile document in 3GPP TS 24.484 [12]);

3) shall include in the <mcdatainfo> element containing the <mcdata-Params> element an <mc-org> element set to the value of the MCData user's Mission Critical Organization; and

4) shall copy the contents of the application/vnd.3gpp.mcdata-location-info+xml MIME body in the received SIP request into an application/vnd.3gpp.mcdata-location-info+xml MIME body included in the outgoing SIP request.

6.3.7.1.4 Retrieving Resource-Priority header field values for emergency communications

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

This clause is referenced from other procedures.

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [67] for an MCData emergency communication, the controlling MCData function:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]).

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [67] for a normal MCData communication, the controlling MCData function:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]).

NOTE: The "normal" Resource-Priority header field value is needed to return to a normal priority value from a priority value adjusted for an MCData emergency communication. The "normal" priority received from the EPS by use of the "normal" Resource-Priority header field value is expected to be the same as the "normal" priority received from the EPS when initiating a communication with no Resource-Priority header field included.

6.3.7.1.5 Generating a SIP MESSAGE request to indicate successful receipt of an emergency alert or emergency cancellation

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

This clause is referenced from other procedures.

This clause describes the procedures for generating a SIP MESSAGE request to notify the originator of an emergency alert or emergency cancellation that the request was successfully received.

The controlling MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

4) shall set the Request-URI to the address of the terminating participating function associated with the MCData ID of the targeted MCData user;

5) shall include a P-Asserted-Identity header field set to the public service identity of controlling MCData function; and

6) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-request-uri> element set to the value of the MCData ID of the targeted MCData user.

6.3.7.2 Authorisations

6.3.7.2.1 Determining authorisation for initiating an MCData emergency alert

If the controlling MCData function has received a SIP request targeted to an MCData group with the <alert-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body set to a value of "true", the controlling MCData function shall check the following conditions:

1) if the <allow-activate-emergency-alert> element of the <actions> element of a <rule> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "true":

   a) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCData-group-call> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "DedicatedGroup" and:

      i) if the MCData group identity targeted for the emergency alert is contained in the <uri-entry> element of the <entry> element of the <EmergencyAlert> element contained within the <MCData-group-call> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

ii) if the <allow-MCData-emergency-alert> element of the <actions> element of a <rule> element of the <ruleset> element of the <list-service> element of the group document identified by the MCData group identity is set to a value of "true" as specified in 3GPP TS 24.481 [11]; or

b) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCData-group-call> element of the MCData user profile (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "UseCurrentlySelectedGroup" and the <allow-MCData-emergency-alert> element of the <actions> element of a <rule> element of the <ruleset> element of the <list-service> element of the group document identified by the MCData group identity targeted for the emergency alert is set to a value of "true" as specified in 3GPP TS 24.481 [11];

then the MCData emergency alert request shall be considered to be an authorised request for an MCData emergency alert targeted to a MCData group. In all other cases, the MCData emergency alert request shall be considered to be an unauthorised request for an MCData emergency alert targeted to an MCData group.

If the controlling MCData function has received a SIP request targeted to an MCData user with the <alert-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body set to a value of "true", the controlling MCData function shall check the following conditions:

1) if the <allow-activate-emergency-alert> element of the <actions> element of the <rule> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "true"; and

a) if the "entry-info" attribute of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "UsePreConfigured" and the MCData ID of the MCData user targeted for the communication is contained in the <uri-entry> element of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element (see the MCData user profile document in 3GPP TS 24.484 [12]); or

b) if the "entry-info" attribute of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "LocallyDetermined";

then the MCData emergency alert request shall be considered to be an authorised request for an MCData emergency alert targeted to an MCData user. In all other cases, it shall be considered to be an unauthorised request for an MCData emergency alert targeted to an MCData user.

6.3.7.2.2 Determining authorisation for cancelling an MCData emergency alert

If the controlling MCData function has received a SIP request with the <alert-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "true", then the MCData emergency alert cancellation request shall be considered to be an authorised request for an MCData emergency alert cancellation; and

2) if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "false", then the MCData emergency alert cancellation request shall be considered to be an unauthorised request for an MCData emergency alert cancellation.

6.3.7.2.3 Determining authorisation for cancelling an MCData emergency communication

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

If the controlling MCData function has received a SIP request for an MCData group communication with the <emergency-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-group-emergency> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in

3GPP TS 24.484 [12]) is set to a value of "true", then the MCData emergency communication cancellation request shall be considered to be an authorised request for an MCData emergency group communication cancellation; and

2) If the <allow-cancel-group-emergency> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "false", then the MCData emergency group communication cancellation request shall be considered to be an unauthorised request for an MCData emergency group communication cancellation.

If the controlling MCData function has received a SIP request for an MCData private communication with the <emergency-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-private-emergency-call> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "true", then the MCData emergency private communication cancellation request shall be considered to be an authorised request for an MCData emergency private communication cancellation; and

2) if the <allow-cancel-private-emergency-call> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index of the calling user (see the MCData user profile document in 3GPP TS 24.484 [12]) is set to a value of "false" or not present, then the MCData emergency private communication cancellation request shall be considered to be an unauthorised request for an MCData emergency private communication cancellation.

6.4 Handling of MIME bodies in a SIP message

The MCData client and the MCData server shall support several MIME bodies in SIP requests and SIP responses.

When the MCData client or the MCData server sends a SIP message and the SIP message contains more than one MIME body, the MCData client or the MCData server:

1) shall, as specified in IETF RFC 2046 [21], include one Content-Type header field with the value set to multipart/mixed and with a boundary delimiter parameter set to any chosen value;

2) for each MIME body:

   a) shall insert the boundary delimiter;

   b) shall insert the Content-Type header field with the MIME type of the MIME body; and

   c) shall insert the content of the MIME body;

3) shall insert a final boundary delimiter; and

4) if an SDP offer or an SDP answer is one of the MIME bodies, shall insert the application/sdp MIME body as the first MIME body.

NOTE: The reason for inserting the application/sdp MIME body as the first body is that if a functional entity in the underlying SIP core does not understand multiple MIME bodies, the functional entity will ignore all MIME bodies with the exception of the first MIME body. The order of multiple MCData application MIME bodies in a SIP message is irrelevant.

When the MCData client or the MCData server sends a SIP message and the SIP message contains only one MIME body, the MCData client or the MCData server:

1) shall include a Content-Type header field set to the MIME type of the MIME body; and

2) shall insert the content of the MIME body.

6.5 Confidentiality and Integrity Protection of sensitive XML content

6.5.1 General

6.5.1.1 Applicability and exclusions

The procedures in subclauses 6.5 apply in general to all procedures described in clause 9, clause 10, clause 12 and clause 13 with the exception that the confidentiality and integrity protection procedures for the registration and service authorisation procedures are described in clause 7.

6.5.1.2 Performing XML content encryption

Whenever the MCData UE includes XML elements or attributes pertaining to the data specified in subclause 4.6 in SIP requests or SIP responses, the MCData UE shall perform the procedures in subclause 6.5.2.3.1.

Whenever the MCData server includes XML elements or attributes pertaining to the data specified in subclause 4.6 in SIP requests or SIP responses, the MCData server shall perform the procedures in subclause 6.5.2.3.2, with the exception that when the MCData server receives a SIP request with XML elements or attributes in an MIME body that need to be copied from the incoming SIP request to an outgoing SIP request without modification, the MCData server shall perform the procedures specified in subclause 6.5.2.5.

NOTE: The procedures in subclause 6.5.2.3.1 and subclause 6.5.2.3.2 first determine (by referring to configuration) if confidentiality protection is enabled and then call the necessary procedures to encrypt the contents of the XML elements if confidentiality protection is enabled.

6.5.1.3 Performing integrity protection on an XML body

The functional entity shall perform the procedures in this subclause just prior to sending a SIP request or SIP response.

1) The MCData UE shall perform the procedures in subclause 6.5.3.3.1; and

2) The MCData server shall perform the procedures in subclause 6.5.3.3.2.

NOTE: The procedures in subclause 6.5.3.3.1 and subclause 6.5.3.3.2 first determine if integrity protection of XML MIME bodies is required and then calls the necessary procedures to integrity protect each XML MIME body if integrity protection is required. Each XML MIME body has its own signature.

6.5.1.4 Verifying integrity of an XML body and decrypting XML elements

Whenever the functional entity (i.e. MCData UE or MCData server) receives a SIP request or a SIP response, the functional entity shall perform the following procedures before performing any other procedures.

1) The functional entity shall determine if integrity protection has been applied to an XML MIME body by following the procedures in subclause 6.5.3.4.1 and if integrity protection has been applied:

   a) shall use the keying information described in subclause 6.5.3.2 and the procedures described in subclause 6.5.3.4.2 to verify the integrity of the XML MIME body; and

   b) if the integrity protection checks fail shall not perform any further procedures in this clause;

2) The functional entity shall determine whether confidentiality protection has been applied to XML elements in XML MIME bodies in a SIP request or SIP response, pertaining to the data specified in subclause 4.6, by following the procedures in subclause 6.5.2.4.1, and if confidentiality protection has been applied:

   a) shall use the keying information described in subclause 6.5.2.2 along with the procedures described in subclause 6.5.2.4.2 to decrypt the received values; and

   b) if any decryption procedures fail, shall not perform any further procedures in this clause.

6.5.2 Confidentiality Protection

6.5.2.1 General

In general, confidentiality protection is applied to specific XML elements and attributes in XML MIME bodies in SIP requests and responses as specified in subclause 4.6.

Configuration for applying confidentiality protection is not selective to a specific XML element or attribute of the data described in subclause 4.6. If configuration for confidentiality protection is turned on, then all XML elements and attributes described in subclause 4.6 are confidentiality protected. If configuration for confidentiality protection is turned off, then no XML content in SIP requests and SIP responses are confidentiality protected.

6.5.2.2 Keys used in confidentiality protection procedures

Confidentiality protection uses an XPK to encrypt the data which (depending on who is the sender and who is the receiver of the encrypted information) can be a CSK or an SPK as specified in subclause 4.6. An XPK-ID (CSK-ID/SPK-ID) is used to key the XPK (CSK/SPK). It is assumed that before the procedures in this subclause are called, the CSK/CSK-ID and/or SPK/SPK-ID are available on the sender and recipient of the encrypted content as described in subclause 4.6.

The procedures in subclause 6.5.2.3 and subclause 6.5.2.4 are used with a XPK equal to the CSK and a XPK-ID equal to the CSK-ID in the following circumstances as described in 3GPP TS 33.180 [26]:

1) MCData client sends confidentiality protected content to an MCData server; and

2) MCData server sends confidentiality protected content to an MCData client.

The procedure in subclause 6.5.2.3 and subclause 6.5.2.4 are used with a XPK equal to the SPK and a XPK-ID equal to the SPK-ID when the MCData server sends confidentiality protected content to an MCData server.

6.5.2.3 Procedures for sending confidentiality protected content

6.5.2.3.1 MCData client

If the <confidentiality-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "true" or no <confidentiality-protection> element is present in the MCData Service Configuration document, then sending confidentiality protected content from the MCData client to the MCData server is enabled, and the MCData client:

1) shall use the appropriate keying information specified in subclause 6.5.2.2;

2) shall perform the procedures in subclause 6.5.2.3.3 to confidentiality protect XML elements containing the content described in subclause 4.6; and

3) shall perform the procedures in subclause 6.5.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in subclause 4.6.

If the <confidentiality-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending confidentiality protected content from the MCData client to the MCData server is disabled, and content is included in XML elements and attributes without encryption.

6.5.2.3.2 MCData server

If the <confidentiality-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "true" or no <confidentiality-protection> element is present in the MCData Service Configuration document, then sending confidentiality protected content from the MCData server to the MCData client is enabled. If the <allow-signalling-protection> element of the <protection-between-mcdata-servers> element is set to "true" in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] or no <allow-signalling-protection> element is present in the MCData Service Configuration document, then sending confidentiality protected content between MCData servers is enabled.

When sending confidentiality protected content, the MCData server:

1) shall use the appropriate keying information specified in subclause 6.5.2.2;

2) shall perform the procedures in subclause 6.5.2.3.3 to confidentiality protect XML elements containing the content described in subclause 4.6, and

3) shall perform the procedures in subclause 6.5.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in subclause 4.6.

If the <confidentiality-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending confidentiality protected content from the MCData server to the MCData client is disabled, and then content is included in XML elements and attributes without encryption.

If the <allow-signalling-protection> element of the <protection-between-mcdata-servers> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending confidentiality protected content between MCData servers is disabled, and content is included in XML elements and attributes without encryption.

6.5.2.3.3 Content Encryption in XML elements

The following procedures shall be performed by an MCData client or an MCData server:

1) perform encryption as specified in W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/ [28] subclause 4.3, using the "AES-128-GCM algorithm HMAC" as the encryption algorithm and the XPK as the key; and

2) follow the semantic for the element of the MIME body as described in Annex F of the present document, to include the encrypted content in the MIME body ensuring that the necessary XML elements required for confidentiality protection are included as specified in 3GPP TS 33.180 [26].

6.5.2.3.4 Attribute URI Encryption

The following procedures shall be performed by an MCData client or an MCData server:

1) perform encryption as specified in [aes-gcm], using the "AES-128-GCM algorithm HMAC" as the encryption algorithm and the XPK as the key, with a 96 bit randomly selected IV; and

2) replace the URI to be protected in the attribute by a URI constructed as follows:

   a) the URI schema is "sip:";

   b) the first part of the userinfo part is the base64 encoded result of the encryption of the original attribute value;

   c) the string ";iv=" is appended to the result of step b);

   d) the base64 encoding of the IV (section 5 of IETF RFC 4648 [30]) is appended to the result of step c);

   e) the string ";key-id=" is appended to the result of step d);

   f) the base64 encoding of the XPK-ID according to 3GPP 33.180 [26] is appended to the result of step e);

   g) the string ";alg=128-aes-gcm" is appended to the result of step f); and

   h) the string "@" followed by the domain name for MC Services confidentiality protection as specified in 3GPP TS 23.003 [31] is appended to the result of step g).

6.5.2.4 Procedures for receiving confidentiality protected content

6.5.2.4.1 Determination of confidentiality protected content

The following procedure is used by the MCData client or MCData server to determine if an XML element is confidentiality protected.

1) if an XML element contains the <EncryptedData> XML element, then the content of the XML element is confidentiality protected; and

2) if an XML element does not contain the <EncryptedData> XML element, then the content of the XML element is.not confidentiality protected.

The following procedure is used by the MCData client or MCData server to determine if a URI in the XML attribute is confidentiality protected.

1) if an XML attribute is a URI with the domain name for MC Services confidentiality protection as specified in the 3GPP TS 23.003 [31], then the URI is confidentiality protected; and

2) if an XML attribute is a URI without the domain name for MC Services confidentiality protection as specified in the 3GPP TS 23.003 [31], then the URI is not confidentiality protected.

6.5.2.4.2 Decrypting confidentiality protected content in XML elements

The following procedure shall be performed by an MCData client or an MCData server to decrypt an individual XML element that has a type of "encrypted" within an XML MIME body:

1) if the <EncryptedData> XML element or any of its sub-elements as described in 3GPP TS 33.180 [26] are not present in the MIME body then send a SIP 403 (Forbidden) response with the warning text set to "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.4, and exit this procedure. Otherwise continue with the rest of the steps;

2) perform decryption on the <EncryptedData> element as specified in W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/ [28] subclause 4.4 to decrypt the contents of the <CipherValue> element contained within the <CipherData> element;

3) if the decryption procedure fails, then send a SIP 403 (Forbidden) response with the warning text set to "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.4. Otherwise continue with the rest of the steps; and

4) return success of this procedure together with the decrypted XML element.

6.5.2.4.3 Decrypting confidentiality protected URIs in XML attributes

The following procedure shall be performed by an MCData client or an MCData server to decrypt a URI in an attribute in a XML document:

1) the value between ";iv=" and the next ";" provides the base64 encoded value of the 96 bit IV and the value between ";=key-id" and the next ";" defines the key which has been used for encryption, i.e. "CSK" or "SPK"; and

2) the original URI is obtained by decrypting the base64 encoded string between the "sip:" URI prefix and the next ";" using the "AES-128-GCM algorithm HMAC" as the decryption algorithm with IV and key as determined in step 1). This value replaces the encrypted URI as the value of the XML attribute.

6.5.2.5 MCData server copying received XML content

The following procedure is executed when an MCData server receives a SIP request containing XML MIME bodies, where the content needs to be copied from the incoming SIP request to the outgoing SIP request.

The MCData server:

1) shall copy the XML elements from the XML MIME body of the incoming SIP request that do not contain a <EncryptedData> XML element, to the same XML body in the outgoing SIP request;

2) for each encrypted XML element in the XML MIME body of the incoming SIP request as determined by subclause 6.5.2.4.1:

   a) shall use the keying information described in subclause 6.5.2.2 to decrypt the content within the XML element by following the procedures specified in subclause 6.5.2.4.2, and shall continue with the steps below if the encrypted XML element was successfully decrypted;

   b) if confidentiality protection is enabled as specified in subclause 6.5.2.3.2, then for each decrypted XML element:

i) shall re-encrypt the content within the XML element using the keying information described in subclause 6.5.2.2 and by following the procedures specified in subclause 6.5.2.3.3; and

ii) shall include the re-encrypted content into the same XML MIME body of the outgoing SIP request; and

c) if confidentiality protection is disabled as specified in subclause 6.5.2.3.2, shall include the decrypted content in the same XML MIME body of the outgoing SIP request.

3) for each encrypted XML URI attribute in the XML MIME body of the incoming SIP request as determined by subclause 6.5.2.4.1:

a) shall use the keying information described in subclause 6.5.2.2 to decrypt the URI value of the XML attribute by following the procedures specified in subclause 6.5.2.4.3, and shall continue with the steps below if the encrypted XML attribute value was successfully decrypted;

b) if confidentiality protection is enabled as specified in subclause 6.5.2.3.2, then for each decrypted XML element:

i) shall re-encrypt the URI value of the XML attribute using the keying information described in subclause 6.5.2.2 and by following the procedures specified in subclause 6.5.2.3.4; and

ii) shall include the re-encrypted attribute value into the same XML MIME body of the outgoing SIP request; and

c) if confidentiality protection is disabled as specified in subclause 6.5.2.3.2, shall include the decrypted value in the same XML MIME body of the outgoing SIP request.

6.5.3 Integrity Protection of XML documents

6.5.3.1 General

Integrity protection can be applied to a whole XML MIME body. When integrity protection is enabled, all XML MIME bodies transported in SIP requests and responses are integrity protected. The following XML MIME bodies used in the present specification in SIP signalling can be integrity protected:

- application/vnd.3gpp.mcdata-info+xml;
- application/vnd.3gpp.mcdata-mbms-usage-info+xml;
- application/vnd.3gpp.mcdata-location-info+xml;
- application/poc-settings+xml;
- application/resources-list+xml; and
- application/vnd.3gpp.mcdata-affiliation-command+xml.

If integrity protection is enabled, and one or more of the XML MIME bodies complying to the types listed above are included in a SIP request or SIP response, then a MIME body of type application/vnd.3gpp.mcptt-signed+xml specified in 3GPP TS 24.379 [10] is included in the SIP request or SIP response containing one or more signatures pointing to those XML MIME bodies as illustrated in Figure 6.5.3.1-1.

In order to integrity protect the XML MIME bodies listed above in this subclause in SIP requests and SIP responses, the MCData client and MCData server shall, for each MIME body, include the Content-ID header field as specified in IETF RFC 2045 [32] containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [33].

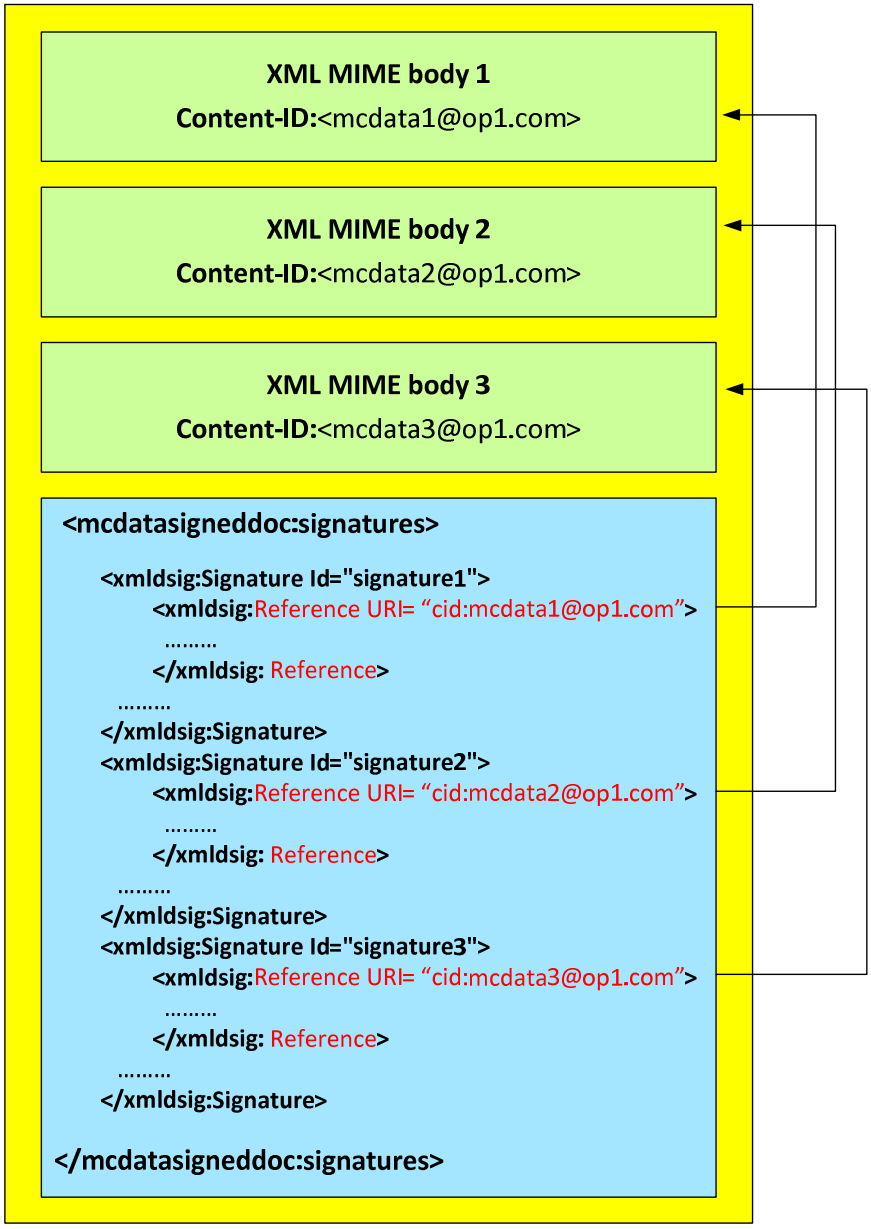

Figure 6.5.3.1-1: Integrity Protection of XML MIME bodies in SIP requests and SIP responses

Each MIME body that is integrity protected is assigned a unique signature.

Configuration for applying integrity protection is not selective to a specific MIME body. If configuration for integrity protection is turned on, then all XML MIME bodies in SIP requests and responses are integrity protected. If configuration for integrity protection is turned off, then no XML MIME bodies in SIP requests and SIP responses are integrity protected.

6.5.3.2 Keys used in integrity protection procedures

Integrity protection uses an XPK to sign the data which (depending on who is the sender and who is the receiver of the signed information) can be a CSK or an SPK as specified in subclause 4.6. An XPK-ID (CSK-ID/SPK-ID) is used to key the XPK (CSK/SPK). It is assumed that before the procedures in subclause 6.5.3.3 and subclause 6.5.3.4 are called, the CSK/CSK-ID and/or SPK/SPK-ID are available on the sender and recipient of the integrity protected content, as described in subclause 4.6.

The procedures in subclause 6.5.3.3 and subclause 6.5.3.4 shall be used with a XPK equal to the CSK and a XPK-ID equal to the CSK-ID in the following circumstances as described in 3GPP TS 33.180 [26]:

1) MCData client sends integrity protected content to an MCData server; and

2) MCData server sends integrity protected content to an MCData client.

The procedure in subclause 6.5.3.3 and subclause 6.5.3.4 shall be used with a XPK equal to the SPK and a XPK-ID equal to the SPK-ID when the MCData server sends integrity protected content to an MCData server

6.5.3.3 Sending integrity protected content

6.5.3.3.1 MCData client

If the <integrity-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "true" or no <integrity-protection> element is present in the MCData Service Configuration document, then sending integrity protected content from the MCData client to the MCData server is enabled, and the MCData client shall use the appropriate keying information specified in subclause 6.5.3.2 and shall perform the procedures in subclause 6.5.3.3.3 to integrity protect XML MIME bodies.

NOTE: Each XML MIME body is integrity protected separately.

If the <integrity-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending integrity protected content from the MCData client to the MCData server is disabled, and all XML MIME bodies are sent without integrity protection.

6.5.3.3.2 MCData server

If the <integrity-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "true", or no <integrity-protection> element is present in the MCData Service Configuration document, then sending integrity protected content from the MCData server to the MCData client is enabled. If the <allow-signalling-protection> element of the <protection-between-mcdata-servers> element is set to "true" in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] or no <allow-signalling-protection> element is present in the MCData Service Configuration document, then sending integrity protected content between MCData servers is enabled.

When sending integrity protected content, the MCData server shall use the appropriate keying information specified in subclause 6.5.3.2 and shall perform the procedures in subclause 6.5.3.3.3 to integrity protect XML MIME bodies.

NOTE: Each XML MIME body is integrity protected separately.

If the <integrity-protection> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending integrity protected content from the MCData server to the MCData client is disabled, and all XML MIME bodies are sent without integrity protection.

If the <allow-signalling-protection> element of the <protection-between-mcdata-servers> element in the MCData Service Configuration document as specified in 3GPP TS 24.484 [12] is set to "false", then sending integrity protected content between MCData servers is disabled, and content is included in XML elements without encryption.

6.5.3.3.3 Integrity protection procedure

The following procedure shall be performed by the MCData client and MCData server to integrity protect the XML bodies defined by the MIME types listed in subclause 6.5.3.1:

1) include a Content-Type header field set to "application/vnd.3gpp.mcptt-signed+xml" defined in 3GPP TS 24.379 [10];

2) for each of the MIME types defined in subclause 6.5.3.1 where the content defined by these MIME types is to be integrity protected:

   a) perform reference generation as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [29] subclause 3.1.1 using the SHA256 algorithm to produce a hash of the MIME body and continue with the procedures below if reference generation is successful;

   b) perform signature generation as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [29] subclause 3.1.2 using the HMAC-SHA256 signature method and the XPK as the key and continue with the procedures below if signature generation is successful; and

3) follow the schema defined in Annex F.6.2 and the semantic described in Annex F.6.3 to create the application/vnd.3gpp.mcptt-signed+xml MIME body, defined in 3GPP TS 24.379 [10], containing signatures referring to the XML MIME bodies included in the SIP request or SIP response.

6.5.3.4 Receiving integrity protected content

6.5.3.4.1 Determination of integrity protected content

The following procedure is used by the MCData client or MCData server to determine if an XML MIME body is integrity protected.

1) if the <Signature> XML element is not present in the XML MIME body, then the content is not integrity protected; and

2) if the <Signature> XML element is present in the XML MIME body, then the content is integrity protected.

6.5.3.4.2 Verification of integrity protected content

The following procedure is used by the MCData client or MCData server to verify the integrity of an XML MIME body:

1) if the required sub-elements of the <Signature> as described in 3GPP TS 33.180 [26] are not present in the MIME body and if not present, are not known to the sender and recipient by other means, then the integrity protection procedure fails and exit this procedure. Otherwise continue with the rest of the steps;

2) perform reference validation on the <Reference> element as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [29] subclause 3.2.1;

3) if reference validation fails, then send a SIP 403 (Forbidden) response towards the functional entity with the warning text set to: "139 integrity protection check failed" in a Warning header field as specified in subclause 4.4, and do not continue with the rest of the steps in this subclause;

4) obtain the XPK using the XPK-ID in the received XML body and use it to perform signature validation of the value of the <SignatureValue> element as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [29] subclause 3.2.2;

5) if signature validation fails, then send a SIP 403 (Forbidden) response towards the functional entity with the warning text set to: "139 integrity protection check failed" in a Warning header field as specified in subclause 4.4, and do not continue with the rest of the steps in this subclause; and

6) return success of the integrity protection of the XML document passes the integrity protection procedure.

6.6 Confidentiality and Integrity Protection of TLV messages

6.6.1 General

Signalling plane provides confidentiality and integrity protection for the MCData Data signalling and MCData Data messages sent over the signalling plane. Signalling plane security also provides the authentication of MCData Data messages.

The signalling plane security is based on 3GPP MCData security solution including key management and end-to-end protection as defined in 3GPP TS 33.180 [26].

Various keys and associated key identifiers protect the MCData Data signalling and MCData Data messages carried on the signalling plane.

The MCData Data signalling messages may be:

1. SDS SIGNALLING PAYLOAD;

2. FD SIGNALLING PAYLOAD;

3. SDS NOTIFICATION;
4. FD NOTIFICATION;
5. FD NETWORK NOTIFICATION;
6. COMMUNICATION RELEASE;
7. SDS OFF-NETWORK MESSAGE; or
8. SDS OFF-NETWORK NOTIFICATION.

The MCData Data messages may be:

1. DATA PAYLOAD.

In an on-network MCData communication for an MCData group, if protection of MCData Data messages is negotiated, the GMK and the GMK-ID of the MCData group protect the MCData Data messages sent and received by MCData clients;

In an on-network one-to-one MCData communications, if protection of MCData Data messages is negotiated, the PCK and the PCK-ID protect the MCData Data messages sent and received by MCData clients;

If protection of MCData Data signalling messages sent using unicast between the MCData client and the participating MCData function serving the the MCData client is negotiated, the CSK and the CSK-ID protect the MCData Data signalling messages sent and received using unicast by the MCData client and by a participating MCData function;

If protection of MCData Data signalling messages between the participating MCData function and the controlling MCData function is configured, the SPK and the SPK-ID protect the MCData Data signalling messages sent and received between the participating MCData function and the controlling MCData function; and

If protection of MCData is configured for an on-network MBMS MCData communication, a MuSiK and the corresponding MuSiK-ID may be used to protect transmissions on an MBMS bearer to and from MCData clients.

The GMK and the GMK-ID are distributed to the MCData clients using the group document subscription and notification procedure specified in 3GPP TS 24.481 [11].

The PCK and the PCK-ID are generated by the MCData client initiating the standalone SDS using signalling control plane or standalone one-to-one SDS using media plane or one-to-one SDS session or one-to-one FD using media plane and provided to the MCData client receiving the SIP signalling.

The CSK and the CSK-ID are generated by the MCData client and provided to the participating MCData function serving the MCData client using SIP signalling.

The SPK and the SPK-ID are configured in the participating MCData function and the controlling MCData function.

The MuSiK and the MuSiK-ID are distributed to the MCData clients as described in clause 19.

The key material for creating and verifying the authentication signature (SSK, PVT and KPAK) is provisioned to the MCData clients by the KMS as specified in 3GPP TS 33.180 [26].

6.6.2 Derivation of master keys for media and media control

Each MCData Payload Protection Key (DPPK) (i.e. GMK, PCK, CSK, SPK) and its associated key identifier DPPK-ID (i.e. GMK-ID, PCK-ID, CSK-ID, SPK -ID) described in subclause 6.6.1 are used to derive a MCData Payload Cipher Key (DPCK) and its associated DPCK-ID as specified in 3GPP TS 33.180 [26].

DPCK and DPCK-ID are used in the protection of MCData Data signalling and MCData Data messages as specified in 3GPP TS 33.180 [26].

6.6.3 Protection of MCData Data signalling and MCData Data messages

6.6.3.1 General

The MCData Data messages may be encrypted and integrity protected. When encryption is applied the media shall be encrypted as specified in subclause 8.5.4 in 3GPP TS 33.180 [26].

The MCData Data signalling messages may be protected by encryption. When encryption is applied the MCData Data signalling shall be encrypted as specified in subclause 8.5.4 in 3GPP TS 33.180 [26].

The MCData Data messages and the protected MCData Data messages may also be end-to-end authenticated as specified in subclause 8.5.5 in 3GPP TS 33.180 [15].

6.6.3.2 The MCData client

A MCData client transmitting MCData Data messages shall protect the MCData Data messages using the related DPPK and DPPK-ID according to the negotiatd protection method. For one-to-one communications PCK and PCK-ID shall be used as DPPK and DPPK-ID. For group communications GMK and GMK-ID shall be used as DPPK and DPPK-ID.

A MCData client transmitting MCData Data messages shall use the key material provisioned by the KMS when generating the authentication signature.

A MCData client which receives protected MCData Data messages shall decrypt and authenticate the protected MCData Data messages using the related DPPK and DPPK-ID according to the negotiated protection method.

A MCData client which receives signed MCData Data messages shall verify the signature using the signature, the identity of the originating MCData client and the KPAK provisioned by the KMS.

A MCData client transmitting MCData Data signalling messages shall encrypt the MCData Data signalling messages using CPK and CPK-ID if MCData Data signalling messages protection is negotiated.

A MCData client which receives encrypted MCData Data signalling messages shall decrypt the media control using CPK and CPK-ID.

6.6.3.3 The participating MCData function

A participating MCData function which receives protected MCData Data messages shall forward it to the next entity without any additional action related to the security framework.

A participating MCData function, when receiving an encrypted MCData Data signalling messages from a MCData client shall decrypt the encrypted MCData Data signalling messages using the CSK and CSK-ID negotiated with the MCData client which has sent the MCData Data signalling message. Then, the participating MCData function shall forward the MCData Data signalling messages to the controlling MCData function by encrypting the MCData Data signalling messages using SPK and SPK-ID, if protection is configured between the participating MCData function and the controlling MCData function.

A participating MCData function, when receiving an encrypted MCData Data signalling messages from the controlling MCData function shall decrypt the encrypted MCData Data signalling messages using the SPK and SPK-ID configured between the participating MCData function and the controlling MCData function. Then, the participating MCData function shall forward the MCData Data signalling messages to the destination MCData client using the CSK and CSK-ID if protection is negotiated between the participating MCData function and the MCData client.

6.6.3.4 The controlling MCData function

A controlling MCData function which receives protected MCData Data messages shall forward it to the next entity without any additional action related to the security framework.

A controlling MCData function, when receiving an encrypted MCData Data signalling messages from a participating MCData function shall decrypt the encrypted MCData Data signalling messages using the SPK and SPK-ID configured between the participating MCData function and the controlling MCData function. Then, the controlling MCData function shall forward the MCData Data signalling messages to the participating MCData function serving the

destination MCData client by encrypting the MCData Data signalling messages using SPK and SPK-ID, if protection is configured between the participating MCData function and the controlling MCData function.

7 Registration and service authorisation

7.1 General

This clause describes the procedures for SIP registration and MCData service authorization for the MCData client and the MCData service. The MCData UE can use SIP REGISTER or SIP PUBLISH for MCData service settings to perform service authorization for MCData. The decision which method to use is based on implementation and on availability of an access-token received as outcome of the user authentication procedure as described in 3GPP TS 24.482 [24].

If another MC service client (e.g. MCPTT, MCVideo) is operating at the same time on the same MC UE as the MCData client, then the MCData client shares the same SIP registration as the other MC service clients. The SIP REGISTER procedures in this clause are combined with the SIP REGISTER procedures for the other operating MC service clients to create a single SIP REGISTER request. If other MC service clients are already operating when the MCData client registers then a re-registration is performed containing the parameters for the other operating MC services.

Although the access-token can be the same for the MCData service as for other MC services when performing service authorization for MCData along with other MC services using SIP REGISTER multipart MIME bodies for each MC service are included in the SIP REGISTER request. The MCData server can therefore receive multipart MIME bodies in the SIP REGISTER request. Multiple contact addresses (one per MC service client) can be included in a SIP REGISTER request provided they all contain the same IP address and port number (see 3GPP TS 24.229 [5] for further details of including multiple contact addresses in a single SIP REGISTER request).

If the MCData client logs off from the MCData service but other MC service clients are to remain registered the MC UE performs a re-registration as specified in 3GPP TS 24.229 [5] without the supported g.3gpp.mcdata media feature tags and the g.3gpp.icsi-ref media feature tags containing the values of the supported MCData service ICSIs in the Contact header field of the SIP REGISTER request but with the parameters for the remaining operating MC service clients.

7.2 MCData client procedures

7.2.1 SIP REGISTER request for service authorisation

When the MCData client performs SIP registration for service authorisation the MCData client shall perform the registration procedures as specified in 3GPP TS 24.229 [5].

The MCData client shall include the following media feature tags in the Contact header field of the SIP REGISTER request:

1) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata";
2) if SDS is supported then:
   a) the g.3gpp.mcdata.sds media feature tag; and
   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds"; and
3) if FD service is supported then:
   a) the g.3gpp.mcdata.fd media feature tag; and
   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd".

NOTE 1: If the MCData client logs off from the MCData service but the MCData UE remains registered the MCData UE performs a re-registration as specified in 3GPP TS 24.229 [5] without the supported g.3gpp.mcdata media feature tags and the g.3gpp.icsi-ref media feature tag containing the supported MCData service ICSIs in the Contact header field of the SIP REGISTER request.

If the MCData client, upon performing SIP registration:

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [24];

2) has available an access-token;

3) based on implementation decides to use SIP REGISTER for service authorization;

4) confidentiality protection is disabled as specified in subclause 6.5.2.3.1; and

5) integrity protection is disabled as specified in subclause 6.5.3.3.1;

then the MCData client shall include an application/vnd.3gpp.mcdata-info+xml MIME body as defined in Annex F.1 with the <mcdata-access-token> element set to the value of the access token received during the user authentication procedures, in the SIP REGISTER request.

NOTE 2: the access-token contains the MCData ID of the user.

If the MCData client, upon performing SIP registration:

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [24];

2) has an available access-token;

3) based on implementation decides to use SIP REGISTER for service authorization; and

4) either confidentiality protection is enabled as specified in subclause 6.5.2.3.1 or integrity protection is enabled as specified in subclause 6.5.3.3.1;

then the MCData client:

1) shall include an application/mikey MIME body with the CSK as MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [26] in the body of the SIP REGISTER request;

2) if confidentiality protection is enabled as specified in subclause 6.5.2.3.1, shall encrypt the received access-token using the CSK and shall include in the body of the SIP REGISTER request, an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdata-access-token> element set to the encrypted access-token, as specified in subclause 6.5.3.3.1;

3) if confidentiality protection is disabled as specified in subclause 6.5.2.3.1, shall include an application/vnd.3gpp.mcdata-info+xml MIME body as defined in Annex F.1 with the <mcdata-access-token> element set to the value of the access token received during the user authentication procedures; and

4) if integrity protection is enabled as specified in subclause 6.5.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcdata-info+xml MIME body by following the procedures in subclause 6.6.3.3.3.

7.2.1AA SIP REGISTER request without service authorisation

When the MCData client performs SIP registration without service authorisation the MCData client shall perform the registration procedures as specified in 3GPP TS 24.229 [4].

The MCData client shall include the following media feature tags in the Contact header field of the SIP REGISTER request:

1) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata";

2) if SDS is supported then:

   a) the g.3gpp.mcdata.sds media feature tag; and

b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds"; and

3) if FD service is supported then:

a) the g.3gpp.mcdata.fd media feature tag; and

b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd".

NOTE: If the MCData client logs off from the MCData service but the MCData UE remains registered the MCData UE performs a re-registration as specified in 3GPP TS 24.229 [5] without the supported g.3gpp.mcdata media feature tags and the g.3gpp.icsi-ref media feature tag containing the supported MCData service ICSIs in the Contact header field of the SIP REGISTER request.

7.2.1A Common SIP PUBLISH procedure

This procedure is only referenced from other procedures.

When populating the SIP PUBLISH request, the MCData client shall:

1) shall set the Request-URI to the public service identity identifying the participating MCData function serving the MCData user;

2) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

3) shall set the Event header field to the "poc-settings" value; and

4) shall set the Expires header field according to IETF RFC 3903 [34], to 4294967295, if the MCData user is not removing the MCData service settings, otherwise to remove the MCData service settings the MCData client shall set the Expires header field to zero.

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

NOTE 2: The expiration timer of the MCData client service settings is only applicable for the MCData client service settings from the MCData client that matches the Instance Identifier URN. The expiration timer of MCData user service settings is also updated in the MCData server if expiration timer of MCData client service settings is updated in the MCData server.

NOTE 3: Removing the MCData service settings by setting the Expires header field to zero, logs off the MCData client from the MCData service.

7.2.2 SIP PUBLISH request for service authorisation and MCData service settings

If based on implementation the MCData client decides to use SIP PUBLISH for MCData server settings to also perform service authorization and

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [24]; and

2) has available an access-token;

then the MCData client:

1) shall perform the procedures in subclause 7.2.1A;

2) if confidentiality protection is disabled as specified in subclause 6.5.2.3.1 and integrity protection is disabled, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcdata-info+xml MIME body as specified in Annex F.1 with the <mcdata-access-token> element set to the value of the access token received during the user authentication procedures;

3) if either confidentiality protection is enabled as specified in subclause 6.5.2.3.1 or integrity protection is enabled as specified in subclause 6.5.3.3.1 shall include an application/mikey MIME body with the CSK as MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [26] in the body of the SIP PUBLISH request;

4) if confidentiality protection is enabled as specified in subclause 6.5.2.3.1, shall include in the body of the SIP PUBLISH request an application/vnd.3gpp.mcdata-info+xml MIME body with:

   a) the <mcdata-access-token> element set to the received access-token encrypted using the CSK, as specified in subclause 6.5.2.3.3; and

   b) the <mcdata-client-id> element set to the encrypted MCData client ID of the originating MCData client, as specified in subclause 6.5.2.3.3;

5) if confidentiality protection is disabled as specified in subclause 6.5.2.3.1, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcdata-info+xml MIME body as specified in Annex F.1 with:

   a) the <mcdata-access-token> element set to the value of the access token received during the user authentication procedures in the body of the SIP PUBLISH request; and

   b) the <mcdata-client-id> element set to the value of the MCData client ID of the originating MCData client;

6) shall include an application/poc-settings+xml MIME body as defined in 3GPP TS 24.379 [10] containing:

   a) the <selected-user-profile-index> element set to the value contained in the "user-profile-index" attribute of the selected MCData user profile as defined in 3GPP TS 24.484 [12]; and

7) if integrity protection is enabled as specified in subclause 6.5.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcdata-info+xml MIME body and application/poc-settings+xml MIME body by following the procedures in subclause 6.5.3.3.3.

The MCData client shall send the SIP PUBLISH request according to 3GPP TS 24.229 [5].

7.2.3 Sending SIP PUBLISH for MCData service settings only

To set, update, remove or refresh the MCData service settings, the MCData client shall generate a SIP PUBLISH request according 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 4354 [35]. In the SIP PUBLISH request, the MCData client:

1) shall perform the procedures in subclause 7.2.1A;

2) if confidentiality protection is enabled as specified in subclause 6.5.2.3.1, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcdata-info+xml MIME body with:

   a) the <mcdata-request-uri> element set to the targeted MCData ID encrypted using the CSK, as specified in subclause 6.5.2.3.3; and

   b) the <mcdata-client-id> element set to the encrypted MCData client ID of the originating MCData client, as specified in subclause 6.5.2.3.3;

3) if confidentiality protection is disabled as specified in subclause 6.5.2.3.1, shall include an application/vnd.3gpp.mcdata-info+xml MIME body as specified in Annex F.1 with:

   a) the <mcdata-request-uri> set to the cleartext targeted MCData ID; and

   b) the <mcdata-client-id> element set to the value of the MCData client ID of the originating MCData client;

4) shall include an application/poc-settings+xml MIME body as defined in 3GPP TS 24.379 [10] containing:

   a) the <selected-user-profile-index> element set to the value contained in the "user-profile-index" attribute of the selected MCData user profile as defined in 3GPP TS 24.484 [12]; and

5) if integrity protection is enabled as specified in subclause 6.5.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcdata-info+xml MIME body and application/poc-settings+xml MIME body by following the procedures in subclause 6.5.3.3.3.

The MCData client shall send the SIP PUBLISH request according to 3GPP TS 24.229 [5].

On receiving the SIP 200 (OK) response to the SIP PUBLISH request the MCData client may indicate to the MCData User the successful communication of the MCData service settings to the MCData server.

7.2.4 Determination of MCData service settings

In order to discover MCData service settings of another MCData client of the same MCData user or to verify the currently active MCData service settings of this MCData client, the MCData client shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36], and IETF RFC 4354 [35].

In the SIP SUBSCRIBE request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

4) shall set the Event header field to the 'poc-settings' value;

5) shall include an Accept header field containing the "application/poc-settings+xml" MIME type;

6) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295; and

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

7) if the MCData client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [36], to zero.

In order to re-subscribe or de-subscribe, the MCData client shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36], IETF RFC 4354 [35]. In the SIP SUBSCRIBE request, the MCData client:

1) shall set the Event header field to the 'poc-settings' value;

2) shall include an Accept header field containing the "application/poc-settings+xml" MIME type;

3) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295; and

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

4) if the MCData client wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [36], to zero.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36] and IETF RFC 4354 [35], that contains an application/poc-settings+xml MIME body the MCData client shall cache:

1) the <am-settings> element of the poc-settings+xml MIME body for each MCData client identified by the "id" attribute according to IETF RFC 4354 [35] as the current Answer-mode indication of that MPCTT client; and

2) the <selected-user-profile-index> element of the poc-settings+xml MIME body for each MCData client identified by the "id" attribute according to IETF RFC 4354 [35] as the active MCData user profile of that MCData client.

7.2.5 Receiving a CSK key download message

When the MCData client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and

2) an application/mikey MIME body;

Then, if the key identifier within the CSB-ID of the MIKEY payload is a CSK-ID (4 most-significant bits have the value '2'), the MCData client:

1) shall follow the security procedures in subclause 9.2.1 of 3GPP TS 33.180 [26] to extract the CSK. The client:

   a) if the initiator field (IDRi) has type 'URI' (identity hiding is not used), the client:

      i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]. If the initiator URI deviates from the public service identity of the participating MCData function serving the MCData user, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9.2 and shall not continue with the rest of the steps; and

      ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.180 [26];

   b) if the initiator field (IDRi) has type 'UID' (identity hiding in use), the client:

      i) shall convert the public service identity of participating MCData function serving the MCData user to a UID as described in 3GPP TS 33.180 [26]; and

      ii) shall compare the generated UID with the UID in the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]. If the two initiator UIDs deviate from each other, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9.2 and shall not continue with the rest of the steps;

   c) shall use the UID to validate the signature of the I_MESSAGE as described in 3GPP TS 33.180 [26];

   d) if authentication verification of the I_MESSAGE fails, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

   e) shall extract and decrypt the encapsulated CSK using the participating MCData function's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26];

   f) shall extract and store the algorithm to be used to protect the MCData signalling fields; and

   g) shall extract the CSK-ID, from the payload as specified in 3GPP TS 33.180 [26]; and

2) Upon successful extraction, the client shall replace the existing CSK and CSK-ID associated with the participating MCData function, with the extracted CSK and CSK-ID in the 'key download' message.

7.3 MCData server procedures

7.3.1 General

The MCData server obtains information that it needs to implement service authorization specific requirements from:

a) any received third-party SIP REGISTER request (e.g. including information contained in the body of the third-party SIP REGISTER request) as specified in 3GPP TS 24.229 [5]. The body will carry the SIP REGISTER request as sent by the MCData client and may contain information needed for service authorization; or

b) any received SIP PUBLISH request for MCData server settings containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters. The body of the SIP PUBLISH request will contain information needed for service authorization.

7.3.1A Confidentiality and Integrity Protection

When the MCData server receives a SIP REGISTER request sent from the MCData client contained within a message/sip MIME body of a received third-party SIP REGISTER request or a SIP PUBLISH request, it first determines whether XML MIME bodies included in the request are integrity protected. If XML MIME bodies are integrity protected the MCData server validates the signature of each of the XML MIME bodies. If the integrity protection check(s) pass or the XML MIME bodies are not integrity protected, the MCData server then determines whether the content in specific XML elements is confidentiality protected. If XML content is confidentiality protected, the MCData server decrypts the protected content.

Upon receiving:

- a SIP REGISTER request containing an application/vnd.3gpp.mcdata-info+xml MIME body within a message/sip MIME body of the SIP REGISTER request sent from the MCData client; or
- a SIP PUBLISH request containing an application/vnd.3gpp.mcdata-info+xml MIME body and an application/poc-settings+xml MIME body;

the MCData server:

1) shall determine if integrity protection has been applied to XML MIME bodies in the SIP request by following the procedures in subclause 6.5.3.4.1 for each XML MIME body;
2) if integrity protection has been applied, shall use the keying data described in subclause 6.5.3.2 and the procedures described in subclause 6.5.3.4.2 to verify the integrity of each of the XML MIME bodies; and
3) if all integrity protection checks succeed, shall continue with the remaining steps of this subclause.

Upon receiving:

- a SIP REGISTER request containing an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-access-token> element and an <mcdata-client-id> element within a message/sip MIME body of the SIP REGISTER request sent from the MCData client; or
- a SIP PUBLISH request containing an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-access-token> element and an <mcdata-client-id> element, and an application/poc-settings+xml MIME body;

the MCData server:

1) shall determine if confidentiality protection has been applied to the <mcdata-access-token> element and the <mcdata-client-id> element in the application/vnd.3gpp.mcdata-info+xml MIME body, by following the procedures in subclause 6.5.2.4.1;
2) if confidentiality protection has been applied to the <mcdata-access-token> element and <mcdata-client-id> element:
   a) shall use the keying information received in the MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [26], along with the procedures described in subclause 6.5.2.4.2 to:
      i) decrypt the received access token in the <mcdata-access-token> element in the application/vnd.3gpp.mcdata-info+xml MIME body; and
      ii) decrypt the received MCData client ID in the <mcdata-client-id> element in the application/vnd.3gpp.mcdata-info+xml MIME body;
   b) if the decryption procedure succeeds, shall identify the MCData ID and the MCData client ID from the decrypted values; and
   c) if the decryption procedure fails, shall determine that confidentiality protection has not been successful;
3) if confidentiality protection has been applied to only one of the <mcdata-access-token> element or the <mcdata-client-id> element:
   a) shall determine that confidentiality protection has not been successful;
4) if confidentiality protection has not been applied:

a) shall identify the MCData ID from <mcdata-access-token> element received in the application/vnd.3gpp.mcdata-info+xml MIME body; and

b) shall identify the MCData client ID from the <mcdata-client-id> element received in the application/vnd.3gpp.mcdata-info+xml MIME body.

Upon receiving a SIP PUBLISH request containing an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-request-uri> element, an <mcdata-client-id> element, and an application/poc-settings+xml MIME body, the MCData server:

1) shall determine if confidentiality protection has been applied to the <mcdata-request-uri> element and the <mcdata-client-id> element in the application/vnd.3gpp.mcdata-info+xml MIME body by following the procedures in subclause 6.5.2.4.1;

2) if confidentiality protection has been applied to the <mcdata-request-uri> element and the <mcdata-client-id> element:

   a) shall use the keying information described in subclause 6.5.2.2 along with the procedures described in subclause 6.5.2.4.2 to:

      i) decrypt the received encrypted MCData ID in the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body; and

      ii) decrypt the received encrypted MCData client ID in the <mcdata-client-id> element in the application/vnd.3gpp.mcdata-info+xml MIME body;

   b) if all decryption procedures succeed, shall identify the MCData ID and MCData client ID from the decrypted values; and

   c) if the decryption procedure fails, shall determine that confidentiality protection has not been successful;

3) if confidentiality protection has been applied to only one of the <mcdata-request-uri> element or <mcdata-client-id> element:

   a) shall determine that confidentiality protection has not been successful;

4) if confidentiality protection has not been applied:

   a) shall identify the MCData ID from the contents of the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body; and

   b) shall identify the MCData client ID from the <mcdata-client-id> element received in the application/vnd.3gpp.mcdata-info+xml MIME body.

7.3.2 SIP REGISTER request for service authorisation

The MCData server shall support obtaining service authorization specific information from the SIP REGISTER request sent from the MCData client and included in the body of a third-party SIP REGISTER request.

NOTE 1: 3GPP TS 24.229 [5] defines how based on initial filter criteria the SIP REGISTER request sent from the UE is included in the body of the third-party SIP REGISTER request.

Upon receiving a third party SIP REGISTER request with a message/sip MIME body containing the SIP REGISTER request sent from the MCData client containing an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-access-token> element and an <mcdata-client-id> element within a message/sip MIME body of the SIP REGISTER request sent from the MCData client, the MCData server:

1) shall identify the IMS public user identity from the third-party SIP REGISTER request;

2) shall identify the MCData ID from the SIP REGISTER request sent from the MCData client and included in the message/sip MIME body of the third-party SIP REGISTER request by following the procedures in subclause 7.3.1A;

2A) shall check if the number of maximum simultaneous authorizations supported for the MCData user as specified in the <max-simultaneous-authorizations> element of the <anyExt> element contained in the

<OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]) has been reached. If reached, the MCData server shall not continue with the rest of the steps in this clause;

3) shall perform service authorization for the identified MCData ID as described in 3GPP TS 33.180 [26]; and

4) if service authorization was successful, shall bind the MCData ID to the IMS public user identity.

NOTE 2: The MCData server will store the binding MCData ID, IMS public user identity and an identifier addressing the MCData server in an external database.

7.3.3 SIP PUBLISH request for service authorisation and service settings

The MCData server shall support obtaining service authorization specific information from a SIP PUBLISH request for MCData server settings.

Upon receiving a SIP PUBLISH request containing:

1) an Event header field set to the "poc-settings" value;

2) an application/poc-settings+xml MIME body; and

3) an application/vnd.3gpp.mcdata-info+xml MIME body containing an <mcdata-access-token> element and an <mcdata-client-id> element;

the MCData server:

1) shall identify the IMS public user identity from the P-Asserted-Identity header field;

2) shall perform the procedures in subclause 7.3.1A;

3) if the procedures in subclause 7.3.1A were not successful shall send a SIP 403 (Forbidden) response towards the MCData client with the warning text set to: "140 unable to decrypt XML content " in a Warning header field as specified in subclause 4.9, and not continue with the rest of the steps in this subclause;

3A) shall check if the number of maximum simultaneous authorizations supported for the MCData user as specified in the <max-simultaneous-authorizations> element of the <anyExt> element contained in the <OnNetwork> element of the MCData service configuration document (see the service configuration document in 3GPP TS 24.484 [12]) has been reached. If reached, the MCData server shall send a SIP 486 (Busy Here) response towards the MCData client with the warning text set to: "228 maximum number of service authorizations reached" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps in this clause;

4) shall perform service authorization for the identified MCData ID as described in 3GPP TS 33.180 [26];

5) if service authorization was successful, shall bind the MCData ID to the IMS public user identity;

NOTE 1: The MCData server will store the binding MCData ID, IMS public user identity and an identifier addressing the MCData server in an external database.

6) if service authorization was not successful, shall send a SIP 403 (Forbidden) response towards the MCData client with the warning text set to: "101 service authorisation failed" in a Warning header field as specified in subclause 4.9, and not continue with the rest of the steps in this subclause;

7) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [34] and if processing of the SIP request was not successful, do not continue with the rest of the steps;

8) shall cache the received MCData service settings until the MCData service settings expiration timer expires;

9) shall send a SIP 200 (OK) response according 3GPP TS 24.229 [5];

10) shall download the MCData user profile from the MCData user database as defined in 3GPP TS 29.283 [37] if not already stored at the MCData server and use the <selected-user-profile-index> element of the poc-settings event package if included to identify the active MCData user profile for the MCData client;

NOTE 2: If the <selected-user-profile-index> element of the poc-settings event package is included then only that MCData user profile is needed to be downloaded from the MCData user database.

11) if there is no <selected-user-profile-index> element included in the poc-settings event package then if multiple MCData user profiles are stored at the MCData server or downloaded for the MCData user from the MCData user database, shall determine the pre-selected MCData user profile to be used as the active MCData user profile by identifying the MCData user profile (see the MCData user profile document in 3GPP TS 24.484 [12]) in the collection of MCData user profiles that contains a <Pre-selected-indication> element; and

NOTE 3: If only one MCData user profile is stored at the MCData server or only one MCData user profile is downloaded from the MCData user database, then by default this MCData user profile is the pre-selected MCData user profile.

12) if an <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCData user profile document with one or more <entry> elements containing an MCData group ID (see the MCData user profile document in 3GPP TS 24.484 [12]) for the served MCData ID, shall perform implicit affiliation as specified in subclause 8.3.2.15.

7.3.4 Receiving SIP PUBLISH request for MCData service settings only

Upon receiving a SIP PUBLISH request containing:

1) an Event header field set to the "poc-settings" value;

2) an application/poc-settings+xml MIME body; and

3) an application/vnd.3gpp.mcdata-info+xml MIME body containing an <mcdata-request-uri> element and an <mcdata-client-id> element;

The MCData server:

1) shall identify the IMS public user identity from the P-Asserted-Identity header field;

2) shall perform the procedures in subclause 7.3.1A;

3) if the procedures in subclause 7.3.1A were not successful, shall send a SIP 403 (Forbidden) response towards the MCData client with the warning text set to: "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.9, and not continue with the rest of the steps in this subclause;

4) shall verify that a binding between the IMS public user identity in the Request-URI and the MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml exists at the MCData server;

5) if a binding exists between the IMS public user identity and the MCData ID in the request and the validity period of the binding has not expired shall download the MCData user profile from the MCData user database as defined in 3GPP TS 29.283 [37] if not already stored at the MCData server;

6) if a binding does not exist between the IMS public user identity and the MCData ID in the request or the binding exists, but the validity period of the binding has expired, shall reject the SIP PUBLISH request with a SIP 404 (Not Found) response and not continue with any of the remaining steps;

7) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [34] and if processing of the SIP request was not successful, do not continue with the rest of the steps;

8) shall cache the received MCData service settings until the MCData service settings expiration timer expires;

9) shall send a SIP 200 (OK) response according 3GPP TS 24.229 [5];

10) shall download the MCData user profile from the MCData user database as defined in 3GPP TS 29.283 [37] if not already stored at the MCData server and use the <selected-user-profile-index> element of the poc-settings event package if included to identify the active MCData user profile for the MCData client;

NOTE 1: If the <selected-user-profile-index> element of the poc-settings event package is included then only that MCData user profile is needed to be downloaded from the MCData user database.

11) if there is no <selected-user-profile-index> element included in the poc-settings event package then if multiple MCData user profiles are stored at the MCData server or downloaded for the MCData user from the MCData user database, shall determine the pre-selected MCData user profile to be used as the active MCData user profile by identifying the MCData user profile (see the MCData user profile document in 3GPP TS 24.484 [12]) in the collection of MCData user profiles that contains a <Pre-selected-indication> element; and

NOTE 2: If only one MCData user profile is stored at the MCData server or only one MCData user profile is downloaded from the MCData user database, then by default this MCData user profile is the pre-selected MCData user profile.

12) if an <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCData user profile document with one or more <entry> elements containing an MCData group ID (see the MCData user profile document in 3GPP TS 24.484 [12]) for the served MCData ID, shall perform implicit affiliation as specified in subclause 8.3.2.15.

7.3.5 Receiving SIP PUBLISH request with "Expires=0"

Upon receiving a SIP PUBLISH request containing:

1) an Event header field set to the "poc-settings" value; and

2) an Expires header field set to 0;

the MCData server:

1) shall identify the IMS public user identity from the P-Asserted-Identity header field;

2) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [34] and if processing of the SIP request was successful, continue with the rest of the steps;

3) shall remove the MCData service settings;

4) shall remove the binding between the MCData ID and public user identity; and

5) shall send a SIP 200 (OK) response according to 3GPP TS 24.229 [5].

7.3.6 Subscription to and notification of MCData service settings

7.3.6.1 Receiving subscription to MCData service settings

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the participating MCData function of the served MCData user;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element which identifies an MCData ID served by the MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata,sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

3) the Event header field of the SIP SUBSCRIBE request contains the 'poc-settings' event type.

the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

2) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the participating MCData function serving the MCData user, shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) if the originating MCData ID is different than the served MCData ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps; and

4) shall generate a 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36] and IETF RFC 4354 [35].

For the duration of the subscription, the MCData server shall notify subscriber about changes of the MCData service settings of the subscribed MCData user, as described in subclause 7.3.6.2.

7.3.6.2 Sending notification of change of MCData service settings

In order to notify the subscriber about changes of the MCData service settings of the subscribed MCData client of the subscribed MCData user, the MCData server:

1) shall generate an application/poc-settings+xml MIME body as defined in 3GPP TS 24.379 [10] containing:

   a) the <selected-user-profile-index> element identifying the active MCData user profile; and

2) send a SIP NOTIFY request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36] and IETF RFC 4354 [35] with the constructed application/poc-settings+xml MIME body.

7.3.7 Sending a CSK key download message

If confidentiality protection is enabled as specified in subclause 6.5.2.3.1, and if the participating MCData function received a Client Server Key (CSK) within a SIP REGISTER request for service authorisation or SIP PUBLISH request for service authorisation, the participating MCData function may decide to update the CSK. In this case, the participating MCData function shall perform a key download procedure for the CSK. The participating MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall set the Request-URI to the URI received in the To header field in the third-party SIP REGISTER request;

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

5) shall include an application/mikey MIME body containing the algorithm to be used to protect the MCData signalling fields, the CSK-ID and the CSK encrypted within a MIKEY message to the MC client as specified in subclause 9.2.1 of 3GPP TS 33.180 [26] in the body of the SIP MESSAGE request; and

6) shall send the SIP MESSAGE request towards the MCData client according to 3GPP TS 24.229 [5].

8 Affiliation

8.1 General

Subclause 8.2 contains the procedures for explicit affiliation at the MCData client.

Subclause 8.3 contains the procedures for explicit affiliation at the MCData server serving the MCData user and the MCData server owning the MCData group.

Subclause 8.3 contains the procedures for implicit affiliation at the MCData server serving the MCData user and the MCData server owning the MCData group.

Subclause 8.4 describes the coding used for explicit affiliation.

The procedures for implicit affiliation in this clause are triggered at the MCData server serving the MCData user in the following circumstances:

- on receipt of a SIP MESSAGE request from an MCData client when initiating an MCData emergency alert targeted to an MCData group and the MCData client is not already affiliated to the MCData group; and

- on receipt of a SIP REGISTER request for service authorisation (as described in subclause 7.3.2) or SIP PUBLISH request for service authorisation and service settings (as described in subclause 7.3.3), as determined by configuration in the MCData user profile document as specified in 3GPP TS 24.484 [12].

The procedures for implicit affiliation in this clause are triggered at the MCData server owning the MCData group in the following circumstances:

- on receipt of a SIP MESSAGE request from the MCData server serving the MCData user when the MCData user initiates an MCData emergency alert targeted to an MCData group and the MCData client is not already affiliated to the MCData group.

8.2 MCData client procedures

8.2.1 General

The MCData client procedures consist of:

- an affiliation status change procedure;
- an affiliation status determination procedure;
- a procedure for sending affiliation status change request in negotiated mode to target MCData user;
- a procedure for receiving affiliation status change request in negotiated mode from authorized MCData user; and
- a rules based affiliation status change procedure.

In order to obtain information about success or rejection of changes triggered by the affiliation status change procedure for an MCData user, the MCData client needs to initiate the affiliation status determination procedure for the MCData user before starting the affiliation status change procedure for the MCData user.

8.2.2 Affiliation status change procedure

In order:

- to indicate that an MCData user is interested in one or more MCData group(s) at an MCData client;
- to indicate that the MCData user is no longer interested in one or more MCData group(s) at the MCData client;
- to refresh indication of an MCData user interest in one or more MCData group(s) at an MCData client due to near expiration of the expiration time of an MCData group with the affiliation status set to the "affiliated" state received in a SIP NOTIFY request in subclause 8.2.3;
- to send an affiliation status change request in mandatory mode to another MCData user;
- to indicate that an MCData user is interested in one or more MCData group(s) at an MCData client triggered by a location or functional alias activation criteria;
- to indicate that the MCData user is no longer interested in one or more MCData group(s) at the MCData client client triggered by location or functional alias deactivation criteria; or
- any combination of the above;

the MCData client shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34], and IETF RFC 3856 [39].

When the MCData user indicates that he is no longer interested in one or more MCData group(s) at the MCData client, the MCData client shall first check value of the <manual-deaffiliation-not-allowed-ifaffiliation-rules-are-met> element if present within the MCData user profile document (see the MCData user profile document specified in 3GPP TS 24.484 [50]). If the affiliation to the group has been activated due to a rule being fulfilled and the <manual-deaffiliation-not-allowed-if- affiliation- rules- are-met> element is present and is set to a value of "true", the MCData client shall suppress the MCData user’s request.

NOTE 0: If the request is suppressed, a notification message can be displayed to the user.

In the SIP PUBLISH request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

4) if the targeted MCData user is interested in at least one MCData group at the targeted MCData client, shall set the Expires header field according to IETF RFC 3903 [34], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the targeted MCData user is no longer interested in any MCData group at the targeted MCData client, shall set the Expires header field according to IETF RFC 3903 [34], to zero; and

6) shall include an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 8.4.1. In the MIME body, the MCData client:

   a) shall include all MCData groups where the targeted MCData user indicates its interest at the targeted MCData client;

   b) shall include the MCData client ID of the targeted MCData client;

   c) shall not include the "status" attribute and the "expires" attribute in the <affiliation> element; and

   d) shall set the <p-id> child element of the <presence> root element to a globally unique value.

The MCData client shall send the SIP PUBLISH request according to 3GPP TS 24.229 [5].

8.2.3 Affiliation status determination procedure

NOTE 1: The MCData UE also uses this procedure to determine which MCData groups the MCData user successfully affiliated to.

In order to discover MCData groups:

1) which the MCData user at an MCData client is affiliated to; or

2) which another MCData user is affiliated to;

the MCData client shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36].

In the SIP SUBSCRIBE request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the targeted MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

4) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the MCData client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [36], to zero; and

6) shall include an Accept header field containing the application/pidf+xml MIME type; and

7) if requesting MCData groups where the MCData user is affiliated to at the MCData client, shall include an application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information according to subclause 8.4.2, indicating the MCData client ID of the MCData client.

In order to re-subscribe or de-subscribe, the MCData client shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36]. In the SIP SUBSCRIBE request, the MCData client:

1) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

2) if the MCData client wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [36], to zero; and

3) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-user affiliation information constructed according to subclause 8.4.1, then the MCData client shall determine affiliation status of the MCData user for each MCData group at the MCData client(s) in the MIME body. If the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request is included, the <p-id> element value indicates the SIP PUBLISH request which triggered sending of the SIP NOTIFY request.

8.2.4 Procedure for sending affiliation status change request in negotiated mode to target MCData user

NOTE: Procedure for sending affiliation status change request in negotiated mode to several target MCData users is not supported in this version of the specification.

Upon receiving a request from the MCData user to send an affiliation status change request in negotiated mode to a target MCData user, the MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. In the SIP MESSAGE request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the target MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

4) shall include an application/vnd.3gpp.mcdata-affiliation-command+xml MIME body as specified in Annex D.3; and

5) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

On receiving a SIP 2xx response to the SIP MESSAGE request, the MCData client shall indicate to the user that the request has been delivered to an MCData client of the target MCData user.

8.2.5 Procedure for receiving affiliation status change request in negotiated mode from authorized MCData user

Upon receiving a SIP MESSAGE request containing:

1) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

2) an application/vnd.3gpp.mcdata-affiliation-command+xml MIME body with a list of MCData groups for affiliation under the <affiliate> element and a list of MCData groups for de-affiliation under the <de-affiliate> element;

then the MCData client:

1) shall send a 200 (OK) response to the SIP MESSAGE request;

2) shall seek confirmation of the list of MCData groups for affiliation and the list of MCData groups for de-affiliation, resulting in an accepted list of MCData groups for affiliation and an accepted list of MCData groups for de-affiliation; and

3) if the user accepts the request:

   a) shall perform affiliation for each entry in the accepted list of MCData groups for affiliation for which the MCData client is not affiliated, as specified in subclause 8.2.2; and

   b) shall perform de-affiliation for each entry in the accepted list of MCData groups for de-affiliation for which the MCData client is affiliated, as specified in subclause 8.2.2.

8.2.6 Rules based affiliation status change procedure

Rules based affiliation is controlled by the elements <RulesForAffiliation> or <RulesForDeaffiliation> of the MCData user profile document identified by the MCData ID of the MCData user (see the MCData user profile document specified in 3GPP TS 24.484 [50]). The rules can be composed of location criteria (including heading and speed) or functional alias based criteria. A rule is fulfilled if any of the location criteria and any of the functional alias based criteria are met. These rules are evaluated whenever a change of location occurs and whenever a functional alias is activated or deactivated. If any defined rule is fulfilled, the MCData client shall initiate the affiliation status change procedure as specified in subclause 8.2.2.

NOTE: Hysteresis can be applied to location changes to avoid too frequent affiliation changes. In addition, the definition of area entry and exit criteria can be specified to provide a buffer space to minimize ping-ponging into and out of an area.

8.3 MCData server procedures

8.3.1 General

The MCData server procedures consist of:

- procedures of MCData server serving the MCData user; and
- procedures of MCData server owning the MCData group.

8.3.2 Procedures of MCData server serving the MCData user

8.3.2.1 General

The procedures of MCData server serving the MCData user consist of:

- a receiving affiliation status change from MCData client procedure;
- a receiving subscription to affiliation status procedure;

- a sending notification of change of affiliation status procedure;
- a sending affiliation status change towards MCData server owning MCData group procedure;
- an affiliation status determination from MCData server owning MCData group procedure;
- a procedure for authorizing affiliation status change request in negotiated mode sent to served MCData user;
- a forwarding affiliation status change towards another MCData user procedure;
- a forwarding subscription to affiliation status towards another MCData user procedure
- an affiliation status determination procedure;
- an affiliation status change by implicit affiliation procedure;
- an implicit affiliation status change completion procedure;
- an implicit affiliation status change cancellation procedure; and
- an implicit affiliation to configured groups procedure.

8.3.2.2 Stored information

The MCData server shall maintain a list of MCData user information entries. The list of the MCData user information entries contains one MCData user information entry for each served MCData ID.

In each MCData user information entry, the MCData server shall maintain:

1) an MCData ID. This field uniquely identifies the MCData user information entry in the list of the MCData user information entries; and
2) a list of MCData client information entries.

In each MCData client information entry, the MCData server shall maintain:

1) an MCData client ID. This field uniquely identifies the MCData client information entry in the list of the MCData client information entries; and
2) a list of MCData group information entries.

In each MCData group information, the MCData server shall maintain:

1) an MCData group ID. This field uniquely identifies the MCData group information entry in the list of the MCData group information entries;
2) an affiliation status;
3) an expiration time;
4) an affiliating p-id; and
5) a next publishing time.

8.3.2.3 Receiving affiliation status change from MCData client procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains either the public service identity identifying the originating participating MCData function serving the MCData user, or the public service identity identifying the terminating participating MCData function serving the MCData user;
2) the SIP PUBLISH request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element which identifies an MCData ID served by the MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 8.4.1;

then the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

2) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the originating participating MCData function serving the MCData user, shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP PUBLISH request;

3) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the terminating participating MCData function serving the MCData user, shall identify the originating MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

4) if the originating MCData ID is different than the served MCData ID and the originating MCData ID is not authorized to modify affiliation status of the served MCData ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps;

5) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

6) if the Expires header field of the SIP PUBLISH request has nonzero value, shall determine the candidate expiration interval to according to IETF RFC 3903 [34];

7) if the Expires header field of the SIP PUBLISH request has zero value, shall set the candidate expiration interval to zero;

8) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34]. In the SIP 200 (OK) response, the MCData server:

   a) shall set the Expires header field according to IETF RFC 3903 [34], to the candidate expiration time;

9) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served MCData ID, shall not continue with the rest of the steps;

10) shall identify the served MCData client ID in the "id" attribute of the <tuple> element of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request;

11) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

12) shall consider an MCData client information entry such that:

   a) the MCData client information entry is in the list of MCData client information entries of the served MCData user information entry; and

   b) the MCData client ID of the MCData client information entry is equal to the served MCData client ID;

   as the served MCData client information entry;

13) shall consider a copy of the list of the MCData group information entries of the served MCData client information entry as the served list of the MCData group information entries;

14) if the candidate expiration interval is nonzero:

a) shall construct the candidate list of the MCData group information entries as follows:

i) for each MCData group ID which has an MCData group information entry in the served list of the MCData group information entries, such that the expiration time of the MCData group information entry has not expired yet, and which is indicated in a "group" attribute of an <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

A) shall copy the MCData group information entry into a new MCData group information entry of the candidate list of the MCData group information entries;

B) if the affiliation status of the MCData group information entry is "deaffiliating" or "deaffiliated", shall set the affiliation status of the new MCData group information entry to the "affiliating" state and shall reset the affiliating p-id of the new MCData group information entry; and

C) shall set the expiration time of the new MCData group information entry to the current time increased with the candidate expiration interval;

ii) for each MCData group ID which has an MCData group information entry in the served list of the MCData group information entries, such that the expiration time of the MCData group information entry has not expired yet, and which is not indicated in any "group" attribute of the <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

A) shall copy the MCData group information entry into a new MCData group information entry of the candidate list of the MCData group information entries; and

B) if the affiliation status of the MCData group information entry is "affiliated" or "affiliating":

- shall set the affiliation status of the new MCData group information entry to the "de-affiliating" state; and

- shall set the expiration time of the new MCData group information entry to the current time increased with twice the value of timer F; and

iii) for each MCData group ID:

A) which does not have an MCData group information entry in the served list of the MCData group information entries; or

B) which has an MCData group information entry in the served list of the MCData group information entries, such that the expiration time of the MCData group information entry has already expired;

and which is indicated in a "group" element of the <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

A) shall add a new MCData group information entry in the candidate list of the MCData group information list for the MCData group ID;

B) shall set the affiliation status of the new MCData group information entry to the "affiliating" state;

C) shall set the expiration time of the new MCData group information entry to the current time increased with the candidate expiration interval; and

D) shall reset the affiliating p-id of the new MCData group information entry;

b) determine the candidate number of MCData group IDs as number of different MCData group IDs which have an MCData group information entry:

i) in the candidate list of the MCData group information entries; or

ii) in the list of the MCData group information entries of an MCData client information entry such that:

A) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry; and

B) the MCData client ID of the MCData client information entry is not equal to the served MCData client ID;

with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

c) if the candidate number of MCData group IDs is bigger than N2 value of the served MCData ID, shall based on MCData service provider policy reduce the candidate MCData group IDs to that equal to N2;

NOTE: The MCData service provider policy can determine to remove an MCData group ID based on the order it appeared in the PUBLISH request or based on the importance or priority of the MCData group or some other policy to determine which MCData groups are preferred.

15) if the candidate expiration interval is zero, constructs the candidate list of the MCData group information entries as follows:

a) for each MCData group ID which has an entry in the served list of the MCData group information entries:

i) shall copy the MCData group entry of the served list of the MCData group information into a new MCData group information entry of the candidate list of the MCData group information entries;

ii) shall set the affiliation status of the new MCData group information entry to the "de-affiliating" state; and

iii) shall set the expiration time of the new MCData group information entry to the current time increased with twice the value of timer F;

16) shall replace the list of the MCData group information entries stored in the served MCData client information entry with the candidate list of the MCData group information entries;

17) shall perform the procedures specified in subclause 8.3.2.6 for the served MCData ID and each MCData group ID:

a) which does not have an MCData group information entry in the served list of the MCData group information entries and which has an MCData group information entry in the candidate list of the MCData group information entries with the affiliation status set to the "affiliating" state;

b) which has an MCData group information entry in the served list of the MCData group information entries with the expiration time already expired, and which has an MCData group information entry in the candidate list of the MCData group information entries with the affiliation status set to the "affiliating" state;

c) which has an MCData group information entry in the served list of the MCData group information entries with the affiliation status set to the "deaffiliating" state or the "deaffiliated" state and with the expiration time not expired yet, and which has an MCData group information entry in the candidate list of the MCData group information entries with the affiliation status set to the "affiliating" state; or

d) which has an MCData group information entry in the served list of the MCData group information entries with the affiliation status set to the "affiliated" state and with the expiration time not expired yet, and which has an MCData group information entry in the candidate list of the MCData group information entries with the affiliation status set to the "de-affiliating" state;

18) shall identify the handled p-id in the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

19) shall perform the procedures specified in subclause 8.3.2.5 for the served MCData ID.

8.3.2.4 Receiving subscription to affiliation status procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains either the public service identity identifying the originating participating MCData function serving the MCData user, or the public service identity identifying the terminating participating MCData function serving the MCData user;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element which identifies an MCData ID served by the MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

2) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the originating participating MCData function serving the MCData user, shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the terminating participating MCData function serving the MCData user, shall identify the originating MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

4) if the originating MCData ID is different than the served MCData ID and the originating MCData ID is not authorized to modify affiliation status of the served MCData ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps; and

5) shall generate a 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36].

For the duration of the subscription, the MCData server shall notify the subscriber about changes of the information of the served MCData ID, as described in subclause 8.3.2.5.

8.3.2.5 Sending notification of change of affiliation status procedure

In order to notify the subscriber about changes of the served MCData ID, the MCData server:

1) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

2) shall consider the list of the MCData client information entries of the served MCData user information entry as the served list of the MCData client information entries;

3) shall generate an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 8.4.1 and the served list of the MCData client information entries with the following clarifications:

   a) the MCData server shall not include information from an MCData group information entry with the expiration time already expired;

   b) the MCData server shall not include information from an MCData group information entry with the affiliation status set to the "deaffiliated" state;

   c) if the SIP SUBSCRIBE request creating the subscription of this notification contains an application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information according to subclause 8.4.2, the MCData server shall restrict the application/pidf+xml MIME body according to the application/simple-filter+xml MIME body; and

d) if this procedures is invoked by procedure in subclause 8.3.2.3 where the handled p-id value was identified, the MCData server shall set the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id value; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [5], and IETF RFC 6665 [36] for the subscription created in subclause 8.3.2.4. In the SIP NOTIFY request, the MCData server shall include the generated application/pidf+xml MIME body indicating per-user affiliation information.

8.3.2.6 Sending affiliation status change towards MCData server owning MCData group procedure

NOTE 1: Usage of one SIP PUBLISH request to carry information about change of affiliation state of several MCData users served by the same MCData server is not supported in this version of the specification.

In order:

- to send an affiliation request of a served MCData ID to a handled MCData group ID;
- to send an de-affiliation request of a served MCData ID from a handled MCData group ID; or
- to send an affiliation request of a served MCData ID to a handled MCData group ID due to near expiration of the previously published information;

the MCData server shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39]. In the SIP PUBLISH request, the MCData server:

1) shall set the Request-URI to the public service identity of the controlling MCData function associated with the handled MCData group ID;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

   a) shall include the <mcdata-request-uri> element set to the handled MCData group ID; and

   b) shall include the <mcdata-calling-user-id> element set to the served MCData ID;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) if sending an affiliation request, shall set the Expires header field according to IETF RFC 3903 [34], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if sending an de-affiliation request, shall set the Expires header field according to IETF RFC 3903 [34], to zero;

6) shall include an P-Asserted-Identity header field set to the public service identity of the MCData server according to 3GPP TS 24.229 [5];

7) shall set the current p-id to a globally unique value;

8) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

9) for each MCData group information entry such that:

   a) the MCData group information entry has the "affiliating" affiliation status, the MCData group ID set to the handled MCData group ID, the expiration time has not expired yet and the affiliating p-id is not set;

b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry; and

c) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry;

shall set the affiliating p-id of the MCData group information entry to the current p-id; and

10) shall include an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 8.4.1. The MCData server shall indicate all served MCData client IDs, such that:

a) the affiliation status is set to "affiliating" or "affiliated", and the expiration time has not expired yet in an MCData group information entry with the MCData group ID set to the handled MCData group;

b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry;

c) the MCData client information entry has the MCData client ID set to the served MCData client ID; and

d) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry.

The MCData server shall set the <p-id> child element of the <presence> root element to the current p-id.

The MCData server shall not include the "expires" attribute in the <affiliation> element.

The MCData server shall send the SIP PUBLISH request according to 3GPP TS 24.229 [5].

If timer F expires for the SIP PUBLISH request sent for a (de)affiliation request of served MCData ID to the MCData group ID or upon receiving a SIP 3xx, 4xx, 5xx or 6xx response to the SIP PUBLISH request, the MCData server:

1) shall remove each MCData group ID entry such that:

a) the MCData group information entry has the MCData group ID set to the handled MCData group ID;

b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry; and

c) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry.

8.3.2.7 Affiliation status determination from MCData server owning MCData group procedure

NOTE 1: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of affiliation state of several MCData users served by the same MCData server is not supported in this version of the specification.

In order to discover whether a served MCData user was successfully affiliated to a handled MCData group in the MCData server owning the handled MCData group, the MCData server shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36].

In the SIP SUBSCRIBE request, the MCData server:

1) shall set the Request-URI to the public service identity of the controlling MCData function associated with the handled MCData group ID;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

a) shall include the <mcdata-request-uri> element set to the handled MCData group ID; and

b) shall include the <mcdata-calling-user-id> element set to the served MCData ID;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) if the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the MCData server wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [36], to zero;

6) shall include an Accept header field containing the application/pidf+xml MIME type; and

7) shall include an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to subclause 8.4.2, indicating the served MCData ID.

In order to re-subscribe or de-subscribe, the MCData server shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36]. In the SIP SUBSCRIBE request, the MCData server:

1) if the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

2) if the MCData server wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [36], to zero; and

3) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 8.4.1, then the MCData server:

1) for each served MCData ID and served MCData client ID such that the application/pidf+xml MIME body of SIP NOTIFY request contains:

   a) a <tuple> element of the root <presence> element;

   b) the "id" attribute of the <tuple> element indicating the served MCData ID;

   c) an <affiliation> child element of the <status> element of the <tuple> element;

   d) the "client" attribute of the <affiliation> element indicating the served MCData client ID; and

   d) the "expires" attribute of the <affiliation> element indicating expiration of affiliation;

   perform the following:

   a) if an MCData group information entry exists such that:

      i) the MCData group information entry has the "affiliating" affiliation status, the MCData group ID set to the handled MCData group ID, and the expiration time has not expired yet;

      ii) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry with the MCData client ID set to the served MCData client ID;

      iii) the MCData client information entry is in the list of the MCData client information entries of a served MCData user information entry with the MCData ID set to the served MCData ID; and

      iv) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

      shall set the affiliation status of the MCData group information entry to "affiliated"; and

      shall set the next publishing time of the MCData group information entry to the current time and half of the time between the current time and the expiration of affiliation; and

2) for each MCData group information entry such that:

a) the MCData group information entry has the "affiliated" affiliation status or the "deaffiliating" affiliation status, the MCData group ID set to the handled MCData group ID, and the expiration time has not expired yet;

b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry with the MCData client ID set to a served MCData client ID;

c) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry with the MCData ID set to a served MCData ID; and

d) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

a) a <tuple> element of the root <presence> element;

b) the "id" attribute of the <tuple> element indicating the served MCData ID;

c) an <affiliation> child element of the <status> child element of the <tuple> element; and

d) the "client" attribute of the <affiliation> element indicating the served MCData client ID.

perform the following:

a) shall set the affiliation status of the MCData group information entry to "deaffiliated"; and

b) shall set the expiration time of the MCData group information entry to the current time; and

3) if a <p-id> element is included in the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request, then for each MCData group information entry such that:

a) the MCData group information entry has the "affiliating" affiliation status, the MCData group ID set to the handled MCData group ID, the expiration time has not expired yet and with the affiliating p-id set to the value of the <p-id> element;

b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry with the MCData client ID set to a served MCData client ID;

c) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry with the MCData ID set to a served MCData ID; and

d) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

a) a <tuple> element of the root <presence> element;

b) the "id" attribute of the <tuple> element indicating the served MCData ID;

c) an <affiliation> child element of the <status> child element of the <tuple> element; and

d) the "client" attribute of the <affiliation> element indicating the served MCData client ID;

perform the following:

a) shall set the affiliation status of the MCData group information entry to "deaffiliated"; and

b) shall set the expiration time of the MCData group information entry to the current time.

8.3.2.8 Procedure for authorizing affiliation status change request in negotiated mode sent to served MCData user

Upon receiving a SIP MESSAGE request such that:

1) Request-URI of the SIP MESSAGE request contains the public service identity identifying the terminating participating MCData function serving the MCData user;

2) the SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element and the <mcdata-calling-user-id> element;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

4) the SIP MESSAGE request contains an application/vnd.3gpp.mcdata-affiliation-command+xml MIME body;

then the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request;

2) shall identify the originating MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request;

3) if the originating MCData ID is not authorized to send an affiliation status change request in negotiated mode to the served MCData ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps;

4) shall set the Request-URI of the SIP MESSAGE request to the public user identity bound to the served MCData ID in the MCData server; and

5) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

before forwarding the SIP MESSAGE request further.

8.3.2.9 Forwarding affiliation status change towards another MCData user procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains the public service identity identifying the originating participating MCData function serving the MCData user;

2) the SIP PUBLISH request contains an application/vnd.3gpp.mcdata-info MIME body containing the<mcdata-request-uri> element which identifies an MCData ID not served by the MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 8.4.1;

then the MCData server:

1) shall identify the target MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info MIME body of the SIP PUBLISH request;

2) shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP PUBLISH request;

3) shall generate a SIP PUBLISH request from the received SIP PUBLISH request. In the generated SIP PUBLISH request, the MCData server:

   a) shall set the Request-URI to the public service identity identifying the terminating participating MCData function serving the target MCData ID;

   b) shall include a P-Asserted-Identity header field containing the public service identity identifying the originating participating MCData function serving the MCData user;

c) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

A) shall include the <mcdata-request-uri> element set to the target MCData ID; and

B) shall include the <mcdata-calling-user-id> element set to the originating MCData ID; and

d) shall include other signalling elements from the received SIP PUBLISH request; and

4) shall send the generated SIP PUBLISH request according to 3GPP TS 24.229 [5].

The MCData server shall forward received SIP responses to the SIP PUBLISH request.

8.3.2.10 Forwarding subscription to affiliation status towards another MCData user procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the originating participating MCData function serving the MCData user;

2) the SIP SUBCRIBE request contains an application/vnd.3gpp.mcdata-info MIME body containing the<mcdata-request-uri> element which identifies an MCData ID not served by MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

then the MCData server:

1) shall identify the target MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info MIME body of the SIP SUBSCRIBE request;

2) shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) shall generate a SIP SUBSCRIBE request from the received SIP SUBSCRIBE request. In the generated SIP SUBSCRIBE request, the MCData server:

a) shall set the Request-URI to the public service identity identifying the terminating participating MCData function serving the target MCData ID;

b) shall include a P-Asserted-Identity header field containing the public service identity identifying the originating participating MCData function serving the MCData user;

c) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

A) shall include the <mcdata-request-uri> element set to the target MCData ID; and

B) shall include the <mcdata-calling-user-id> element set to the originating MCData ID; and

d) shall include other signalling elements from the received SIP SUBSCRIBE request; and

4) shall send the generated SIP SUBSCRIBE request according to 3GPP TS 24.229 [5].

The MCData server shall forward any received SIP responses to the SIP SUBSCRIBE request, any received SIP NOTIFY request and any received SIP responses to the SIP NOTIFY request.

8.3.2.11 Affiliation status determination

This subclause is referenced from other procedures.

If the participating MCData function needs to determine the affiliation status of an MCData user to an MCData group, the participating function:

1) shall find the user information entry in the list of MCData user information entries described in subclause 8.3.2.2 such that the MCData ID of the MCData user information entry is equal to the MCData ID of the originator of the received SIP request;

   a) if the applicable MCData group information entry cannot be found, then the participating MCData function shall determine that the MCData user is not affiliated to the MCData group at the MCData client and the skip the rest of the steps;

2) shall find the MCData client information entry in the list of MCData client information entries of MCData user information entry found in step 1) in which the MCData client id matches the value of the <mcdata-client-id> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body in the received SIP request;

   a) if the applicable MCData client information entry cannot be found, then the participating MCData function shall determine that the MCData user is not affiliated to the MCData group at the MCData client and the skip the rest of the steps;

3) shall find the MCData group information entry in the list of MCData group information entries of MCData client information entry found in step 2 such that the MCData group identity matches the value of the identity of the targeted MCData group;

   a) if the applicable MCData group information entry was found in step 3) and the affiliation status of the MCData group information entry is "affiliating" or "affiliated", shall determine that the MCData user at the MCData client to be affiliated to the targeted MCData group and skip the rest of the steps;

   b) if the applicable MCData group information entry was found in step 3) and the affiliation status of the MCData group information entry is "deaffiliating" or "deaffiliated", shall determine that the MCData user at the MCData client to not be affiliated to the targeted MCData group and skip the rest of the steps; or

   c) if the applicable MCData group information entry was not found in step 3), shall determine that the MCData user at the MCData client is not affiliated to the targeted MCData group.

8.3.2.12 Affiliation status change by implicit affiliation

This subclause is referenced from other procedures.

Upon receiving a SIP request that requires implicit affiliation of the sending MCData client to an MCData group, the participating MCData function:

1) shall determine the served MCData client ID from the <mcdata-client-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the received SIP request;

2) shall determine the MCData group ID from the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the received SIP request;

3) shall determine the served MCData ID by using the public user identity in the P-Asserted-Identity header field of the SIP request;

NOTE 1: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

4) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

5) shall consider an MCData client information entry such that:

   a) the MCData client information entry is in the list of MCData client information entries of the served MCData user information entry; and

   b) the MCData client ID of the MCData client information entry is equal to the served MCData client ID;

as the served MCData client information entry;

6) shall consider a copy of the list of the MCData group information entries of the served MCData client information entry as the served list of the MCData group information entries;

7) shall construct the candidate list of the MCData group information entries as follows:

   a) for each MCData group ID which has an MCData group information entry in the served list of the MCData group information entries shall copy the MCData group information entry into a new MCData group information entry of the candidate list of the MCData group information entries; and

   b) if the determined MCData group ID does not have an MCData group information entry in the served list of the MCData group information entries or has an MCData group information entry in the served list of the MCData group information entries, such that the expiration time of the MCData group information entry has already expired:

      i) shall add a new MCData group information entry in the candidate list of the MCData group information list for the determined MCData group ID;

      ii) shall set the affiliation status of the new MCData group information entry to the "affiliating" state; and

      iii) shall set the expiration time of the new MCData group information entry to the current time increased with the candidate expiration interval;

8) determine the candidate number of MCData group IDs as the number of different MCData group IDs which have an MCData group information entry:

   a) in the candidate list of the MCData group information entries; or

   b) in the list of the MCData group information entries of an MCData client information entry such that:

      i) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry; and

      ii) the MCData client ID of the MCData client information entry is not equal to the served MCData client ID;

   with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

9) if the candidate number of MCData group IDs is bigger than the N2 value of the served MCData ID, shall based on MCData service provider policy reduce the candidate MCData group IDs to that equal to N2;

10) if the determined MCData group ID cannot be added to the the candidate list of the MCData group information entries due to exceeding the MCData user's N2 limit, shall discard the candidate list of the MCData group information entries and skip the remaining steps of the current procedure; and

11) shall replace the list of the MCData group information entries stored in the served MCData client information entry with the candidate list of the MCData group information entries.

8.3.2.13 Implicit affiliation status change completion

This subclause is referenced from other procedures.

If the participating MCData function has received a SIP 2xx response from the controlling MCData function to a SIP request that had triggered performing the procedures of subclause 8.3.2.12, the participating MCData function:

1) shall set the affiliation status of the MCData group information entry added to the candidate list of the MCData group information entries by the procedures of subclause 8.3.2.12 to "affiliated"; and

2) shall perform the procedures specified in subclause 8.3.2.5 for the served MCData ID.

8.3.2.14 Implicit affiliation status change cancellation

This subclause is referenced from other procedures.

If the participating MCData function determines that a received SIP request that had triggered performing the procedures of subclause 8.3.2.12 needs to be rejected or if the participating MCData function receives a SIP 4xx, 5xx or 6xx response from the controlling MCData function for the received SIP request, the participating MCData function:

1) shall remove the MCData group ID entry added by the procedures of subclause 8.3.2.12 such that:

   a) the MCData group information entry has the MCData group ID set to the MCData group ID of the MCData group targeted by the received SIP request;

   b) the MCData group information entry is in the list of the MCData group information entries of an MCData client information entry containing the MCData client ID included in the received SIP request; and

   c) the MCData client information entry is in the list of the MCData client information entries of the MCData user information entry containing the MCData ID of the sender of the received SIP request.

8.3.2.15 Implicit affiliation to configured groups procedure

This subclause is referenced from other procedures.

If the participating MCData function has successfully performed service authorization for the MCData ID identified in the service authorisation procedure as described in 3GPP TS 33.179 [56], the participating MCData function:

1) shall identify the MCData ID included in the SIP request received for service authorisation procedure as the served MCData ID;

2) shall identify the MCData client ID from the <mcdata-client-id> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body included in the SIP request received for service authorisation as the served MCData client ID;

3) shall download the MCData user profile from the MCData user database as defined in 3GPP TS 29.283 [37] if not already stored at the participating MCData function;

4) if no <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]) for the served MCData ID or the <ImplicitAffiliations> element contains no <entry> elements containing an MCData group ID, shall skip the remaining steps;

5) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 8.3.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

6) shall consider an MCData client information entry such that:

   a) the MCData client information entry is in the list of MCData client information entries of the served MCData user information entry; and

   b) the MCData client ID of the MCData client information entry is equal to the served MCData client ID;

   as the served MCData client information entry;

7) shall consider a copy of the list of the MCData group information entries of the served MCData client information entry as the served list of the MCData group information entries;

8) shall construct the candidate list of the MCData group information entries as follows:

   a) for each MCData group ID which has an MCData group information entry in the served list of the MCData group information entries shall copy the MCData group information entry into a new MCData group information entry of the candidate list of the MCData group information entries;

   b) for each MCData group ID contained in an <entry> element of the <ImplicitAffiliations> element in the <OnNetwork> element of the MCData user profile document (see the MCData user profile document in

3GPP TS 24.484 [12]) for the served MCData ID that does not have an MCData group information entry in the served list of the MCData group information entries or has an MCData group information entry in the served list of the MCData group information entries such that the expiration time of the MCData group information entry has already expired:

i) shall add a new MCData group information entry in the candidate list of the MCData group information list for the MCData group ID;

ii) shall set the affiliation status of the new MCData group information entry to the "affiliating" state; and

iii) shall set the expiration time of the new MCData group information entry to the current time increased with the candidate expiration interval;

c) if in step b) above, no new MCData group information entries were added to the candidate list of the MCData group information list for the MCData group ID:

i) shall discard the candidate list; and

ii) shall skip the remaining steps;

9) determine the candidate number of MCData group IDs as the number of different MCData group IDs which have an MCData group information entry:

a) in the candidate list of the MCData group information entries; or

b) in the list of the MCData group information entries of an MCData client information entry such that:

i) the MCData client information entry is in the list of the MCData client information entries of the served MCData user information entry; and

ii) the MCData client ID of the MCData client information entry is not equal to the served MCData client ID;

with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

c) if the candidate number of MCData group IDs is bigger than the N2 value of the served MCData ID, shall based on MCData service provider policy reduce the candidate MCData group IDs to that equal to N2;

10) shall replace the list of the MCData group information entries stored in the served MCData client information entry with the candidate list of the MCData group information entries; and

11) for each MCData group ID contained in an <entry> element of the <ImplicitAffiliations> element in the <OnNetwork> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]) for the served MCData ID and which has an MCData group information entry in the candidate list of the MCData group information entries with an affiliation status of "affiliating", shall perform the procedures specified in subclause 8.3.2.6 for the served MCData ID and each MCData group ID.

NOTE 2: To learn of the MCData groups successfully affiliated to, the MCData client can subscribe to that information by the procedures specified in subclause 8.2.3.

8.3.3 Procedures of MCData server owning the MCData group

8.3.3.1 General

The procedures of MCData server owning the MCData group consist of:

- receiving group affiliation status change procedure;
- receiving subscription to affiliation status procedure;
- sending notification of change of affiliation status procedure;
- implicit affiliation eligibilty check procedure; and

- affiliation status change by implicit affiliation procedure.

NOTE: Usage of CSC-3 part of MCData group affiliation procedure and of CSC-3 part of MCData group de-affiliation procedure is not specified in this version of the specification.

8.3.3.2 Stored information

The MCData server shall maintain a list of MCData group information entries.

In each MCData group information entry, the MCData server shall maintain:

1) an MCData group ID. This field uniquely identifies the MCData group information entry in the list of the MCData group information entries; and

2) a list of MCData user information entries.

In each MCData user information entry, the MCData server shall maintain:

1) an MCData ID. This field uniquely identifies the MCData user information entry in the list of the MCData user information entries;

2) a list of MCData client information entries; and

3) an expiration time.

In each MCData client information entry, the MCData server shall maintain:

1) an MCData client ID. This field uniquely identifies the MCData client information entry in the list of the MCData client information entries.

8.3.3.3 Receiving group affiliation status change procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains the public service identity of the controlling MCData function associated with the served MCData group;

2) the SIP PUBLISH request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the <mcdata-request-uri> element and the <mcdata-calling-user-id> element;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 8.4.1;

then the MCData server:

1) shall identify the served MCData group ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

3) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

4) if an MCData group for the served MCData group ID does not exist in the group management server according to 3GPP TS 24.481 [11], shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

5) if the handled MCData ID is not a member of the MCData group identified by the served MCData group ID, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

6) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34]. In the SIP 200 (OK) response, the MCData server:

   a) shall set the Expires header field according to IETF RFC 3903 [34], to the selected expiration time;

7) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served MCData group ID, shall not continue with the rest of the steps;

8) if the handled MCData ID is different from the MCData ID in the "id" attribute of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request, shall not continue with the rest of the steps;

9) shall consider an MCData group information entry such that:

   a) the MCData group information entry is in the list of MCData group information entries described in subclause 8.3.3.2; and

   b) the MCData group ID of the MCData group information entry is equal to the served MCData group ID;

   as the served MCData group information entry;

10) if the selected expiration time is zero:

   a) shall remove the MCData user information entry such that:

      i) the MCData user information entry is in the list of the MCData user information entries of the served MCData group information entry; and

      ii) the MCData user information entry has the MCData ID set to the served MCData ID;

11) if the selected expiration time is not zero:

   a) shall consider an MCData user information entry such that:

      i) the MCData user information entry is in the list of the MCData user information entries of the served MCData group information entry; and

      ii) the MCData ID of the MCData user information entry is equal to the handled MCData ID;

      as the served MCData user information entry;

   b) if the MCData user information entry does not exist:

      i) shall insert an MCData user information entry with the MCData ID set to the handled MCData ID into the list of the MCData user information entries of the served MCData group information entry; and

      ii) shall consider the inserted MCData user information entry as the served MCData user information entry; and

   c) shall set the following information in the served MCData user information entry:

      i) set the MCData client ID list according to the "client" attributes of the <affiliation> elements of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

      ii) set the expiration time according to the selected expiration time;

12) shall identify the handled p-id in the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

13) shall perform the procedures specified in subclause 8.3.3.5 for the served MCData group ID.

8.3.3.4 Receiving subscription to affiliation status procedure

NOTE: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of affiliation state of several MCData users served by the same MCData server is not supported in this version of the specification.

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity of the controlling MCData function associated with the served MCData group;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element and the <mcdata-calling-user-id> element;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type; and

5) the SIP SUBSCRIBE request contains an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to subclause 8.4.2 indicating the same MCData ID as in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

then the MCData server:

1) shall identify the served MCData group ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

3) if the Expires header field of the SIP SUBSCRIBE request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP SUBSCRIBE request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

4) if an MCData group for the served MCData group ID does not exist in the group management server according to 3GPP TS 24.481 [11], shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

5) if the handled MCData ID is not a member of the MCData group identified by the served MCData group ID, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps; and

6) shall generate a SIP 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [5], IETF RFC 6665 [36].

For the duration of the subscription, the MCData server shall notify subscriber about changes of the information of the served MCData ID, as described in subclause 8.3.3.5.

8.3.3.5 Sending notification of change of affiliation status procedure

In order to notify the subscriber identified by the handled MCData ID about changes of the affiliation status of the served MCData group ID, the MCData server:

1) shall consider an MCData group information entry such that:

   a) the MCData group information entry is in the list of MCData group information entries described in subclause 8.3.3.2; and

   b) the MCData group ID of the MCData group information entry is equal to the served MCData group ID;

2) shall consider an MCData user information entry such:

   a) the MCData user information entry is in the list of the MCData user information entries of the served MCData group information entry; and

   b) the MCData ID of the MCData user information entry is equal to the handled MCData ID;

   as the served MCData user information entry;

3) shall generate an application/pidf+xml MIME body indicating per-group affiliation information according to subclause 8.4.1 and the served list of the served MCData user information entry of the MCData group information entry with following clarifications:

   a) the MCData server shall include the "expires" attribute in the <affiliation> element; and

   b) if this procedures is invoked by procedure in subclause 8.3.3.3 where the handled p-id was identified, the MCData server shall set the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id value; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [5], and IETF RFC 6665 [36] for the subscription created in subclause 8.3.3.4. In the SIP NOTIFY request, the MCData server shall include the generated application/pidf+xml MIME body indicating per-group affiliation information.

8.3.3.6 Implicit affiliation eligibilty check procedure

This subclause is referenced from other procedures.

Upon receiving a SIP request for an MCData group that the MCData user is not currently affiliated to and that requires the controlling MCData function to check on the eligibility of the MCData user to be implicitly affiliated to the MCData group, the controlling MCData function:

1) shall identify the served MCData group ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request;

2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request;

3) if an MCData group for the served MCData group ID does not exist in the group management server according to 3GPP TS 24.481 [11], shall consider the MCData user to be ineligible for implicit affiliation and skip the rest of the steps;

4) if the handled MCData ID is not a member of the MCData group identified by the served MCData group ID, shall consider the MCData user to be ineligible for implicit affiliation and skip the rest of the steps;

5) if there is no MCData group information entry in the list of MCData group information entries described in subclause 8.3.3.2 with an MCData group identity matching the served MCData group ID, then shall consider the MCData user to be ineligible for implicit affiliation and skip the rest of the steps; or

6) shall consider the MCData user to be eligible for implicit affiliation.

8.3.3.7 Affiliation status change by implicit affiliation procedure

This subclause is referenced from other procedures.

Upon receiving a SIP request for an MCData group that the MCData user is not currently affiliated to and that requires the controlling MCData function to perform an implicit affiliation to, the controlling MCData function:

1) shall identify the served MCData group ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request;

2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP request;

3) shall consider an MCData group information entry such that:

a) the MCData group information entry is in the list of MCData group information entries described in subclause 8.3.3.2; and

b) the MCData group ID of the MCData group information entry is equal to the served MCData group ID;

as the served MCData group information entry;

4) shall consider an MCData user information entry such that:

a) the MCData user information entry is in the list of the MCData user information entries of the served MCData group information entry; and

b) the MCData ID of the MCData user information entry is equal to the handled MCData ID;

as the served MCData user information entry;

c) if the MCData user information entry does not exist:

i) shall insert an MCData user information entry with the MCData ID set to the handled MCData ID into the list of the MCData user information entries of the served MCData group information entry; and

ii) shall consider the inserted MCData user information entry as the served MCData user information entry; and

d) shall make the following modifications in the served MCData user information entry:

i) add the MCData client ID derived from the received SIP request to the MCData client ID list if not already present; and

ii) set the expiration time as determined by local policy;

5) shall perform the procedures specified in subclause 8.3.3.5 for the served MCData group ID.

8.4 Coding

8.4.1 Extension of application/pidf+xml MIME type

8.4.1.1 Introduction

The subclauses of the parent subclause describe an extension of the application/pidf+xml MIME body specified in IETF RFC 3863 [40]. The extension is used to indicate:

- per-user affiliation information; and
- per-group affiliation information.

8.4.1.2 Syntax

The application/pidf+xml MIME body indicating per-user affiliation information is constructed according to IETF RFC 3863 [40] and:

1) contains a <presence> root element according to IETF RFC 3863 [40];

2) contains an "entity" attribute of the <presence> element set to the MCData ID of the MCData user;

3) contains one <tuple> child element according to IETF RFC 3863 [40] per each MCData client of the <presence> element;

4) can contain a <p-id> child element defined in the XML schema defined in table 8.4.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;

5) contains an "id" attribute of the <tuple> element set to the MCData client ID;

6) contains one <status> child element of each <tuple> element;

7) contains one <affiliation> child element defined in the XML schema defined in table 8.4.1.2-1, of the <status> element, for each MCData group in which the MCData user is interested at the MCData client;

8) contains a "group" attribute of each <affiliation> element set to the MCData group ID of the MCData group in which the MCData user is interested at the MCData client;

9) can contain a "status" attribute of each <affiliation> element indicating the affiliation status of the MCData user to MCData group at the MCData client; and

10) can contain an "expires" attribute of each <affiliation> element indicating expiration of affiliation of the MCData user to MCData group at the MCData client.

The application/pidf+xml MIME body indicating per-group affiliation information is constructed according to IETF RFC 3856 [39] and:

1) contains the <presence> root element according to IETF RFC 3863 [40];

2) contains an "entity" attribute of the <presence> element set to the MCData group ID of the MCData group;

3) contains one <tuple> child element according to IETF RFC 3863 [40] of the <presence> element;

4) can contain a <p-id> child element defined in the XML schema defined in table 8.4.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;

5) contains an "id" attribute of the <tuple> element set to the MCData ID of the MCData user;

6) contains one <status> child element of each <tuple> element;

7) contains one <affiliation> child element defined in the XML schema defined in table 8.4.1.2-1, of the <status> element, for each MCData client at which the MCData user is interested in the MCData group;

8) contains one "client" attribute defined in the XML schema defined in table 8.4.1.2-2, of the <affiliation> element set to the MCData client ID; and

9) can contain an "expires" attribute defined in the XML schema defined in table 8.4.1.2-2, of the <affiliation> element indicating expiration of affiliation of the MCData user to MCData group at the MCData client.

Table 8.4.1.2-1: XML schema with elements and attributes extending the application/pidf+xml MIME body

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:mcdataPresInfo:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:mcdataPI10="urn:3gpp:ns:mcdataPresInfo:1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- MCData specific child elements of tuple element -->
  <xs:element name="affiliation" type="mcdataPI10:affiliationType"/>
  <xs:complexType name="affiliationType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="group" type="xs:anyURI" use="optional"/>
    <xs:attribute name="client" type="xs:anyURI" use="optional"/>
    <xs:attribute name="status" type="mcdataPI10:statusType" use="optional"/>
    <xs:attribute name="expires" type="xs:dateTime" use="optional"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="statusType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="affiliating"/>
      <xs:enumeration value="affiliated"/>
      <xs:enumeration value="deaffiliating"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="p-id" type="xs:string"/>

  </xs:schema>
```

The application/pidf+xml MIME body refers to namespaces using prefixes specified in table 8.4.1.2-2.

Table 8.4.1.2-2: Assignment of prefixes to namespace names in the application/pidf+xml MIME body

Prefix	Namespace
mcdataPI10	urn:3gpp:ns:mcdataPresInfo:1.0
NOTE: The "urn:ietf:params:xml:ns:pidf" namespace is the default namespace so no prefix is used for it in the application/pidf+xml MIME body.	

8.4.2 Extension of application/simple-filter+xml MIME type

8.4.2.1 Introduction

The subclauses of the parent subclause describe an extension of the application/simple-filter+xml MIME body specified in IETF RFC 4661 [41].

The extension is used to indicate per-client restrictions of presence event package notification information and per-user restrictions of presence event package notification information.

8.4.2.2 Syntax

The application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information is constructed according to IETF RFC 4661 [41] and:

1) contains a <filter-set> root element according to IETF RFC 4661 [41];
2) contains a <ns-bindings> child element according to IETF RFC 4661 [41], of the <filter-set> element;
3) contains a <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:
   A) contains a "prefix" attribute according to IETF RFC 4661 [41] set to "pidf"; and
   B) contains a "urn" attribute set to the "urn:ietf:params:xml:ns:pidf" value;
4) contains a <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:
   A) contains a "prefix" attribute according to IETF RFC 4661 [41], set to "mcdataPI10"; and
   B) contains an "urn" attribute according to IETF RFC 4661 [41], set to the "urn:3gpp:ns:mcdataPresInfo:1.0" value;
5) contains a <filter> child element according to IETF RFC 4661 [41], of the <filter-set> element where the <filter> element;
   A) contains an "id" attribute set to a value constructed according to IETF RFC 4661 [41];
   B) does not contain an "uri" attribute of the <filter> child element according to IETF RFC 4661 [41]; and
   C) does not contain an "domain" attribute according to IETF RFC 4661 [41];
6) contains a <what> child element according to IETF RFC 4661 [41], of the <filter> element; and
7) contains an <include> child element according to IETF RFC 4661 [41], of the <what> element where the <include> element;
   A) does not contain a "type" attribute according to IETF RFC 4661 [41]; and
   B) contains the value, according to IETF RFC 4661 [41], set to concatenation of the '//pidf:presence/pidf:tuple[@id="' string, the MCData client ID, and the '"]' string.

The application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information is constructed according to IETF RFC 4661 [41] and:

1) contains a <filter-set> root element according to IETF RFC 4661 [41];

2) contains a <ns-bindings> child element according to IETF RFC 4661 [41], of the <filter-set> element;

3) contains a <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [41] set to "pidf"; and

   B) contains a "urn" attribute set to the "urn:ietf:params:xml:ns:pidf" value;

4) contains a <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [41], set to "mcdataPI10"; and

   B) contains an "urn" attribute according to IETF RFC 4661 [41], set to the "urn:3gpp:ns:mcdataPresInfo:1.0" value;

5) contains a <filter> child element according to IETF RFC 4661 [41], of the <filter-set> element where the <filter> element;

   A) contains an "id" attribute set to a value constructed according to IETF RFC 4661 [41];

   B) does not contain an "uri" attribute of the <filter> child element according to IETF RFC 4661 [41]; and

   C) does not contain an "domain" attribute according to IETF RFC 4661 [41];

6) contains a <what> child element according to IETF RFC 4661 [41], of the <filter> element; and

7) contains an <include> child element according to IETF RFC 4661 [41], of the <what> element where the <include> element;

   A) does not contain a "type" attribute according to IETF RFC 4661 [41]; and

   B) contains the value, according to IETF RFC 4661 [41], set to concatenation of the '//pidf:presence/pidf:tuple[@id="' string, the MCData ID, and the '"]' string.

9 Short Data Service (SDS)

9.1 General

The group administrator can disable the SDS service on a MCData group by setting the <mcdata-allow-short-data-service> element under the <list-service> element, in the group document, to "false".

If the <mcdata-allow-short-data-service> element under the <list-service> element, in the group document, is set to "false" for a MCData group:

- an MCData client should not use the procedures in the subclauses of the parent subclause to send SDS to the said MCData group.

- a terminating MCData controlling function should reject the request to send SDS to the said MCData group.

9.2 On-network SDS

9.2.1 General

9.2.1.1 Sending an SDS message

When the MCData user wishes to send:

- a one-to-one standalone Short Data Service (SDS) message to another MCData user; or
- a group standalone Short Data Service (SDS) message to a pre-arranged group ;

the MCData client:

1) shall follow the procedures in subclause 11.1 for transmission control; and
2) if the procedures in subclause 11.1 are successful and the size of the payload the MCData user wishes to send:
   a) is less than or equal to the value contained in the <max-payload-size-sds-cplane-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], shall follow the procedures specified in subclause 9.2.2.2.1:
   b) is greater than the value contained in the <max-payload-size-sds-cplane-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], shall follow the procedures specified in subclause 9.2.3.2.3.

When the MCData user wishes to:

- initiate a Short Data Service (SDS) session with another MCData user; or
- initiate a group Short Data Service (SDS) session to a pre-configured group or to particular members of the pre-configured group;

the MCData client:

1) shall follow the procedures in subclause 11.1 for transmission control; and
2) if the procedures in subclause 11.1 are successful, shall follow the procedures specified in subclause 9.2.4.2.3.

9.2.1.2 Handling of received SDS messages with or without disposition requests

When a MCData client has received a SIP request containing:

- an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and
- an application/vnd.3gpp.mcdata-payload MIME body as specified in subclause E.2;

the MCData Client:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;
2) shall decode the contents of the application/vnd.3gpp.mcdata-payload MIME body;
3) if the SDS SIGNALLING PAYLOAD message contains a new Conversation ID, shall instantiate a new conversation with the Message ID in the SDS SIGNALLING PAYLOAD identifying the first message in the conversation thread;
4) if the SDS SIGNALLING PAYLOAD message contains an existing Conversation ID and:
   a) if the SDS SIGNALLING PAYLOAD message does not contain an InReplyTo message ID, shall use the Message ID in the SDS SIGNALLING PAYLOAD to identify a new message in the existing conversation thread; and
   b) if the SDS SIGNALLING PAYLOAD message contains an InReplyTo message ID, shall associate the message to an existing message in the conversation thread as identified by the InReplyTo message ID in the SDS SIGNALLING PAYLOAD, and use the Message ID in the SDS SIGNALLING PAYLOAD to identify the new message;
5) shall identify the number of Payload IEs in the DATA PAYLOAD message from the Number of payloads IE in the DATA PAYLOAD message;
6) if the SDS SIGNALLING PAYLOAD message does not contain an Application ID IE and does not contain an Extended application ID IE:
   a) shall determine that the payload contained in the DATA PAYLOAD message is for user consumption

b) may notify the MCData user;

c) may display to the MCData user the functional alias of the originating MCData user, if provided; and

d) shall render the contents of the Payload IE(s) to the MCData user.

7) if the SDS SIGNALLING PAYLOAD message contains an Application ID IE:

a) shall determine that the payload contained in the DATA PAYLOAD message is not for user consumption,

b) shall not notify the MCData user;

c) if the Application ID value is unknown, shall discard the SDS message; and

d) if the Application ID value is known, shall deliver the contents of the Payload IE(s) to the identified application;

NOTE 1: If required, the MCData client decrypts the Payload IEs before rendering the SDS message to the user or delivering the SDS message to the application.

NOTE 2: The actions taken when the payload contains application data not meant for user consumption or command instructions are based upon the contents of the payload. If the payload content is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application and delivers the payload to that application.

NOTE 3: User consent is not required before accepting the data.

8) if the SDS SIGNALLING PAYLOAD message contains an Extended application ID IE:

a) shall determine that the payload contained in the DATA PAYLOAD message is not for user consumption;

b) shall not notify the MCData user;

c) if the Extended application ID value is unknown, shall discard the SDS message; and

d) if the Extended application ID value is known, shall deliver the contents of the Payload IE(s) to the identified application;

NOTE 4: If required, the MCData client decrypts the Payload IEs before rendering the SDS message to the user or delivering the SDS message to the application.

NOTE 5: The actions taken when the payload contains application data not meant for user consumption or command instructions are based upon the contents of the payload. If the payload content is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application and delivers the payload to that application.

NOTE 6: User consent is not required before accepting the data.

9) may store the message payload in local storage along with the Conversation ID, Message ID, InReplyTo message ID and Date and time; and

10) if the received SDS SIGNALLING PAYLOAD message contains an SDS disposition request type IE shall follow the procedures in subclause 9.2.1.3.

9.2.1.3 Handling of disposition requests

To handle the disposition requests, the MCData client:

1) If the SDS disposition request type IE is set to:

a) "DELIVERY" then, shall send a delivered notification as described in subclause 12.2.1.1;

b) "READ", shall send a read notification as described in subclause 12.2.1.1, when a display indication is received; or

c) "DELIVERY AND READ" then, shall start timer TDU1 (delivery and read).

Upon receiving a display indication before timer TDU1 (delivery and read) expires, the MCData client:

1) shall stop timer TDU1 (delivery and read); and

2) shall send a delivered and read notification as described in subclause 12.2.1.1.

Upon expiry of timer TDU1 (delivery and read), the MCData client:

1) shall send a delivered notification as described in subclause 12.2.1.1; and

2) upon receiving a display indication, send a read notification as described in subclause 12.2.1.1.

9.2.2 Standalone SDS using signalling control plane

9.2.2.1 General

The procedures in the subclauses of the parent subclause are used by a MCData functional entity to send or receive:

- a one-to-one standalone SDS message using the signalling control plane; or
- a group standalone SDS message using the signalling control plane.

9.2.2.2 MCData client procedures

9.2.2.2.1 MCData client originating procedures

The MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] with the clarifications given below.

The MCData client:

1) shall build the SIP MESSAGE request as specified in subclause 6.2.4.1;

2) if a one-to-one standalone SDS message is to be sent, shall insert in the SIP MESSAGE request:

   a) an application/resource-lists+xml MIME body with the MCData ID of the target MCData user, according to rules and procedures of IETF RFC 4826 [9];

   b) an application/vnd.3gpp.mcdata-info+xml MIME body with:

      i) a <request-type> element set to a value of "one-to-one-sds"; and

      ii) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> element set to the URI of the used functional alias; and

   c) if end-to-end security is required and the security context does not exist or if the existing security context has expired, an application/mikey MIME body with the MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [26]. The MCData client:

      i) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];

      ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [26];

      iii) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect one-to-one communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [26];

      iv) shall encrypt the PCK to a UID associated to the MCData client using the MCData ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [26];

      v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [26]; and

vi) shall add the MCData ID of the originating MCData to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCData user's signing key provided in the keying material together with a time related parameter; and

viii) shall include the MIKEY-SAKKE I_MESSAGE in an application/mikey MIME body as specified in 3GPP TS 33.180 [26];

3) if a group standalone SDS message is to be sent:

a) if the "/<*x*>/<x>/Common/MCData/AllowedSDS" leaf node present in the group document of the requested MCData group, configured on the group management client as specified in 3GPP TS 24.483 [42] is set to "false", shall reject the request to send SDS and not continue with the rest of the steps in this subclause; and

b) shall insert in the SIP MESSAGE request an application/vnd.3gpp.mcdata-info+xml MIME body with:

i) the <request-type> element set to a value of "group-sds";

ii) the <mcdata-request-uri> element set to the MCData group identity;

iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

iv) if the MCData client is aware of active functional aliases, and an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> set to the URI of the used functional alias;

4) shall generate a standalone SDS message as specified in subclause 6.2.2.1; and

5) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

9.2.2.2.2 MCData client terminating procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for terminating MCData client", the MCData client:

1) may reject the SIP MESSAGE request if there are not enough resources to handle the SIP MESSAGE request;

2) if the SIP MESSAGE request is rejected in step 1), shall respond toward participating MCData function with a SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this subclause;

3) if the SIP MESSAGE request contains an application/mikey MIME body containing a MIKEY-SAKKE I_MESSAGE:

a) shall extract the MCData ID of the originating MCData user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

b) shall convert the MCData ID to a UID as described in 3GPP TS 33.180 [26];

c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [26];

d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP MESSAGE request with a SIP 606 (Not Acceptable) response, and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and not continue with rest of the steps in this subclause; and

e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26]; and

ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [26];

NOTE: With the PCK successfully shared between the originating MCData client and the terminating MCData client, both clients are able to exchange end-to-end secure message.

4) shall generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

5) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5]; and

6) shall handle the received message as specified in subclause 9.2.1.2.

9.2.2.3 Participating MCData function procedures

9.2.2.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for originating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the originating user from the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is:

   a) set to a value of "group-sds", shall determine the public service identity of the controlling MCData function associated with the MCData group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request; or

   b) set to a value of "one-to-one-sds", shall determine the public service identity of the controlling MCData function hosting the one-to-one standalone SDS service for the calling user;

5) if unable to identify the controlling MCData function for standalone SDS, it shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID:

   a) is not allowed to send MCData communications as determined by step 1) of subclause 11.1, shall reject the "SIP MESSAGE request for standalone SDS for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

   b) is not allowed to initiate one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request as determined by step 7) of subclause 11.1, shall reject the "SIP MESSAGE request for standalone SDS for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "202 user not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

c) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of subclause 11.1, shall reject the "SIP MESSAGE request for standalone SDS for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData communication not authorised to the targeted user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

8) if the payload size of the message is larger than the value contained in the <max-payload-size-sds-cplane-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], shall reject the "SIP MESSAGE request for standalone SDS for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "203 message too large to send over signalling control plane" in a Warning header field as specified in subclause 4.9;

NOTE: The term "payload size" refers to the "Length of Payload contents" of the payload IE of the DATA PAYLOAD message transported in the SIP MESSAGE request, minus 1 (to account for the added "Payload content type" field).

9) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

10) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

11) shall copy all MIME bodies included in the incoming SIP MESSAGE request to the outgoing SIP MESSAGE request;

12) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

12A) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element;

13) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

14) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

15) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 202 (Accepted) response in response to the SIP MESSAGE request in step 15):

1) shall generate a SIP 202 (Accepted) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 202 (Accepted) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP MESSAGE request in step 15):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request in step 15) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

9.2.2.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for terminating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

3) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

3a) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [12]) and:

   i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

   ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [12]);

   then:

   i) shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.1;

5) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request; and

6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

9.2.2.4 Controlling MCData function procedures

9.2.2.4.1 Originating controlling MCData function procedures

This subclause describes the procedures for sending a SIP MESSAGE from the controlling MCData function and is initiated by the controlling MCData function as a result of an action in subclause 9.2.2.4.2.

The controlling MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

4) shall copy the following MIME bodies in the received SIP MESSAGE request into the outgoing SIP MESSAGE request by following the guidelines in subclause 6.4:

   a) application/vnd.3gpp.mcdata-info+xml MIME body;

   b) application/vnd.3gpp.mcdata-signalling MIME body; and

   c) application/vnd.3gpp.mcdata-payload MIME body

5) in the application/vnd.3gpp.mcdata-info+xml MIME body:

   a) shall set the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

   b) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request was set to a value of "group-sds", shall set the <mcdata-calling-group-id> element to the group identity;

6) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

7) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request;

8) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds"; and

9) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [5].

9.2.2.4.2 Terminating controlling MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for controlling MCData function", the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4]. Otherwise, continue with the rest of the steps;

2) if the SIP MESSAGE does not contain:

   a) an application/vnd.3gpp.mcdata-info+xml MIME body;

   b) an application/vnd.3gpp.mcdata-signalling MIME body; and

   c) an application/vnd.3gpp.mcdata-payload MIME body;

   shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "199 expected MIME bodies not in the request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

3) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body contained in the SIP MESSAGE;

4) if the application/vnd.3gpp.mcdata-signalling MIME body contains a SDS SIGNALLING PAYLOAD message with a SDS disposition request type IE, shall store the value of the Conversation ID IE and the value of the Message ID IE in the SDS SIGNALLING PAYLOAD message;

NOTE: The controlling MCData function uses the Conversation ID and Message ID for correlation with disposition notifications.

5) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is set to a value of "one-to-one-sds" and:

   a) the conditions in subclause 11.1 indicate that the MCData user is not allowed to SDS communications due to message size as determined by step 3) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "218 user not authorised for one-to-one SDS communications due to message size" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   b) the SIP MESSAGE request:

      i) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "204 unable to determine targeted user for one-to-one SDS" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

      ii) contains an application/resource-lists MIME body with exactly one <entry> element, shall send a SIP MESSAGE request to the MCData user identified in the <entry> element of the MIME body, as specified in subclause 9.2.2.4.1;

6) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is set to a value of "group-sds":

   a) shall retrieve the group document associated with the group identity in the SIP MESSAGE request by following the procedures in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

   b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   c) if the <entry> element of the <list> element of the <list-service> element in the group document does not contain an <mcdata-mcdata-id> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   d) if the <list-service> element contains a <mcdata-allow-short-data-service> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "206 short data service not allowed for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", shall send a SIP 488 (Not Acceptable) response with the warning text set to "207 SDS services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   f) if the MCData server group SDS procedures in subclause 11.1 indicate that the user identified by the MCData ID:

      i) is not allowed to send group MCData communications on this group identity as determined by step 2) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "201 user not authorised to transmit data on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

      ii) is not allowed to send group MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request as determined by step 8) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "208 user not authorised for MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request" in a Warning

header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

iii) is not allowed to send SDS communications on this group identity due to message size as determined by step 5) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "217 user not authorised for SDS communications on this group identity due to message size" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

g) the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP MESSAGE request, as specified in subclause 6.3.5, shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

h) shall determine targeted group members for MCData communications by following the procedures in subclause 6.3.4;

j) if the procedures in subclause 6.3.4 result in no affiliated members found in the selected MCData group, shall return a SIP 403 (Forbidden) response with the warning text set to "198 no users are affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

k) shall send SIP MESSAGE requests to the targeted group members identified in step h) above by following the procedure in subclause 9.2.2.4.1;

7) shall generate a SIP 202 (Accepted) response in response to the "SIP MESSAGE request for standalone SDS for controlling MCData function"; and

8) shall send the SIP 202 (Accepted) response towards the originating participating MCData function according to 3GPP TS 24.229 [5].

9.2.3 Standalone SDS using media plane

9.2.3.1 General

The procedures in the subclauses of the parent subclause are used by a MCData functional entity to send or receive:

- a one-to-one standalone SDS message using the media control plane; or
- a group standalone SDS message using the media control plane.

The procedures in the subclauses of the parent subclause are applicable to establish an on-demand standalone SDS using media plane.

9.2.3.2 MCData client procedures

9.2.3.2.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 4975 [17], IETF RFC 6135 [19] and IETF RFC 6714 [20] the MCData client:

1) shall include an "m=message" media-level section for the MCData media stream consisting of:

a) the port number;

b) a protocol field value of "TCP/MSRP", or "TCP/TLS/MSRP" for TLS;

c) a format list field set to ‘*’;

d) an "a=sendonly" attribute;

e) an "a=path" attribute containing its own MSRP URI;

f) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload"; and

g) set the a=setup attribute as "actpass"; and

2) if end-to-end security is required for a one-to-one communication and the security context does not exist or if the existing security context has expired, shall include the MIKEY-SAKKE I_MESSAGE in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP offer as specified in IETF RFC 4567 [45].

9.2.3.2.2 SDP answer generation

When the MCData client receives an initial SDP offer for an MCData standalone SDS, the MCData client shall process the SDP offer and shall compose an SDP answer according to 3GPP TS 24.229 [5] and IETF RFC 4975 [17].

When composing an SDP answer, the MCData client:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:

   a) the port number;

   b) a protocol field value of "TCP/MSRP", or "TCP/TLS/MSRP" for TLS according to the received SDP offer;

   c) a format list field set to ‘*’;

   d) an "a=recvonly" attribute;

   e) an "a=path" attribute containing its own MSRP URI;

   f) set the content type as a=accept-types: application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload; and

   g) set the a=setup attribute according to IETF RFC 6135 [19].

9.2.3.2.3 MCData client originating procedures

The MCData client shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5] with the clarifications given below.

The MCData client:

1) shall include the g.3gpp.mcdata.sds media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

4) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP INVITE request;

5) should include the "timer" option tag in the Supported header field;

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) if a one-to-one standalone SDS message is to be sent:

   a) shall insert in the SIP INVITE request a MIME resource-lists body with the MCData ID of the invited MCData user, according to rules and procedures of IETF RFC 5366 [18];

   b) shall contain an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

i) the <request-type> element set to a value of "one-to-one-sds"; and

ii) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> element set to the URI of the used functional alias; and

NOTE 0: The MCData client learns the functional aliases that are activated for an MCData ID from procedures specified in subclause 22.2.1.3.

c) if an end-to-end security context needs to be established and the security context does not exist or if the existing security context has expired, then:

i) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];

ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [26];

iii) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect one-to-one communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [26];

iv) shall encrypt the PCK to a UID associated to the MCData client using the MCData ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [26];

v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [26];

vi) shall add the MCData ID of the originating MCData to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]; and

vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCData user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [26];

8) if a group standalone SDS message is to be sent:

a) if the "/<*x*>/<x>/Common/MCData/AllowedSDS" leaf node present in the group document of the requested MCData group, configured on the group management client as specified in 3GPP TS 24.483 [42] is set to "false", shall reject the request to send SDS and not continue with the rest of the steps in this subclause; and

b) shall contain in an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

i) the <request-type> element set to a value of "group-sds";

ii) the <mcdata-request-uri> element set to the MCData group identity;

iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

NOTE 1: The MCData client does not include the MCData ID of the originating MCData user in the body, as this will be inserted into the body of the SIP INVITE request that is sent from the originating participating MCData function.

iv) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, may include the <functional-alias-URI> element set to the URI of the used functional alias;

9) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCData function serving the MCData user;

NOTE 2: The MCData client is configured with public service identity identifying the participating MCData function serving the MCData user.

10) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

11) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 9.2.3.2.1; and

12) shall send the SIP INVITE request towards the MCData server according to 3GPP TS 24.229 [5].

On receipt of a SIP 2xx response to the SIP INVITE request, the MCData client:

1) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5];

2) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38]; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.1.1.2.

On receipt of a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request:

1) shall indicate to the MCData user that the SDS message could not be sent; and

2) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5].

On receipt of an indication from the media plane indicating that the standalone SDS message was not sent successfully, the MCData client shall:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5] with:

   a) Reason code set to "SIP";

   b) cause set to "480"; and

   c) text set to "transmission failed";

2) shall set the Request-URI to the MCData session identity to release; and

3) shall send a SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

On receipt of an indication from the media plane indicating that the standalone SDS message has been successfully transferred, the MCData client shall:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5] with:

   a) Reason code set to "SIP";

   b) cause set to "200"; and

   c) text set to "transmission succeeded";

2) shall set the Request-URI to the MCData session identity to release; and

3) shall send a SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request, the MCData client shall interact with the media plane and indicate to terminate the session, as specified in 3GPP TS 24.582 [15].

9.2.3.2.4 MCData client terminating procedures

Upon receipt of an "initial SIP INVITE request for standalone SDS over media plane for terminating MCData client" request, the MCData client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [5] with the clarifications below.

The MCData client:

1) may reject the SIP INVITE request if either of the following conditions are met:

   a) MCData client does not have enough resources to handle the call; or

   b) any other reason outside the scope of this specification;

   and skip the rest of the steps after step 2;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCData function either with appropriate reject code as specified in 3GPP TS 24.229 [5] and warning texts as specified in subclause 4.9 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

3) if the SDP offer of the SIP INVITE request contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCData ID of the originating MCData user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

   b) shall convert the MCData ID to a UID as described in 3GPP TS 33.180 [26];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [26];

   d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP INVITE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and not continue with rest of the steps in this subclause; and

   e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [26];

NOTE: With the PCK successfully shared between the originating MCData client and the terminating MCData client, both clients are able to create an end-to-end secure session.

3) may display to the MCData user the MCData ID of the inviting MCData user and the type of SDS request;

4) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

5) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

6) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [38]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

7) shall include the g.3gpp.mcdata.sds media feature tag in the Contact header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in the Contact header field of the SIP 200 (OK) response;

9) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [5] with the clarifications given in subclause 9.2.3.2.2; and

10) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of an SIP ACK message to the sent SIP 200 (OK) message, the MCData client shall:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.1.1.3.

9.2.3.3 Participating MCData function procedures

9.2.3.3.1 SDP offer generation

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the participating MCData function:

1) shall contain only one SDP media-level section for SDS message as contained in the received SDP offer; and

2) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value, if present in the received SDP offer.

When composing the SDP offer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the participating MCData function, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced, shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP offer.

9.2.3.3.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCData function, for the accepted media stream in the received SDP offer, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP answer.

9.2.3.3.3 Originating participating MCData function procedures

Upon receipt of a "SIP INVITE request for standalone SDS over media plane for originating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is:

   a) set to a value of "group-sds", shall determine the public service identity of the controlling MCData function associated with the MCData group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request; or

b) set to a value of "one-to-one-sds", shall determine the public service identity of the controlling MCData function hosting the one-to-one standalone SDS over media plane service for the calling user;

5) if unable to identify the controlling MCData function for standalone SDS over media plane, it shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID

a) is authorised for MCData communications by following the procedures in subclause 11.1; and

b) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of subclause 11.1, shall reject the "SIP INVITE request for standalone SDS over media plane for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData communication not authorised to the targeted user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to initiate MCData communications, shall reject the "SIP INVITE request for standalone SDS over media plane for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

8) shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5];

9) shall include the option tag "timer" in the Supported header field;

10) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

11) shall set the Request-URI of the outgoing SIP INVITE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

12) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

12A) if the incoming SIP INVITE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element;

13) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

14) shall set the P-Asserted-Identity in the outgoing SIP INVITE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP INVITE request;

15) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the MCData client as specified in subclause 9.2.3.3.1; and

16) shall send the SIP INVITE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP INVITE request in step 16):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 9.2.3.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

5) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

   c) the isfocus media feature tag;

6) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

7) shall include an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP 200 (OK) response;

8) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

9) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response; and

10) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.2.1.4

11) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5]; and

12) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP INVITE request in step 16) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

9.2.3.3.4 Terminating participating MCData function procedures

Upon receipt of a "SIP INVITE request for standalone SDS over media plane for terminating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCData function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

4) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

4A) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [12]) and:

   i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [12]);

then:

i) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

5) shall generate a SIP INVITE request accordance with 3GPP TS 24.229 [5];

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall include the option tag "timer" in the Supported header field;

8) shall include the following in the Contact header field:

a) the g.3gpp.mcdata.sds media feature tag;

b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”;

c) the isfocus media feature tag;

d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

9) shall include in the SIP INVITE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP INVITE request;

10) shall set the Request-URI of the outgoing SIP INVITE request to the public user identity associated to the MCData ID of the terminating MCData user;

11) shall populate the outgoing SIP INVITE request with the MIME bodies that were present in the incoming SIP INVITE request;

12) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for standalone SDS over media plane for terminating participating MCData function" as specified in subclause 9.2.3.3.1; and

14) shall send the SIP INVITE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 9.2.3.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

5) shall include the following in the Contact header field:

a) the g.3gpp.mcdata.sds media feature tag;

b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

c) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCData function;

6) if the incoming SIP response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

7) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

8) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.2.1.5; and

10) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

9.2.3.4 Controlling MCData function procedures

9.2.3.4.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 4975 [17], IETF RFC 6135 [19] and IETF RFC 6714 [20] the controlling MCData function:

1) shall include an "m=message" media-level section for the MCData media stream received from the originating MCData client consisting of:

a) the port number;

b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;

c) a format list field set to ‘*’;

d) an "a=sendonly" attribute;

e) an "a=path" attribute containing its own MSRP URI;

f) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload"; and

g) set the a=setup attribute as "actpass".

9.2.3.4.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the controlling MCData function:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:

a) the port number;

b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS according to the received SDP offer;

c) a format list field set to ‘*’;

d) an "a=recvonly" attribute;

e) an "a=path" attribute containing its own MSRP URI;

f) set the content type as a=accept-types: application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload; and

g) set the a=setup attribute set to "passive" according to IETF RFC 6135 [19].

9.2.3.4.3 Originating controlling MCData function procedures

This subclause describes the procedures for inviting an MCData user to an MCData session. The procedure is initiated by the controlling MCData function as the result of an action in subclause 9.2.3.4.4.

The controlling MCData function:

1) shall generate a SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the Supported header field set to "timer";

3) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38]. The refresher parameter shall be omitted;

4) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

5) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

6) shall include a Referred-By header field with the public user identity of the inviting MCData client;

7) shall include in the Contact header field an MCData session identity for the MCData session with the g.3gpp.mcdata.sds media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" according to IETF RFC 3840 [16];

8) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

   b) the <mcdata-calling-group-id> element set to the group identity;

9) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

NOTE 1: How the controlling MCData function finds the address of the terminating participating MCData function is out of the scope of the current release.

10) shall set the P-Asserted-Identity header field to the public service identity of the controlling MCData function;

11) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] in the SIP INVITE request;

12) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the originating client according to the procedures specified in subclause 9.2.3.4.1; and

13) shall send the SIP INVITE request towards the terminating client in accordance with 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.1.

NOTE 2: The procedures executed by the controlling MCData function prior to sending a response to the inviting MCData client are specified in subclause 9.2.3.4.4.

9.2.3.4.4 Terminating controlling MCData function procedures

In the procedures in this subclause:

1) MCData ID in an incoming SIP INVITE request refers to the MCData ID of the originating user from the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request;

2) group identity in an incoming SIP INVITE request refers to the group identity from the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request; and

3) MCData ID in an outgoing SIP INVITE request refers to the MCData ID of the called user in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

Upon receipt of a "SIP INVITE request for controlling MCData function for standalone SDS over media plane", the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine if the media parameters are acceptable and the MSRP URI is offered in the SDP offer and if not reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcdata.sds media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

4) shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported;

5) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

6) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-sds" and the SIP INVITE request:

   a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "204 unable to determine targeted user for one-to-one SDS" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

   b) contains an application/resource-lists MIME body with exactly one <entry> element, shall invite the MCData user identified by the <entry> element of the MIME body, as specified in subclause 9.2.3.4.3; and

   c) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.1;

7) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "group-sds":

   a) shall retrieve the necessary group document(s) from the group management server for the group identity contained in the SIP INVITE request and carry out initial processing as specified in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

   b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   c) if the <entry> element of the <list> element of the <list-service> element in the group document does not contain an <mcdata-mcdata-id> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   d) if the <list-service> element contains a <mcdata-allow-short-data-service> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "206 short data

service not allowed for this group" in a Warning header field as specified in subclause 4.x and shall not continue with the rest of the steps;

e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", shall send a SIP 488 (Not Acceptable) response with the warning text set to "207 SDS services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

f) if the MCData server group SDS procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to send group MCData communications on this group identity as determined by step 2) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response, with warning text set to "201 user not authorised to transmit data on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

g) the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP INVITE request, as specified in subclause 6.3.5, shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

h) shall determine targeted group members for MCData communications by following the procedures in subclause 6.3.4;

i) if the procedures in subclause 6.3.4 result in no affiliated members found in the selected MCData group, shall return a SIP 403 (Forbidden) response with the warning text set to "198 no users are affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

j) shall invite each group member determined in step h) above, to the group session, as specified in subclause 9.2.3.4.3; and

k) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.1.

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 9.2.3.4.3 and if the MCData ID in the SIP 200 (OK) response matches to the MCData ID in the corresponding SIP INVITE request. the controlling MCData function:

1) shall generate SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCData function;

5) shall include a SIP URI for the MCData session identity in the Contact header field identifying the MCData session at the controlling MCData function;

6) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

   c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 9.2.3.4.2;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.1; and

10) shall send a SIP 200 (OK) response to the inviting MCData client according to 3GPP TS 24.229 [5].

9.2.4 SDS session

9.2.4.1 General

The procedures in the subclauses of the parent subclause are used by a MCData functional entity to establish:

- a one-to-one SDS session; or
- a group SDS session.

The procedures in the subclauses of the parent subclause are applicable to establish an on-demand SDS session.

9.2.4.2 MCData client procedures

9.2.4.2.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 4975 [17], IETF RFC 6135 [19] and IETF RFC 6714 [20] the MCData client:

1) shall include an "m=message" media-level section for the MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;
   c) an "a=sendrecv" attribute;
   d) an "a=path" attribute containing its own MSRP URI;
   e) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload"; and
   f) set the a=setup attribute as "actpass"; and
2) if end-to-end security is required for a one-to-one communication and the security context does not exist or if the existing security context has expired, shall include the MIKEY-SAKKE I_MESSAGE in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP offer as specified in IETF RFC 4567 [45].

9.2.4.2.2 SDP answer generation

When the MCData client receives an initial SDP offer for an MCData SDS session, the MCData client shall process the SDP offer and shall compose an SDP answer according to 3GPP TS 24.229 [5] and IETF RFC 4975 [17].

When composing an SDP answer, the MCData client:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS according to the received SDP offer;
   c) an "a=sendrecv" attribute;
   d) an "a=path" attribute containing its own MSRP URI;
   e) set the content type as a=accept-types: application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload; and
   f) set the a=setup attribute according to IETF RFC 6135 [19].

9.2.4.2.3 MCData client originating procedures

The MCData client shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5] with the clarifications given below.

The MCData client:

1) shall include the g.3gpp.mcdata.sds media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

4) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP INVITE request;

5) should include the "timer" option tag in the Supported header field;

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) if a one-to-one SDS session is requested:

   a) shall insert in the SIP INVITE request a MIME resource-lists body with the MCData ID of the invited MCData user, according to rules and procedures of IETF RFC 5366 [18];

   b) shall contain an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

      i) the <request-type> element set to a value of "one-to-one-sds-session"; and

      ii) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> element set to the URI of the used functional alias; and

NOTE 0: The MCData client learns the functional aliases that are activated for an MCData ID from procedures specified in subclause 22.2.1.3.

   c) if an end-to-end security context needs to be established and the security context does not exist or if the existing security context has expired, then:

      i) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];

      ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [26];

      iii) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect one-to-one communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [26];

      iv) shall encrypt the PCK to a UID associated to the MCData client using the MCData ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [26];

      v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [26];

      vi) shall add the MCData ID of the originating MCData to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]; and

vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCData user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [26];

8) if a group SDS session is requested:

   a) if the "/<*x*>/<x>/Common/MCData/AllowedSDS" leaf node present in the group document of the requested MCData group, configured on the group management client as specified in 3GPP TS 24.483 [42] is set to "false", shall reject the request to send SDS and not continue with the rest of the steps in this subclause; and

   b) shall contain in an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

      i) the <request-type> element set to a value of "group-sds-session";

      ii) the <mcdata-request-uri> element set to the MCData group identity; and

      iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client;

NOTE 1: The MCData client does not include the MCData ID of the originating MCData user in the body, as this will be inserted into the body of the SIP INVITE request that is sent from the originating participating MCData function.

      iv) if the MCData client is aware of active functional aliases, and an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> set to the URI of the used functional alias;

9) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCData function serving the MCData user;

NOTE 2: The MCData client is configured with public service identity identifying the participating MCData function serving the MCData user.

10) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

11) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 9.2.4.2.1; and

12) shall send the SIP INVITE request towards the MCData server according to 3GPP TS 24.229 [5].

On receipt of a SIP 2xx response to the SIP INVITE request, the MCData client:

1) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5];

2) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38]; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.1.2.2.

On receipt of a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request, the MCData client:

1) shall indicate to the MCData user that the SDS message could not be sent; and

2) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5].

On receipt of an indication from the media plane indicating that the SDS message was not sent successfully, the MCData client:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5] with:

   a) Reason code set to "SIP";

   b) cause set to "480"; and

   c) text set to "transmission failed";

2) shall set the Request-URI to the MCData session identity to release; and

3) shall send a SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

9.2.4.2.4 MCData client terminating procedures

Upon receipt of an "initial SIP INVITE request for SDS session for terminating MCData client"request, the MCData client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [5] with the clarifications below.

The MCData client:

1) may reject the SIP INVITE request if either of the following conditions are met:

   a) MCData client does not have enough resources to handle the call; or

   b) any other reason outside the scope of this specification;

   and skip the rest of the steps after step 2;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCData function either with appropriate reject code as specified in 3GPP TS 24.229 [5] and warning texts as specified in subclause 4.9 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

3) if the SDP offer of the SIP INVITE request contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCData ID of the originating MCData user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

   b) shall convert the MCData ID to a UID as described in 3GPP TS 33.180 [26];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [26];

   d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP INVITE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and not continue with rest of the steps in this subclause; and

   e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [26];

NOTE: With the PCK successfully shared between the originating MCData client and the terminating MCData client, both clients are able to create an end-to-end secure session.

4) may display to the MCData user the MCData ID of the inviting MCData user and the type of SDS request;

5) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

6) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

7) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [38]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

8) shall include the g.3gpp.mcdata.sds media feature tag in the Contact header field of the SIP 200 (OK) response;

9) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" in the Contact header field of the SIP 200 (OK) response;

10) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [5] with the clarifications given in subclause 9.2.4.2.2; and

11) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of an SIP ACK message to the sent SIP 200 (OK) message, the MCData client shall:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.1.2.3.

To send a disposition notification after the media plane is released, the MCData client:

1) shall follow the procedures described in subclause 12.2.1.1.

9.2.4.3 Participating MCData function procedures

9.2.4.3.1 SDP offer generation

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the participating MCData function:

1) shall contain only one SDP media-level section for SDS message as contained in the received SDP offer;and

2) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value, if present in the received SDP offer.

When composing the SDP offer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the participating MCData function, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced, shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP offer.

9.2.4.3.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCData function, for the accepted media stream in the received SDP offer, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP answer.

9.2.4.3.3 Originating participating MCData function procedures

Upon receipt of a "SIP INVITE request for SDS session for originating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is:

   a) set to a value of "group-sds-session", shall determine the public service identity of the controlling MCData function associated with the MCData group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request; or

   b) set to a value of "one-to-one-sds-session", shall determine the public service identity of the controlling MCData function hosting the one-to-one SDS session service for the calling user;

5) if unable to identify the controlling MCData function for SDS session, it shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID

   a) is not allowed to send MCData communications as determined by step 1) of subclause 11.1, shall reject the "SIP INVITE request for SDS session for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "221 user not authorised to initiate one-to-one SDS session" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   b) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of subclause 11.1, shall reject the "SIP INVITE request for SDS session for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData communication not authorised to the targeted user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

8) shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5];

9) shall include the option tag "timer" in the Supported header field;

10) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

11) shall set the Request-URI of the outgoing SIP INVITE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

12) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

12A) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the

<functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element;

13) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

14) shall set the P-Asserted-Identity in the outgoing SIP INVITE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP INVITE request;

15) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the MCData client as specified in subclause 9.2.4.3.1; and

16) shall send the SIP INVITE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP INVITE request in step 16):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 9.2.4.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

5) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

   c) the isfocus media feature tag;

6) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

7) shall include an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP 200 (OK) response;

8) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

9) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response; and

10) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.2.2.4;

11) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5]; and

12) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP INVITE request in step 16) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

9.2.4.3.4 Terminating participating MCData function procedures

Upon receipt of a "SIP INVITE request for SDS session for terminating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCData function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

4) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

4A) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [12]) and:

   i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

   ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [12]);

   then:

   i) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

5) shall generate a SIP INVITE request accordance with 3GPP TS 24.229 [5];

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall include the option tag "timer" in the Supported header field;

8) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”;

   c) the isfocus media feature tag;

   d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

   e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

9) shall include in the SIP INVITE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP INVITE request;

10) shall set the Request-URI of the outgoing SIP INVITE request to the public user identity associated to the MCData ID of the terminating MCData user;

11) shall populate the outgoing SIP INVITE request with the MIME bodies that were present in the incoming SIP INVITE request;

12) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for SDS session for terminating participating MCData function" as specified in subclause 9.2.4.3.1; and

14) shall send the SIP INVITE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 9.2.4.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

5) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

   c) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCData function;

6) if the incoming SIP response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

7) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

8) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.2.2.5; and

10) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

9.2.4.4 Controlling MCData function procedures

9.2.4.4.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 4975 [17], IETF RFC 6135 [19] and IETF RFC 6714 [20] the controlling MCData function:

1) shall include an "m=message" media-level section for the MCData media stream received from the originating MCData client consisting of:

   a) the port number;

   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;

c) an "a=sendrecv" attribute;

d) an "a=path" attribute containing its own MSRP URI;

e) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload"; and

f) set the a=setup attribute as "actpass".

9.2.4.4.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the controlling MCData function:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:

   a) the port number;

   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS according to the received SDP offer;

   c) an "a=sendrecv" attribute;

   d) an "a=path" attribute containing its own MSRP URI;

   e) set the content type as a=accept-types: application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload; and

   f) set the a=setup attribute set to "passive" according to IETF RFC 6135 [19].

9.2.4.4.3 Originating controlling MCData function procedures

This subclause describes the procedures for inviting an MCData user to an MCData session. The procedure is initiated by the controlling MCData function as the result of:

- an action in subclause 9.2.4.4.4; or
- for group SDS session, when an MCData client successfully affiliates the MCData group after the SDS session has been established.

The controlling MCData function:

1) shall generate a SIP INVITE according to 3GPP TS 24.229 [5];

2) shall include the Supported header field set to "timer";

3) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38]. The refresher parameter shall be omitted;

4) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

5) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

6) shall include a Referred-By header field with the public user identity of the inviting MCData client;

7) shall include in the Contact header field an MCData session identity for the MCData session with the g.3gpp.mcdata.sds media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" according to IETF RFC 3840 [16];

8) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

   b) the <mcdata-calling-group-id> element set to the group identity if the request is for group sds;

9) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

NOTE 1: How the controlling MCData function finds the address of the terminating participating MCData function is out of the scope of the current release.

10) shall set the P-Asserted-Identity header field to the public service identity of the controlling MCData function;

11) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] in the SIP INVITE request;

12) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the originating client according to the procedures specified in subclause 9.2.4.4.1; and

13) shall send the SIP INVITE request towards the terminating client in accordance with 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.2.

NOTE 2: The procedures executed by the controlling MCData function prior to sending a response to the inviting MCData client are specified in subclause 9.2.4.4.4.

9.2.4.4.4 Terminating controlling MCData function procedures

In the procedures in this subclause:

1) MCData ID in an incoming SIP INVITE request refers to the MCData ID of the originating user from the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request;

2) group identity in an incoming SIP INVITE request refers to the group identity from the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request; and

3) MCData ID in an outgoing SIP INVITE request refers to the MCData ID of the called user in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

Upon receipt of a "SIP INVITE request for controlling MCData function for SDS session", the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine if the media parameters are acceptable and the MSRP URI is offered in the SDP offer and if not reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcdata.sds media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

4) shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported;

6) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

7) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-sds-session" and the SIP INVITE request:

   a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text

set to "204 unable to determine targeted user for one-to-one SDS" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

b) contains an application/resource-lists MIME body with exactly one <entry> element, shall invite the MCData user identified by the <entry> element of the MIME body, as specified in subclause 9.2.4.4.3; and

c) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.2;

8) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "group-sds-session":

a) shall retrieve the necessary group document(s) from the group management server for the group identity contained in the SIP INVITE request and carry out initial processing as specified in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

c) if the <entry> element of the <list> element of the <list-service> element in the group document does not contain an <mcdata-mcdata-id> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

d) if the <list-service> element contains a <mcdata-allow-short-data-service> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "206 short data service not allowed for this group" in a Warning header field as specified in subclause 4.x and shall not continue with the rest of the steps;

e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds", shall send a SIP 488 (Not Acceptable) response with the warning text set to "207 SDS services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

f) if the MCData server group SDS procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to send group MCData communications on this group identity as determined by step 2) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response, with warning text set to "222 user not authorised to initiate group SDS session on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

g) if the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP INVITE request, as specified in subclause 6.3.5, shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

h) shall determine targeted group members for MCData communications by following the procedures in subclause 6.3.4;

i) if the procedures in subclause 6.3.4 result in no affiliated members found in the selected MCData group, shall return a SIP 403 (Forbidden) response with the warning text set to "198 no users are affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

j) shall invite each group member determined in step g) above, to the group session, as specified in subclause 9.2.4.4.3; and

k) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.2.

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 9.2.4.4.3 and if the MCData ID in the SIP 200 (OK) response matches to the MCData ID in the corresponding SIP INVITE request the controlling MCData function:

1) shall generate SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCData function;

5) shall include a SIP URI for the MCData session identity in the Contact header field identifying the MCData session at the controlling MCData function;

6) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.sds media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.sds”; and

   c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 9.2.4.4.2;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 6.3.2; and

10) shall send a SIP 200 (OK) response to the inviting MCData client according to 3GPP TS 24.229 [5].

9.2.5 SDS communication using pre-established session

9.2.5.1 Common procedure

9.2.5.1.1 Generating an INVITE request on receipt of a REFER request

This subclause is referenced from other procedures.

When generating an initial SIP INVITE request according to 3GPP TS 24.229 [5], on receipt of an incoming SIP REFER request, the participating MCData function:

1) shall include in the SIP INVITE request all header fields included in the headers portion of the SIP URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER request;

2) should include the Session-Expires header field according to IETF RFC 4028 [38].

3) shall include the option tag "timer" in the Supported header field;

4) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP REFER request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

5) shall include the g.3gpp.mcdata.sds media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" into the Contact header field of the outgoing SIP INVITE request;

6) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request; and

7) shall include in the SIP INVITE request the option tag "tdialog" in a Supported header field according to the rules and procedures of IETF RFC 4538 [54];

8) shall include in the SIP INVITE request an SDP offer as specified in subclause 9.2.3.3.1 based upon:

a) the SDP negotiated during the pre-established session establishment and any subsequent pre-established session modification; and

b) the SDP offer (if any) included in the"body" URI parameter of the SIP URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER request for a pre-established session;

9) shall copy the application/vnd.3gpp.mcdata-info+xml MIME body from the "body" URI parameter of the SIP URI in the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field of the SIP REFER request, to the outgoing SIP INVITE request;

9A) if the incoming SIP REFER request contained a <functional-alias-URI> element in an application/vnd.3gpp.mcdata-info+xml MIME body in the hname "body" parameter in the headers portion of the SIP URI in the Refer-To header field, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element; and

10) if the incoming SIP REFER request contained an application/resource-lists MIME body in the "body" URI parameter of the SIP URI contained in the <entry> element of an application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field, shall copy the application/resources-lists MIME body in the "body" URI parameter to the SIP INVITE request.

9.2.5.1.2 Generating Re-INVITE request towards originating MCData client within pre-established session

This subclause is referenced from other procedures.

The participating MCData function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [5] to be sent within the SIP dialog of the pre-established session;

2) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing Re-INVITE request:

a) the <mcdata-communication-state> element with a value set to "establish-success", if a SIP 2xx response is received to a SIP INVITE request sent to the controlling MCData function; or

b) the <mcdata-communication-state> element with a value set to "establish-fail", if an error response is received to a SIP INVITE request sent to the controlling MCData function;

9.2.5.1.3 Generating Re-INVITE request towards terminating MCData client within pre-established session

This subclause is referenced from other procedures.

The participating MCData function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [5] to be sent within the SIP dialog of the pre-established session;

2) should include the Session-Expires header field according to IETF RFC 4028 [38].

3) shall include the option tag "timer" in the Supported header field;

4) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

5) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

6) shall include in the Contact header field an MCData session identity for the MCData session with the g.3gpp.mcdata.sds media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" according to IETF RFC 3840 [16];

9.2.5.2 Initiating one-to-one SDS communication

The procedures in this subclause are used to initiate one-to-one standalone SDS using media plane or one-to-one SDS session within the pre-established session.

9.2.5.2.1 MCData client procedures

9.2.5.2.1.1 Client originating procedures

Upon receiving a request from an MCData user to initiate one-to-one standalone SDS using media plane or one-to-one SDS session within the pre-established session, the MCData client shall generate a SIP REFER request outside a dialog as specified in IETF RFC 3515 [51] as updated by IETF RFC 6665 [36] and IETF RFC 7647 [52], and in accordance with the UE procedures specified in 3GPP TS 24.229 [5], with the clarifications given below.

The MCData client:

1) shall set the Request URI of the SIP REFER request to the session identity of the pre-established session;

2) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [51] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [33] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [18], and with the Content-ID header field set to this "cid" URL;

3) if an end-to-end security context needs to be established and the security context does not exist or if the existing security context has expired, then:

   i) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];

   ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [26];

   iii) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect one-to-one communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [26];

   iv) shall encrypt the PCK to a UID associated to the MCData client using the MCData ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [26];

   v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [26];

   vi) shall add the MCData ID of the originating MCData to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]; and

   vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCData user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [26];

4) shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to MCData ID of the called user, extended with the following parameters in the headers portion of the SIP URI:

NOTE: Characters that are not formatted as ASCII characters are escaped in the following parameters in the headers portion of the SIP URI.

   a) an hname "body" parameter populated with:

      i) an application/sdp MIME body containing an SDP offer with media attributes specified in subclause 9.2.3.2.1, if if a one-to-one standalone SDS message is requested;

      ii) an application/vnd.3gpp.mcdata-info MIME body with:

         A) if a one-to-one standalone SDS message is requested, the <request-type> element set to a value of "one-to-one-sds". If a one-to-one SDS session is requested, the <request-type> element set to a value of "one-to-one-sds-session";

B) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

C) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP REFER request, the <functional-alias-URI> element set to the URI of the used functional alias;

5) shall include a P-Preferred-Service header field set to the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), according to IETF RFC 6050 [7];

6) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

7) shall include the following according to IETF RFC 4488 [53]:

a) the option tag "norefersub" in the Supported header field; and

b) the value "false" in the Refer-Sub header field;

8) shall include a Target-Dialog header field as specified in IETF RFC 4538 [54] identifying the pre-established session;

9) shall include the g.3gpp.mcdata.sds media feature tag in the Contact header field of the SIP REFER request according to IETF RFC 3840 [16]; and

10) shall send the SIP REFER request according to 3GPP TS 24.229 [5].

On receiving a final SIP 2xx response to the SIP REFER request, the MCData client:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

On receiving a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-success":

i) shall notify MCData user about successful the MCData communication establishement;

2) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-fail":

i) shall notify MCData user about the MCData communication establishement failure; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.2.1.2 Client terminating procedrues

Upon receiving a SIP re-INVITE request within a pre-established Session without an associated MCData session, the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-request":

i) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-sds", shall follow the procedures in subclause 9.2.3.2.4; and

ii) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-sds-session", shall follow the procedures in subclause 9.2.4.2.4.

9.2.5.2.2 Participating MCData function procedures

9.2.5.2.2.1 Originating procedures

Upon receiving a SIP REFER request, with:

1) the Request-URI set to a public service identity identifying the pre-established session on the participating MCData function;

2) the Refer-To header field containing a Content-ID ("cid") URL as specified in IETF RFC 2392 [33] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [18] containing one or more <entry> element(s) with a "uri" attribute containing a SIP URI set to the MCData ID of the called user(s);

3) an hname "body" parameter in the headers portion of the SIP URI specified above containing an application/vnd.3gpp.mcdata-info MIME body with the <request-type> element set to "one-to-one-sds" or "one-to-one-sds-session"; and

4) a Content-ID header field set to the "cid" URL;

the participating function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP REFER request;

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

4) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

   i) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to initiate MCData communications, shall reject the SIP REFER request with a SIP 403 (Forbidden) response with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

5) if the received SIP REFER request does not contain an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall reject the SIP REFER request with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

6) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with more than one <entry> element each with an application/vnd.3gpp.mcdata-info MIME body with the <request-type> element set to "one-to-one-sds" or "one-to-one-sds-session", determine that the communication type is one-to-one standalone SDS or one-to-one SDS session;

7) shall determine the public service identity of the controlling MCData function associated with the originating user's MCData ID;

   i) if the participating MCData function is unable to identify the controlling MCData function, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

8) if the SIP REFER request contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [5], IETF RFC 3515 [51] as updated by IETF RFC 6665 [36], and IETF RFC 4488 [53] without establishing an implicit subscription;

9) shall generate a final SIP 200 (OK) response to the SIP REFER request according to 3GPP TS 24.229 [5];

NOTE: In accordance with IETF RFC 4488 [53], the participating MCData function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

10) shall send the response to the SIP REFER request towards the MCData client according to 3GPP TS 24.229 [5];

11) shall generate SIP INVITE request as described in subclause 9.2.5.1.1;

12) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCData function serving the calling MCData user as determined above in step 7); and

13) shall forward the SIP INVITE request according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the participating MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

2) shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.2 with following clarifications:

   i) shall set the Request-URI to a public service identity identifying the pre-established session;

3) shall send the SIP re-INVITE request towards the originating MCData client according to 3GPP TS 24.229 [5]; and

4) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.2.2.2 Terminating procedures

Upon receipt of a "SIP INVITE request for standalone SDS over media plane for terminating participating MCData function" or "SIP INVITE request for SDS session for terminating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the "SIP INVITE request for terminating participating MCData function" with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4], and skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity;

   i) if the binding between the MCData ID and public user identity does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and skip the rest of the steps;

3) shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.3 with following clarifications:

   i) shall set the Request-URI to a public service identity identifying the pre-established session;

   ii) if the incoming SIP INVITE request contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP INVITE request with following clarification:

      a) shall include <mcdata-communication-state> element with a value set to "establish-request"; and

   iii) shall include the following in the Contact header field:

      a) the g.3gpp.mcdata.sds media feature tag;

      b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

      c) the isfocus media feature tag;

      d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

      e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

4) shall send the SIP re-INVITE request towards the terminating MCData client according to 3GPP TS 24.229 [5]; and

5) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.3 Initiating group SDS communication

The procedures in this subclause are used to initiate group standalone SDS using media plane or group SDS session within the pre-established session.

9.2.5.3.1 MCData client procedures

9.2.5.3.1.1 Client originating procedures

Upon receiving a request from an MCData user to initiate group SDS session within the pre-established session, the MCData client shall generate a SIP REFER request outside a dialog as specified in IETF RFC 3515 [51] as updated by IETF RFC 6665 [36] and IETF RFC 7647 [52], and in accordance with the UE procedures specified in 3GPP TS 24.229 [5], with the clarifications given below.

The MCData client:

1) shall set the Request URI of the SIP REFER request to the session identity of the pre-established session;

2) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [51] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [33] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [18], and with the Content-ID header field set to this "cid" URL;

3) shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to the MCData group identity, extended with the following parameters in the headers portion of the SIP URI:

NOTE: Characters that are not formatted as ASCII characters are escaped in the following parameters in the headers portion of the SIP URI.

   a) an hname "body" parameter populated with:

      i) an application/sdp MIME body containing an SDP offer with media attributes specified in subclause 9.2.3.2.1, if if a group standalone SDS message is requested;

      ii) an application/vnd.3gpp.mcdata-info MIME body with:

         A) if a group standalone SDS message is requested, the <request-type> element set to a value of "group-sds". If a group SDS session is requested, the <request-type> element set to a value of "group-sds-session";

         B) the <mcdata-request-uri> element set to the MCData group identity;

         C) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

         D) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP REFER request, the <functional-alias-URI> element set to the URI of the used functional alias;

4) shall include a P-Preferred-Service header field set to the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), according to IETF RFC 6050 [7];

5) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

6) shall include the following according to IETF RFC 4488 [53]:

   a) the option tag "norefersub" in the Supported header field; and

   b) the value "false" in the Refer-Sub header field;

7) shall include a Target-Dialog header field as specified in IETF RFC 4538 [54] identifying the pre-established session;

8) shall include the g.3gpp.mcdata.sds media feature tag in the Contact header field of the SIP REFER request according to IETF RFC 3840 [16]; and

9) shall send the SIP REFER request according to 3GPP TS 24.229 [5].

On receiving a final SIP 2xx response to the SIP REFER request, the MCData client:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

On receiving a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-success":

   i) shall notify MCData user about successful the MCData communication establishement;

2) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-fail":

   i) shall notify MCData user about the MCData communication establishement failure; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.3.1.2 Client terminating procedrues

Upon receiving a SIP re-INVITE request within a pre-established Session without an associated MCData session the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "establish-request":

   i) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "group-sds", shall follow the procedures in subclause 9.2.3.2.4;

   ii) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "group-sds-session", shall follow the procedures in subclause 9.2.4.2.4;

9.2.5.3.2 Participating MCData function procedures

9.2.5.3.2.1 Originating procedures

Upon receiving a SIP REFER request, with:

1) the Request-URI set to a public service identity identifying the pre-established session on the participating MCData function;

2) the Refer-To header field containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [33] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [18] containing one or more <entry> element(s) with a "uri" attribute containing a SIP URI set to the MCData group identity;

3) an hname "body" parameter in the headers portion of the SIP URI specified above containing an application/vnd.3gpp.mcdata-info MIME body with the <request-type> element set to "group-sds" or "group-sds-session"; and

4) a Content-ID header field set to the "cid" URL;

the participating function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP REFER request;

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

4) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

   i) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to initiate MCData communications, shall reject the SIP REFER request with a SIP 403 (Forbidden) response with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

5) if the received SIP REFER request does not contain an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall reject the SIP REFER request with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

6) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with more than one <entry> element each with an application/vnd.3gpp.mcdata-info MIME body with the <request-type> element set to "group-sds", determine that the communication type is group SDS session;

7) shall determine the public service identity of the controlling MCData function associated with the originating user's MCData ID;

   i) if the participating MCData function is unable to identify the controlling MCData function, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

8) if the SIP REFER request contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [5], IETF RFC 3515 [51] as updated by IETF RFC 6665 [36], and IETF RFC 4488 [53] without establishing an implicit subscription;

9) shall generate a final SIP 200 (OK) response to the SIP REFER request according to 3GPP TS 24.229 [5];

NOTE: In accordance with IETF RFC 4488 [53], the participating MCData function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

10) shall send the response to the SIP REFER request towards the MCData client according to 3GPP TS 24.229 [5];

11) shall generate SIP INVITE request as described in subclause 9.2.5.1.1;

12) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCData function servicing for the calling MCData user as determined above in step 7); and

13) shall forward the SIP INVITE request according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the participating MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

2) shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.2 with following clarifications:

   i) shall set the Request-URI to a public service identity identifying the pre-established session;

3) shall send the SIP re-INVITE request towards the originating MCData client according to 3GPP TS 24.229 [5]; and

4) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.3.2.2 Terminating procedures

Upon receipt of a "SIP INVITE request for standalone SDS over media plane for terminating participating MCData function" or "SIP INVITE request for SDS session for terminating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the "SIP INVITE request for terminating participating MCData function" with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4], and skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity;

   i) if the binding between the MCData ID and public user identity does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and skip the rest of the steps;

3) shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.3 with following clarifications:

   i) shall set the Request-URI to a public service identity identifying the pre-established session;

   ii) if the incoming SIP INVITE request contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP INVITE request with following clarification:

      a) shall include <mcdata-communication-state> element with a value set to "establish-request"; and

   iii) shall include the following in the Contact header field:

      a) the g.3gpp.mcdata.sds media feature tag;

      b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

      c) the isfocus media feature tag;

      d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

      e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

4) shall send the SIP re-INVITE request towards the terminating MCData client according to 3GPP TS 24.229 [5]; and

5) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.5.4 Leaving SDS communication

9.2.5.4.1 MCData client procedures

9.2.5.4.1.1 Client originating procedures

Upon receiving a request from an MCData user to leave an MCData session within a pre-established session, the MCData client:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

2) shall generate an initial SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [5], IETF RFC 4488 [53] and IETF RFC 3515 [51] as updated by IETF RFC 6665 [36] and IETF RFC 7647 [r7647];

3) shall set the Request-URI of the SIP REFER request to the public service identity identifying the pre-established session on the MCData server serving the MCData user;

4) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [53];

5) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [53];

6) shall set the Refer-To header field of the SIP REFER request to the MCData session identity to leave;

7) shall include the "method" SIP URI parameter with the value "BYE" in the URI in the Refer-To header field;

8) shall include a Target-Dialog header field as specified in IETF RFC 4538 [54] identifying the pre-established session; and

9) shall send the SIP REFER request according to 3GPP TS 24.229 [5].

Upon receiving a SIP 2xx response to the SIP REFER request, the MCData client shall interact with media plane as specified in 3GPP TS 24.582 [15].

On receiving a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "terminated":

   i) shall notify MCData user about successful the MCData communication termination.

9.2.5.4.1.2 Client terminating procedures

Upon receiving a SIP re-INVITE request within a pre-established Session without an associated MCData session, the MCData client:

1) if the <mcdata-communication-state> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "terminate-request":

   i) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

   ii) shall release all media plane resources corresponding to the MCData communication being released.

9.2.5.4.2 Participating MCData function procedures

9.2.5.4.2.1 Originating procedures

Upon receiving a SIP REFER request with the "method" SIP URI parameter set to value "BYE" in the URI in the Refer-To header field from the MCData client, the participating MCData function:

1) shall determine the MCData ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP REFER request;

2) if the participating MCData function cannot find a binding between the public user identity, then the participating MCData function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps;

3) if the SIP REFER request contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [5], IETF RFC 3515 [53] as updated by IETF RFC 6665 [36], and IETF RFC 4488 [53] without establishing an implicit subscription;

4) shall generate a SIP 200 (OK) response to the SIP REFER request, and in the SIP 200 (OK) response:

   a) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [53]; and

b) shall check the presence of the Refer-Sub header field of the SIP REFER request and if it is present and set to the value "false" shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [53];

5) shall send the SIP 200 (OK) response to the SIP REFER request towards MCData client according to 3GPP TS 24.229 [5];

6) shall generate a SIP BYE request, and in the SIP BYE request:

a) shall set the Request-URI to the MCData session identity which was included at the Refer-To header field of the received REFER request; and

b) shall copy the contents of the P-Asserted-Identity header field of the received REFER request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

7) shall send the SIP BYE request toward the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the participating MCData function shall interact with the media plane as specified in 3GPP TS 24.582 [15] for releasing media plane resources associated with the SIP session with the controlling MCData function. The participating MCData function shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.2 with following clarifications and send the request towards the originating MCData client according to 3GPP TS 24.229 [5]:

1) shall set the Request-URI to a public service identity identifying the pre-established session; and

2) shall set the <mcdata-communication-state> element with a value of "terminated".

9.2.5.4.2.2 Terminating procedures

Upon receiving a SIP BYE request from the controlling MCData function, the participating MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

2) shall send a SIP 200 (OK) response to the controlling MCData function;

3) shall generate a SIP re-INVITE request as specified in subclause 9.2.5.1.2 with following clarifications:

i) shall set the Request-URI to a public service identity identifying the pre-established session; and

ii) shall set the <mcdata-communication-state> element with a value of "terminate-request";

4) shall send the SIP re-INVITE request towards the originating MCData client according to 3GPP TS 24.229 [5]; and

5) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.582 [15].

9.2.6 SDS session using MBMS delivery in the media plane

The procedures for group SDS delivery using MBMS can be seen as extensions of group SDS delivery using unicast session via the media plane.

Group SDS delivery using MBMS enables dynamic toggling between unicast and MBMS delivery at any time during a session, assuming the proper bearers are available. Only the terminating MCData clients and the respective associated MCData terminating participating functions become aware of and involved in the potential MBMS delivery.

The terminating participating function can signal the start/stop/resume MBMS transmissions to the MCData client by using the media control plane Map Group To Bearer and Unmap Group To Bearer messages, described in 3GPP TS 24.582 [15]. The media control plane signaling associates the TMGI of an announced MBMS bearer with the MCData group ID of the communication and with the MBMS transmission parameters (IP address and UDP port).

Guaranteed delivery for SDS when using MBMS can be achieved by the SDS originator through use of dispositions (i.e. "DELIVERED") and SDS NOTIFICATION mechanisms. It is up to the terminating participating function to decide whether or not to use MBMS for a session, and it is possible that the terminating participating function will not use MBMS delivery for SDS messages without the “DELIVERED” disposition.

9.3 Off-network SDS

9.3.1 General

9.3.1.1 Message transport to a MCData Client

In order to transmit an off-network SDS message or SDS notification to an MCData user, the MCData client:

1) shall send the MCData message transported in an MONP MCDATA MESSAGE CARRIER message, specified in TS 24.379 [10], message as a UDP message to the local IP address of the MCData user, on UDP port 8809 (as specified in TS 24,379 [10]), with an IP time-to-live set to 255; and

2) shall treat UDP messages received on the port TBD as received messages.

NOTE: An MCData client that supports IPv6 shall listen to the IPv6 addresses.

9.3.1.2 Message transport to a MCData Group

In order to transmit an off-network SDS message, an SDS notification or any one of the emergency alert messages mentioned in subclause 16.3 to an MCData group, the MCData client:

1) shall send the MCData message transported in a MONP MCDATA MESSAGE CARRIER message, specified in 3GPP TS 24.379 [10], as a UDP message to the multicast IP address of the MCData group, on UDP port 8809, with an IP time-to-live set to 255; and

2) shall treat UDP messages received on the multicast IP address of the MCData group and on port TBD as received messages, with the IP address treated as mentioned in "/<x>/<x>/OffNetwork/MCPTTGroupParameter/<x>/IPMulticastAddress" leaf node within the group configuration specified in 3GPP TS 24.483 [42].

The MONP MCDATA MESSAGE CARRIER message is the entire payload of the UDP message.

9.3.2 Standalone SDS using signalling control plane

9.3.2.1 General

9.3.2.2 Sending SDS message

Upon receiving an indication to send an SDS message, the MCData client:

1) if the request to send the SDS message is for a MCData group, shall check if the value of "/<*x*>/<x>/Common/MCData/AllowedSDS" leaf node, present in the group configuration as specified in 3GPP TS 24.483 [42], is set to "false". It the value is set to "false", shall reject the request to send the SDS message and not continue with the remaining procedures in this subclause;

2) if:

   a) a one-to-one SDS message is to be sent then, shall store the MCData user ID of the intended recipient as the target MCData user ID; or

   b) a group SDS message is to be sent then, shall store the MCData group ID as the target MCData group ID;

3) may set the stored SDS disposition request type as:

   a) "DELIVERY", if only delivery disposition is requested;

   b) "READ", if only read disposition is requested; or

   c) "DELIVERY AND READ", if both delivery and read dispositions are requested;

4) if an existing conversation is indicated then, shall store the conversation identifier of the indicated conversation as SDS conversation ID. Otherwise, shall generate an UUID as described in IETF RFC 4122 [14] and store SDS conversation ID;

5) shall generate an UUID as described in IETF RFC 4122 [14] and store as the SDS message ID;

6) if indicated that the SDS message is in reply to another SDS message then, shall store the message identifier of the indicated message as SDS reply ID;

7) if indicated that the target recipient of the SDS message is an application then, shall store the application ID of the indicated application as the SDS application ID or as the SDS extended application ID;

8) shall store the received payload as the SDS payload;

9) shall store the received payload type as the SDS payload type;

10) shall store the current UTC time as the SDS transmission time;

11) shall generate a SDS OFF-NETWORK MESSAGE message as specified in subclause 15.1.7. In the SDS OFF-NETWORK MESSAGE message, the MCData client:

   a) shall set the Sender MCData user ID IE to its own MCData user ID;

   b) if:

      i) a one-to-one SDS message is to be sent then shall set the Recipient MCData user ID IE to the stored target MCData user ID as specified in subclause 15.2.15; or

      ii) a group SDS message is to be sent then, shall set the MCData group ID IE to the stored target MCData group ID as specified in subclause 15.2.14;

   c) may set the SDS disposition request type IE to the stored the SDS disposition request type as specified in subclause 15.2.3;

   d) shall set the Conversation ID IE to the stored conversation ID as specified in subclause 15.2.9;

   e) shall set the Message ID IE to the stored SDS message ID as specified in subclause 15.2.10;

   f) shall set the Date and time IE to the stored SDS transmission time as specified in subclause 15.2.8;

   g) may include the InReplyTo message ID IE set to the stored SDS reply ID as specified in subclause 15.2.11;

   h) may include:

      i) the Application ID IE set to the stored SDS application ID as specified in subclause 15.2.7; or

      ii) the Extended application ID IE set to the stored SDS extended application ID as specified in subclause 15.2.24;

   i) if end-to-end security is required for a one-to-one communication and the security context does not exist or if the existing security context has expired, shall include the Security parameters and Payload IE with security parameters as described in 3GPP TS 33.180 [26];

   j) if

      i) end-to-end security is not required for a one-to-one communication, or

      ii) sending the SDS OFF-NETWORK MESSAGE message to a MCData group;

      may include the Payload IE as specified in subclause 15.2.13 with:

      i) the Payload content type to the stored SDS payload type; and

      ii) the Payload data set to the stored SDS payload;

12) if:

a) a one-to-one SDS message is to be sent then, shall send the SDS OFF-NETWORK MESSAGE message as specified in subclause 9.3.1.1; or

b) a group SDS message is to be sent then, shall send the SDS OFF-NETWORK MESSAGE message as specified in subclause 9.3.1.2;

13) shall initialise the counter CFS1 (SDS retransmission) with the value set to 1; and

14) shall start timer TFS1 (SDS retransmission).

9.3.2.3 Retransmitting SDS message

Upon expiry of timer TFS1 (SDS retransmission), the MCData client:

1) shall generate a SDS OFF-NETWORK MESSAGE message as specified in subclause 15.1.7. In the SDS OFF-NETWORK MESSAGE message, the MCData client:

   a) shall set the Sender MCData user ID IE to its own MCData user ID;

   b) if:

      i) a one-to-one SDS message is to be sent then, shall set the Recipient MCData user ID IE to the stored target MCData user ID; or

      ii) a group SDS message is to be sent then, shall set the MCData group ID IE to the stored target MCData group ID;

   c) may set the SDS disposition request type IE to the stored the SDS disposition request type as specified in subclause 15.2.3;

   d) shall set the Conversation ID IE to the stored conversation ID as specified in subclause 15.2.9;

   e) shall set the Message ID IE to the stored SDS message ID as specified in subclause 15.2.10;

   f) shall set the Date and time IE to the stored the SDS transmission time as specified in subclause 15.2.8;

   g) may include the InReplyTo message ID IE set to the stored SDS reply ID as specified in subclause 15.2.11;

   h) may include:

      i) the Application ID IE set to the stored SDS application ID as specified in subclause 15.2.7; or

      ii) the Extended application ID IE set to the stored SDS extended application ID as specified in subclause 15.2.24;

   i) if end-to-end security is required for a one-to-one communication and the security context does not exist or if the existing security context has expired, shall include the Security parameters IE with security parameters as described in 3GPP TS 33.180 [26]; and

   j) if:

      i) end-to-end security is not required for a one-to-one communication, or

      ii) sending the SDS OFF-NETWORK MESSAGE message to a MCData group;

      may include the Payload IE as specified in subclause 15.2.13 with:

      i) the Payload content type to the stored SDS payload type; and

      ii) the Payload data set to the stored SDS payload;

2) if:

   a) a one-to-one SDS message was sent then, shall send the SDS OFF-NETWORK MESSAGE message as specified in subclause 9.3.1.1; or

b) a group SDS message was sent then, shall send the SDS OFF-NETWORK MESSAGE message as specified in subclause 9.3.1.2;

3) shall increment the counter CFS1(SDS retransmission) by 1; and

4) shall start timer TFS1 (SDS retransmission) if the associated counter CFS1 (SDS retransmission) has not reached its upper limit.

9.3.2.4 Receiving SDS message

Upon receiving an SDS OFF-NETWORK MESSAGE message with a SDS disposition request type IE, the MCData client:

1) shall store the value of Sender MCData user ID IE as the stored notification target MCData user ID;

2) shall store the value of Conversation ID IE as the stored conversation ID;

3) shall store the value of Message ID IE as the stored SDS message ID;

4) shall store the current UTC time as the stored SDS notification time;

5) if present, shall store the value of Application ID IE as the stored SDS application ID;

6) if present, shall store the value of the Extended application ID IE as the stored SDS extended application ID;

7) if present, shall store the value of MCData group ID IE to the stored target MCData group ID; and

8) if the SDS disposition request type IE is set to:

a) "DELIVERY" then, shall send a SDS OFF-NETWORK NOTIFICATION message as described in subclause 12.3.2;

b) "READ" then, shall send a SDS OFF-NETWORK NOTIFICATION message as described in subclause 12.3.3; or

c) "DELIVERY AND READ" then, shall start timer TFS3 (delivery and read).

NOTE: Duplicate messages (re-transmissions) that are received by the MCData client should not be processed again.

9.3.2.5 SDS Read while TFS3 (delivery and read) is running

Upon receiving a display indication before timer TFS3 (delivery and read) expires, the MCData client:

1) shall generate and send a SDS OFF-NETWORK NOTIFICATION message as described in subclause 12.3.4.

9.3.2.6 Timer TFS3 (delivery and read) expires

Upon expiry of timer TFS3 (delivery and read), the MCData client:

1) shall generate and send a SDS OFF-NETWORK NOTIFICATION message as described in subclause 12.3.2; and

2) upon receiving a display indication, shall generate and send a SDS OFF-NETWORK NOTIFICATION message as described in subclause 12.3.3.

10 File Distribution (FD)

10.1 General

The group administrator can disable the FD service on a MCData group by setting the <mcdata-allow-file-distribution> element under the <list-service> element, in the group document, to "false".

If the <mcdata-allow-file-distribution> element under the <list-service> element, in the group document, is set to "false" for a MCData group:

-- an MCData client should not use the procedures in the subclauses of the parent subclause for FD to the said MCData group.

- a terminating MCData controlling function should reject the request for FD to the said MCData group.

10.2 On-network FD

10.2.1 General

10.2.1.1 Sending an FD message

When the MCData user wishes to send:

- a one-to-one standalone File Distribution (FD) message to another MCData user; or
- a group standalone File Distribution (FD) message to a pre-configured group;

the MCData client:

1) shall follow the procedures in subclause 11.1 for transmission control; and
2) if the procedures in subclause 11.1 are successful:
   a) if requiring to send data without mandatory download, shall follow the procedures in subclause 10.2.4; and
   b) if requiring to send data with mandatory download, shall follow the the procedures in subclause 10.2.5.

10.2.1.2 Handling of received FD messages

10.2.1.2.1 Initial processing of the received FD message

When a MCData client has received a SIP request containing an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1, the MCData Client:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;
2) if the application/vnd.3gpp.mcdata-signalling MIME body does not contain an FD SIGNALLING PAYLOAD message as specified in subclause 15.1.3, shall exit this subclause;
3) if more than one Payload IE is included in the FD SIGNALLING PAYLOAD message, shall exit this subclause;
4) if the Payload content type in the Payload IE in the FD SIGNALLING PAYLOAD message is not set to "FILEURL", shall exit this subclause;
5) if the FD SIGNALLING PAYLOAD message contains a Mandatory download IE set to the value of "MANDATORY DOWNLOAD" shall follow the procedures in subclause 10.2.1.2.2; and
6) if the FD SIGNALLING PAYLOAD message does not contain a Mandatory download IE, shall follow the procedures in subclause 10.2.1.2.3.

10.2.1.2.2 Mandatory Download

The MCData client:

1) if the FD SIGNALLING PAYLOAD message contains a new Conversation ID, shall instantiate a new conversation with the Message ID in the FD SIGNALLING PAYLOAD identifying the first message in the conversation thread;

2) if the FD SIGNALLING PAYLOAD message contains an existing Conversation ID and:

   a) if the FD SIGNALLING PAYLOAD message does not contain an InReplyTo message ID, shall use the Message ID in the FD SIGNALLING PAYLOAD to identify a new message in the existing conversation thread; and

   b) if the FD SIGNALLING PAYLOAD message contains an InReplyTo message ID, shall associate the message to an existing message in the conversation thread as identified by the InReplyTo message ID in the FD SIGNALLING PAYLOAD, and use the Message ID in the FD SIGNALLING PAYLOAD to identify the new message;

3) may store the Conversation ID, Message ID, InReplyTo message ID and Date and time in local storage;

4) if the FD SIGNALLING PAYLOAD message does not contain an Application ID IE and does not contain an Extended application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is for user consumption;

   b) shall notify the user or application that the file identified by file URL in the Payload data in the Payload IE will be downloaded automatically; and

   c) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the user or application;

5) if the FD SIGNALLING PAYLOAD message contains an Application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is not for user consumption;

   b) if the Application ID value is unknown, shall discard the FD message and exit this subclause;

   c) if the Application ID value is known, shall notify the application that the file identified by file URL in the Payload data in the Payload IE will be downloaded automatically; and

NOTE 1: If the FD request is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application. Subsequent automatic download of the file is then started and the file is delivered to that application.

   d) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the application;

6) if the FD SIGNALLING PAYLOAD message contains an Extended application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is not for user consumption;

   b) if the Extended application ID value is unknown, shall discard the FD message and exit this clause;

   c) if the Extended application ID value is known, shall notify the application that the file identified by file URL in the Payload data in the Payload IE will be downloaded automatically; and

NOTE 2: If the FD request is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application. Subsequent automatic download of the file is then started and the file is delivered to that application.

   d) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the application;

7) shall generate an FD NOTIFICATION indicating acceptance of the FD request as specified in subclause 12.2.1.1;

8) shall attempt to download the file as identified by the file URL in the Payload IE in the FD SIGNALLING PAYLOAD message, as specified in subclause 10.2.3.1; and

9) if the received FD SIGNALLING PAYLOAD message contains an FD disposition request type IE requesting a file download completed update indication, then after the file has been successfully downloaded, shall generate an FD NOTIFICATION indicating file download completed, by following the procedures in subclause 12.2.1.1.

10.2.1.2.3 Non-Mandatory download

The MCData client:

1) if the FD SIGNALLING PAYLOAD message does not contain an Application ID IE and does not contain an Extended application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is for user consumption;

   b) shall notify the user about the incoming FD request; and

   c) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the user;

2) if the FD SIGNALLING PAYLOAD message contains an Application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is not for user consumption;

   b) if the Application ID value is unknown, shall discard the FD message and exit this subclause;

   c) if the Application ID value is known, shall notify the application of the incoming FD request; and

NOTE 1: If FD request is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application.

   d) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the application;

2A) if the FD SIGNALLING PAYLOAD message contains an Extended application ID IE:

   a) shall determine that the payload contained in the Payload IE in the FD SIGNALLING PAYLOAD message is not for user consumption;

   b) if the Extended application ID value is unknown, shall discard the FD message and exit this clause;

   c) if the Extended application ID value is known, shall notify the application of the incoming FD request; and

NOTE 2: If the FD request is addressed to a non-MCData application that is not running, the MCData client starts the local non-MCData application.

   d) if the FD SIGNALLING PAYLOAD message contains a Metadata IE, shall deliver the contents of the Metadata IE to the application;

3) shall start a timer TDU2 (FD non-mandatory download timer) with the timer value as specified in subclause F.2.3;

4) shall wait for the user or application to request to download the file indicated by file URL in the Payload data in the Payload IE in the FD SIGNALLING PAYLOAD message;

5) if the user or application accepts or rejects or decides to defer the FD request, shall stop timer TDU2 (FD non-mandatory download timer);

6) if the user defered the FD request while the timer TDU2 (FD non-mandatory download timer) was running, shall generate an FD NOTIFICATION indicating deferral of the FD request as specified in subclause 12.2.1.1;

NOTE 3: Once the timer TDU2 (FD non-mandatory download timer) has expired the FD request can only be accepted or rejected with an appropriate action by the MCData client.

NOTE 4: Once the timer TDU2 (FD non-mandatory download timer) has expired, no action is taken by the MCData client if the FD request is deferred.

7) if the user or application rejects the FD request, shall generate an FD NOTIFICATION indicating rejection of the FD request as specified in subclause 12.2.1.1 and shall exit this subclause; and

8) if the user accepts the FD request:

   a) shall generate an FD NOTIFICATION indicating acceptance of the FD request as specified in subclause 12.2.1.1;

   b) if the FD SIGNALLING PAYLOAD message contains a new Conversation ID, shall instantiate a new conversation with the Message ID in the FD SIGNALLING PAYLOAD identifying the first message in the conversation thread;

   c) if the FD SIGNALLING PAYLOAD message contains an existing Conversation ID and:

      i) if the FD SIGNALLING PAYLOAD message does not contain an InReplyTo message ID, shall use the Message ID in the FD SIGNALLING PAYLOAD to identify a new message in the existing conversation thread; and

      ii) if the FD SIGNALLING PAYLOAD message contains an InReplyTo message ID, shall associate the message to an existing message in the conversation thread as identified by the InReplyTo message ID in the FD SIGNALLING PAYLOAD, and use the Message ID in the FD SIGNALLING PAYLOAD to identify the new message;

   d) may store the Conversation ID, Message ID, InReplyTo message ID and Date and time in local storage;

   e) shall attempt to download the file as identified by the file URL in the Payload IE in the FD SIGNALLING PAYLOAD message, as specified in subclause 10.2.3.1; and

   f) if the received FD SIGNALLING PAYLOAD message contains an FD disposition request type IE requesting a file download completed update, then after the file download has been successfully downloaded, shall generate an FD NOTIFICATION by following the procedures in subclause 12.2.1.1.

10.2.1.3 Discovery of the Absolute URI of the media storage function

10.2.1.3.1 General

In order to upload a file to the media storage function on the controlling MCData function, the MCData UE if not aware of the absolute URI of the media storage function, discovers the absolute URI of the media storage function.

10.2.1.3.2 Void

10.2.1.3.3 Participating MCData function procedures

On receipt of a "SIP MESSAGE request for absolute URI discovery request for participating MCData function", the originating participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE request;

NOTE 1: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is "msf-disc-req":

   a) if the application/vnd.3gpp.mcdata-info+xml MIME body does not contain a MCData group ID, shall determine the public service identity of the controlling MCData function hosting the one-to-one FD using HTTP service for the calling user; and

   b) if the application/vnd.3gpp.mcdata-info+xml MIME body contains a MCData group ID, shall determine the public service identity of the controlling MCData function hosting the group standalone FD using HTTP service, associated with the MCData group identity in the <mcdata-calling-group-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request;

5) if unable to identify the controlling MCData function, it shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request does not contain a <mcdata-calling-group-id> element or the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to send MCData communications as determined by step 1) of subclause 11.1, shall reject the "SIP MESSAGE request for and absolute URI discovery request for participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

8) shall generate a SIP MESSAGE request accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

9) shall copy all MIME bodies included in the incoming SIP MESSAGE request to the outgoing SIP MESSAGE request;

10) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

11) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

12) shall set the Request-URI of the outgoing SIP MESSAGE request to the public user identity of the controlling MCData function as determined by step 4) in this subclause;

13) shall set the P-Asserted-Identity header field of the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

14) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP MESSAGE request in step 14):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the originating MCData client according to 3GPP TS 24.229 [5].

On receipt of a "SIP MESSAGE request for absolute URI discovery response for the participating function", the participating MCData function shall: forward the SIP MESSAGE request to the originating MCData client.

Upon receipt of a SIP 200 (OK) response in response to the forwarded SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

10.2.1.3.4 Controlling MCData function procedures

Upon receiving a "SIP MESSAGE request for absolute URI discovery request" message, the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4]. Otherwise, continue with the rest of the steps;

2) if the SIP MESSAGE does not contain an application/vnd.3gpp.mcdata-info+xml MIME body, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "199 expected MIME bodies not in the request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

3) shall decode the contents of the application/vnd.3gpp.mcdata-info+xml MIME body contained in the SIP MESSAGE;

4) if the <mcdata-calling-group-id> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is present:

   a) shall retrieve the group document associated with the group identity in the SIP MESSAGE request by following the procedures in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

   b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   c) if the <list> element of the <list-service> element in the group document does not contain an <entry> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   d) if the <list-service> element contains a<mcdata-allow-file-distribution> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "213 file distribution not allowed for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", shall send a SIP 488 (Not Acceptable) response with the warning text set to "214 FD services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   f) if the MCData server group FD procedures in subclause 11.1 indicate that the user identified by the MCData ID:

      i) is not allowed to send group MCData communications on this group identity as determined by step 1) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "201 user not authorised to transmit data on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

      ii) the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP MESSAGE request, as specified in subclause 6.x.x, shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

5) shall generate a SIP 200 (OK) response in response to the "SIP MESSAGE request for absolute URI discovery request for controlling MCData function";

6) shall send the SIP 200 (OK) response towards the originating participating MCData function according to 3GPP TS 24.229 [5]; and

7) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. In the generation of the SIP MESSAGE request, the controlling MCData function:

   a) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

   b) shall identify the absolute URI of the media storage function associated with the controlling function:

   c) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

   d) shall include an application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, following the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message, with:

      i) a <request-type> element containing the value "msf-disc-res"; and

      ii) an <mcdata-controller-psi> element set to the absolute URI of the media storage function if in step b) above;

   e) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the participating MCData function associated to the MCData ID of the originating user mentioned in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request; and

   f) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request; and

8) shall send the SIP MESSAGE request towards the participating MCData function as specified in 3GPP TS 24.229 [5].

10.2.2 File upload using HTTP

10.2.2.1 Media storage client procedures

The media storage client shall determine the value of the absolute URI associated with the media storage function of the MCData content server from the <MCDataContentServerURI> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]).

The media storage client shall send HTTP requests over a TLS connection as specified for the HTTP client in the UE in annex A of 3GPP TS 24.482 [24].

NOTE 1: The HTTP client encodes the MCData ID in the bearer access token of the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

NOTE 2: The HTTP client always sends the HTTP requests to an HTTP proxy. Annex A of 3GPP TS 24.482 [24] indicates how the HTTP proxy forwards the HTTP request to the HTTP server.

To upload a file to media storage function on the MCData content server, the media storage client:

1) shall generate an HTTP POST request as specified in IETF RFC 7230 [22] and IETF RFC 7231 [23];

2) shall set the Request-URI to the absolute URI identifying the resource on a media storage function;

3) shall set the Host header field to a hostname identifying the media storage function;

4) shall set the Content-Type header field to multipart/mixed and with a boundary delimiter parameter set to any chosen value;

5) if the file upload is for one-to-one file distribution, shall insert an application/vnd.3gpp.mcdata-info+xml MIME body with:

a) the <request-type> element set to a value of "one-to-one-fd"; and

b) the <mcdata-calling-user-id> element set to the originating MCData ID;

6) if the file upload is for group file distribution, shall insert an application/vnd.3gpp.mcdata-info+xml MIME body with:

a) the <request-type> element set to a value of "group-fd";

b) the <mcdata-request-uri> element set to the MCData group identity; and

c) the <mcdata-calling-user-id> element set to the originating MCData ID;

7) if end-to-end security is required for a one-to-one communication, the MCData client protects the binary data representing the file and prefixes the protected binary data with security parameters as described in 3GPP TS 33.180 [26];

8) if

i) end-to-end security is not required for a one-to-one communication, or

ii) the file upload is for group file distribution;

shall include the binary data representing the file with Content-Type field set to application/octet-stream and Content-Length field set to the file size; and

9) shall send the HTTP POST request towards the media storage function.

On receipt of a HTTP 201 Created containing a Location header field with a URL identifying the location of the resource where the file has been stored on the media storage function, then the media storage client shall store this information.

10.2.2.2 Media storage function procedures

The media storage function on the MCData content server shall act as an HTTP server as defined in annex A of 3GPP TS 24.482 [24].

NOTE: The HTTP server validates the MCData ID in the bearer access token of the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

On receipt of an HTTP POST request with a Request-URI identifying a resource on the media storage function, the media storage function:

1) shall decode the contents of application/vnd.3gpp.mcdata-info+xml MIME body:

a) if the user indicated by <mcdata-calling-user-id> element is not allowed to upload files due to transmission control policy, shall return a HTTP 403 Forbidden response and not continue with the remaining steps in this subclause;

b) If the <request-type> element is set to:

a) "one-to-one-fd" and the Content-Length header under application/octet-stream MIME is greater than <max-data-size-fd-bytes> element present in the service configuration document as specified in 3GPP TS 24.484 [12], shall generate and send a HTTP 413 Payload Too Large response and not continue with the remaing steps in this subclause;

b) "group-fd":

i) shall retrieve the group document associated with the group identity indicated in the <mcdata-request-uri> element by following the procedures in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

ii) if the Content-Length header under application/octet-stream MIME is greater than <mcdata-on-network-max-data-size-for-FD> element present in the group document retrieved in step i), shall generate and send a HTTP 413 Payload Too Large response and not continue with the remaing steps in this subclause;

Editor's Note: [CR 0133, WI eMCData2] it is FFS to determine how the MCData content server will apply transmission control policy by accessing the configuration documents (e.g service configuration and group configuration) from the MCData server.

2) shall process the HTTP POST request by following the procedures in IETF RFC 7230 [22] and IETF RFC 7231 [23] with the following clarifications:

   a) shall store the file in the resource location as identified by the Request-URI; and

   b) shall generate and send a HTTP 201 Created response containing a Location header field with a URL identifying the location of the stored file.

10.2.3 File download using HTTP

10.2.3.1 Media storage client procedures

The media storage client shall send HTTP requests over a TLS connection as specified for the HTTP client in the UE, in annex A of 3GPP TS 24.482 [24].

NOTE 1: The HTTP client encodes the MCData ID in the bearer access token of the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

NOTE 2: The HTTP client always sends the HTTP requests to an HTTP proxy. Annex A of 3GPP TS 24.482 [24] indicates how the HTTP proxy forwards the HTTP request to the HTTP server.

To download a file from the media storage function on the MCData content server, the media storage client:

1) shall generate an HTTP GET request as specified in IETF RFC 7230 [22] and IETF RFC 7231 [23] with a Request-URI set to an absolute URI identifying the URL of the file being requested from the media storage function on the MCData content server; and

2) shall send the HTTP GET request towards the media storage function on the MCData content server.

On receipt of a HTTP 200 OK response containing the requested file, the MCData client shall notify the user or application that the file has been successfully downloaded.

10.2.3.2 Media storage function procedures

The media storage function on the MCData content server shall act as an HTTP server as defined in annex A of 3GPP TS 24.482 [24].

NOTE 1: The HTTP server validates the MCData ID in the bearer access token of the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

On receipt of an HTTP GET request with a Request-URI identifying a file, the media storage function on the MCData content server:

1) if the MCData user is not allowed to download files due to reception control policy, shall return an HTTP 403 Forbidden response;

2) shall process the HTTP GET request by following the procedures in IETF RFC 7230 [22] and IETF RFC 7231 [23], and shall return a HTTP 200 OK response containing the requested file.

Editor's Note: [CR 0133, WI eMCData2] it is FFS to determine how the MCData content server will apply reception control policy by accessing the configuration documents (e.g service configuration and group configuration) from the MCData server.

10.2.4 FD using HTTP

10.2.4.1 General

The procedures in the subclauses of the parent subclause describe the SIP signalling procedures for:

- one-to-one file distribution using HTTP; and
- group standalone file distribution using HTTP.

When the MCData user wishes to perform file distribution via HTTP, the MCData client:

1) shall check that the file size is less than or equal to the:
   a) <mcdata-on-network-max-data-size-for-FD> element present in the group document retrieved by the group management client as specified in 3GPP TS 24.481 [11], if the file upload is for a group file distribution; or
   b) <max-data-size-fd-bytes> element present in the service configuration document as specified in 3GPP TS 24.484 [12], if the file upload is for a one-to-one file distribution;
2) if the size of the file:
   a) is acceptable for upload as determined by step 1), shall determine the value of the absolute URI associated with the media storage function of the MCData content server from the <MCDataContentServerURI> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]);
   b) is not acceptable for upload, shall not continue with the remaining steps in this subclause;
3) shall request the media storage client to upload the file to the media storage function by following the procedures in subclause 10.2.2.1; and
4) shall initiate an FD request containing a file URL as specified in subclause 10.2.4.2.1.

10.2.4.2 MCData client procedures

10.2.4.2.1 MCData client originating procedures

The MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] with the clarifications given below.

The MCData client:

1) shall build the SIP MESSAGE request as specified in subclause 6.2.4.1;
2) if a one-to-one standalone FD message is to be sent shall insert in the SIP MESSAGE request:
   a) an application/resource-lists+xml MIME body with the MCData ID of the target MCData user, according to rules and procedures of IETF RFC 4826 [9]; and
   b) an application/vnd.3gpp.mcdata-info+xml MIME body with:
      i) a <request-type> element set to a value of "one-to-one-fd"; and
      ii) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> element set to the URI of the used functional alias;
3) if a group standalone FD message is to be sent:
   a) if the "/<*x*>/<x>/Common/MCData/AllowedFD" leaf node present in the group document of the requested MCData group, configured on the group management client as specified in 3GPP TS 24.483 [42] is set to "false", shall reject the request for FD and not continue with the rest of the steps in this subclause; and
   b) shall insert in the SIP MESSAGE request an application/vnd.3gpp.mcdata-info+xml MIME body with:
      i) the <request-type> element set to a value of "group-fd";
      ii) the <mcdata-request-uri> element set to the MCData group identity;
      iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

iv) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> element set to the URI of the used functional alias;

4) shall generate a standalone FD message as specified in subclause 6.2.2.2; and

5) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

10.2.4.2.2 MCData client terminating procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for terminating MCData client", the MCData client:

1) may reject the SIP MESSAGE request if there are not enough resources to handle the SIP MESSAGE request;

2) if the SIP MESSAGE request is rejected in step 1), shall respond towards the participating MCData function with a SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this subclause;

3) shall generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

4) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5]; and

5) shall handle the received message as specified in subclause 10.2.1.2.

10.2.4.3 Participating MCData function procedures

10.2.4.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for originating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the originating user from the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if <mcdata-controller-psi> element is present in the application/vnd.3gpp.mcdata-info+xml, shall use its value as public service identity of the controlling MCData function. Otherwise, if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is:

   a) set to a value of "group-fd", shall determine the public service identity of the controlling MCData function hosting the group standalone FD using HTTP service, associated with the MCData group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request; or

   b) set to a value of "one-to-one-fd", shall determine the public service identity of the controlling MCData function hosting the one-to-one FD using HTTP service for the calling user;

5) if unable to identify the controlling MCData function, it shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if <mcdata-controller-psi> in not present in the application/vnd.3gpp.mcdata-info+xml and if the procedures in subclause 11.1 indicate that the user identified by the MCData ID:

   a) is not allowed to initiate MCData communications as determined by step 1) of subclause 11.1, shall reject the "SIP MESSAGE request for FD using HTTP for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

   b) is not allowed to initiate one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request as determined by step 7) of subclause 11.1, shall reject the "SIP MESSAGE request for FD using HTTP for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "202 user not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   c) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of subclause 11.1, shall reject the "SIP MESSAGE request for FD using HTTP for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData communication not authorised to the targeted user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

8) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

9) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

10) shall copy all MIME bodies included in the incoming SIP MESSAGE request to the outgoing SIP MESSAGE request;

10A) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element;

11) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

12) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

13) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

14) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 202 (Accepted) response in response to the SIP MESSAGE request in step 14):

1) shall generate a SIP 202 (Accepted) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 202 (Accepted) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP MESSAGE request in step 14):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request in step 14) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

10.2.4.3.2 Terminating participating MCData function procedures

Upon receipt of a:

- "SIP MESSAGE request for FD using HTTP for terminating participating MCData function"; or

- "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function";

the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

3) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

4) if the SIP MESSAGE is a "SIP MESSAGE request for FD using HTTP for terminating participating MCData function", and if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message with a FD disposition request type IE, shall store the value of the Conversation ID IE, the value of the Message ID IE and the payload IE in the FD SIGNALLING PAYLOAD message;

5) if the SIP MESSAGE is a "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function", and if FD NETWORK NOTIFICATION message within the application/vnd.3gpp.mcdata-signalling MIME body contains an FD notification type IE with value set as "FILE EXPIRED UNAVAILABLE TO DOWNLOAD" as specified in subclause 15.2.6, the file identified using Conversation ID IE shall be removed from the stored file list;

5) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.1;

5A) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [12]) and:

   i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP message does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

   ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [12]);

   then:

   i) shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

6) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request; and

7) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

10.2.4.4 Controlling MCData function procedures

10.2.4.4.1 Originating controlling MCData function procedures

This subclause describes the procedures for sending a SIP MESSAGE from the controlling MCData function and is initiated by the controlling MCData function as a result of an action in subclause 10.2.4.4.2.

The controlling MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

4) shall copy the following MIME bodies in the received SIP MESSAGE request into the outgoing SIP MESSAGE request by following the guidelines in subclause 6.4:

   a) application/vnd.3gpp.mcdata-info+xml MIME body; and

   b) application/vnd.3gpp.mcdata-signalling MIME body;

5) if the application/vnd.3gpp.mcdata-signalling MIME body in the received SIP MESSAGE request contained a FD SIGNALLING PAYLOAD message without the Mandatory download IE included, then:

   a) shall execute the procedures in subclause 11.2;

   b) if the procedures in subclause 11.2 indicate that the mandatory download indication needs to be included,shall include the Mandatory download IE set to a value of "MANDATORY DOWNLOAD" in the FD SIGNALLING PAYLOAD message of the outgoing SIP MESSAGE request;

6) in the application/vnd.3gpp.mcdata-info+xml MIME body:

   a) shall set the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

   b) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request was set to a value of "group-fd", shall set the <mcdata-calling-group-id> element to the group identity;

7) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

8) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request;

9) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd"; and

10) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [5].

10.2.4.4.2 Terminating controlling MCData function procedures

The procedures in this subclause are executed upon:

- receipt of a "SIP MESSAGE request for FD using HTTP for controlling MCData function", the controlling MCData function; or

- a decision to now process a previously received "SIP MESSAGE request for FD using HTTP for controlling MCData function" that had been queued for later transmission;

NOTE 1: The controlling MCData function may postpone the continuation of an FD using HTTP procedure by queuing the received "SIP MESSAGE request for FD using HTTP for controlling MCData function". The management of the queue is specified in Annex B of 3GPP TS 23.282 [2].

the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response or queue the received SIP MESSAGE. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4];

2) if the received SIP MESSAGE request has been queued for later transmission, shall include warning text set to "215 request to transmit is queued by the server" in a Warning header field as specified in subclause 4.9;, in the SIP 202 (Accepted) response and not continue with the remaining steps in this subclause. Otherwise, continue with the rest of the steps;

3) if the SIP MESSAGE does not contain:

   a) an application/vnd.3gpp.mcdata-info+xml MIME body; and

   b) an application/vnd.3gpp.mcdata-signalling MIME body;

   shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "199 expected MIME bodies not in the request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

4) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body contained in the SIP MESSAGE;

5) if the application/vnd.3gpp.mcdata-signalling MIME body does not contain only one FD SIGNALLING PAYLOAD message or FD HTTP TERMINATION message, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "209 one FD SIGNALLING PAYLOAD message or FD HTTP TERMINATION message only must be present in FD request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

6) if the FD SIGNALLING PAYLOAD message or FD HTTP TERMINATION messagedoes not contain only one Payload IE, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "210 Only one File URL must be present in the FD request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

7) if the Payload IE has Payload contents:

   a) with a Payload content type set to a value other than "FILEURL" shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "211 payload for an FD request is not FILEURL" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   b) with Payload data containing a file URL identifying a file that does not exist on the media storage function, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "212 file referenced by file URL does not exist" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

8) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message with a FD disposition request type IE, shall store the value of the Conversation ID IE and the value of the Message ID IE in the FD SIGNALLING PAYLOAD message;

NOTE 2: The controlling MCData function uses the Conversation ID and Message ID for correlation with disposition notifications.

9) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message:

   a) with a Metadata IE, shall derive a timer value for the file availability timer as the minimum of the file availability information in the metadata and the value contained in the <max-file-availability> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12]; and

   b) without a Metadata IE, shall derive a timer value for the file availability timer as the value contained in the <default-file-availability> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12];

10) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is set to a value of "one-to-one-fd" and the SIP MESSAGE request:

   a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "205 unable to determine targeted user for one-to-one FD" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

   b) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message contains an application/resource-lists MIME body with exactly one <entry> element, shall send a SIP MESSAGE request to the MCData user identified in the <entry> element of the MIME body, as specified in subclause 10.2.4.4.1;

11) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD HTTP TERMINATION message:

   a) if the FD HTTP TERMINATION message doesn’t contain Conversation Id or Message Id, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "223 No Conversation ID or Message ID present" and shall not continue with rest of the steps;and

   b) if not identified any transmission with given Conversation ID, Message ID shall send 404 with reason with waring text set to "224 No transmission available" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps;

12) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message and if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request is set to a value of "group-fd":

   a) shall retrieve the group document associated with the group identity in the SIP MESSAGE request by following the procedures in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

   b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   c) if the <entry> element of the <list> element of the <list-service> element in the group document does not contain an <mcdata-mcdata-id> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

   d) if the <list-service> element contains a <mcdata-allow-file-distribution> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "213 file distribution not allowed for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", shall send a SIP 488 (Not Acceptable) response with the warning text set to "214 FD services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

f) if the MCData server group FD procedures in subclause 11.1 indicate that the user identified by the MCData ID:

   i) is not allowed to initiate group MCData communications on this group identity as determined by step 2) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response, with warning text set to "201 user not authorised to transmit data on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   ii) is not allowed to initiate group MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request as determined by step 8) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "208 user not authorised for MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

   iii) is not allowed to initiate group MCData communications on this group identity due to exceeding the maximum allowed file size as determined by step 6) of subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "208 user not authorised for MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

g) if the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP MESSAGE request, as specified in subclause 6.3.5, shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

j) shall determine targeted group members for MCData communications by following the procedures in subclause 6.3.4;

k) if the procedures in subclause 6.3.4 result in no affiliated members found in the selected MCData group, shall return a SIP 403 (Forbidden) response with the warning text set to "198 no users are affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

l) shall send SIP MESSAGE requests to the targeted group members identified in step j) above by following the procedure in subclause 10.2.4.4.1;

13) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message, shall start TDC2 (file availability timer) with the value derived in step 9 of this subclause;

14) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD SIGNALLING PAYLOAD message, shall associate the running timer TDC2 (file availability timer) to the Conversation ID, Message ID, Application ID (if included), and Extended application ID (if included) contained in the FD SIGNALLING PAYLOAD message;

NOTE 3: Multiple file availability timers can be running for a file. Each file availability timer is uniquely associated to a Conversation ID and Message ID.

15) shall generate a SIP 202 (Accepted) response in response to the "SIP MESSAGE request for FD using HTTP for controlling MCData function"; and

16) shall send the SIP 202 (Accepted) response towards the originating participating MCData function according to 3GPP TS 24.229 [5].

17) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD HTTP TERMINATION message and Termination information type IE set to "TERMINATION REQUEST" then:

a) shall identify the FILE transmission with Conversation ID and Message ID and "FILE URL". If any ongoing transmission exist then execute procedure described in subclause 12.4.2.1 withfollowing clarifications:

   i) shall set FD notification type IE as "FILE DELETED UNAVAILABLE TO DOWNLOAD" as specified in subclause 15.2.18;

b) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. In the generation of the SIP MESSAGE request, the controlling MCData function:

   i) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

   ii) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

   iii) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the participating MCData function associated to the MCData ID of the originating user mentioned in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request;

   iv) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request;

   v) shall include an application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, following the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message:

      A) fill <mcdata-request-uri> element from <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml in received SIP MESSAGE;

   vi) shall generate FD HTTP TERMINATION message as described in subclause 6.3.6.1;

   vii) shall set the Termination information type IE set to "TERMINATION RESPONSE" as specified in subclause 15.2.22.

   viii) if clause is successful shall set Release response type IE of FD HTTP TERMINATION MESSAGE to "RELEASE SUCCESS" else set to "RELEASE FAILED" as described in subclause 15.2.23; and

   ix) shall include in the SIP request, the FD HTTP TERMINATION message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1;

c) shall send the SIP MESSAGE request towards the originating participating MCData function as specified in 3GPP TS 24.229 [5]; and

18) if the application/vnd.3gpp.mcdata-signalling MIME body contains an FD HTTP TERMINATION message and Termination information type IE set to other than "TERMINATION REQUEST" then follow procedures described on subclause 13.2.5 and subclause 13.2.6.

10.2.5 FD using media plane

10.2.5.1 General

The procedures in the subclauses of the parent subclause describe the SIP signalling procedures for:

- one-to-one file distribution using media plane; and
- group standalone file distribution using media plane.

10.2.5.2 MCData client procedures

10.2.5.2.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 5547 [69] IETF RFC 6135 [19] and IETF RFC 6714 [20] the MCData client:

1) shall include an "m=message" media-level section for the MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;
   c) an "a=sendonly" attribute;
   d) an "a=path" attribute containing its own MSRP URI;
   e) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling";
   f) set the a=setup attribute as "actpass";
   g) a file-selector attribute containing:
      i) a 'name' selector;
      ii) a 'type' selector;
      iii) a 'size' selector; and
      iv) a 'hash' selector;
   h) a file-date attribute; and
2) if end-to-end security is required for a one-to-one communication and the security context does not exist or if the existing security context has expired, shall include the MIKEY-SAKKE I_MESSAGE in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP offer as specified in IETF RFC 4567 [45].

10.2.5.2.2 SDP answer generation

When the MCData client receives an initial SDP offer for file distribution, the MCData client shall process the SDP offer and shall compose an SDP answer according to 3GPP TS 24.229 [5] and IETF RFC 5547 [69].

When composing an SDP answer, the MCData client:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS according to the received SDP offer;
   c) an "a=recvonly" attribute;
   d) an "a=path" attribute containing its own MSRP URI;
   e) set the content type as a=accept-types:application/vnd.3gpp.mcdata-signalling;
   f) set the a=setup attribute according to IETF RFC 6135 [19]; and
   g) a file-selector attribute containing:
      i) a 'name' selector;
      ii) a 'type' selector;
      iii) a 'size' selector; and
      iv) a 'hash' selector.

10.2.5.2.3 MCData client originating procedures

The MCData client shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5] with the clarifications given below.

The MCData client:

1) shall include the g.3gpp.mcdata.fd media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

4) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP INVITE request;

5) should include the "timer" option tag in the Supported header field;

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall generate and contain an application/vnd.3gpp.mcdata-signalling MIME body with the FD SIGNALLING PAYLOAD as described in subclause 6.2.2.3;

8) if a one-to-one file distribution is requested:

   a) shall insert in the SIP INVITE request a MIME resource-lists body with the MCData ID of the invited MCData user, according to rules and procedures of IETF RFC 5366 [18]; and

   b) shall contain an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

      i) the <request-type> element set to a value of "one-to-one-fd"; and

      ii) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> element set to the URI of the used functional alias;

   c) if an end-to-end security context needs to be established and the security context does not exist or if the existing security context has expired, then:

      i) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];

      ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [26];

      iii) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect one-to-one communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [26];

      iv) shall encrypt the PCK to a UID associated to the MCData client using the MCData ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [26];

      v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [26]; and

      vi) shall add the MCData ID of the originating MCData to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]; and

vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCData user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [26];

9) if a group file distribution is requested:

a) if the "/<*x*>/<x>/Common/MCData/AllowedFD" leaf node present in the group document of the requested MCData group, configured on the group management client as specified in 3GPP TS 24.483 [42] is set to "false", shall reject the request for FD and not continue with the rest of the steps in this subclause; and

b) shall contain in an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

i) the <request-type> element set to a value of "group-fd";

ii) the <mcdata-request-uri> element set to the MCData group identity;

iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

NOTE 1: The MCData client does not include the MCData ID of the originating MCData user in the body, as this will be inserted into the body of the SIP INVITE request that is sent from the originating participating MCData function.

iv) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> element set to the URI of the used functional alias;

10) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCData function serving the MCData user;

NOTE 2: The MCData client is configured with public service identity identifying the participating MCData function serving the MCData user.

11) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

12) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 10.2.5.2.1; and

13) shall send the SIP INVITE request towards the MCData server according to 3GPP TS 24.229 [5].

On receipt of a SIP 2xx response to the SIP INVITE request, the MCData client:

1) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5];

2) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38]; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 10.2.5.1.1..

On receipt of a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request:

1) shall indicate to the MCData user that the file could not be sent; and

2) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5].

On receipt of an indication from the media plane indicating that the file was not sent successfully, the MCData client shall:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5] with:

a) Reason code set to "SIP";

b) cause set to "480"; and

c) text set to "transmission failed";

2) shall set the Request-URI to the MCData session identity to release; and

3) shall send a SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

10.2.5.2.4 MCData client terminating procedures

Upon receipt of an "initial SIP INVITE request for file distribution for terminating MCData client"request, the MCData client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [5] with the clarifications below.

The MCData client:

1) may reject the SIP INVITE request if either of the following conditions are met:

   a) MCData client does not have enough resources to handle the call; or

   b) any other reason outside the scope of this specification;

   and skip the rest of the steps after step 2;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCData function either with appropriate reject code as specified in 3GPP TS 24.229 [5] and warning texts as specified in subclause 4.9 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

3) if the SDP offer of the SIP INVITE request contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCData ID of the originating MCData user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

   b) shall convert the MCData ID to a UID as described in 3GPP TS 33.180 [26];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [26];

   d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP INVITE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and not continue with rest of the steps in this subclause; and

   e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [26];

NOTE: With the PCK successfully shared between the originating MCData client and the terminating MCData client, both clients are able to create an end-to-end secure session.

4) may display to the MCData user the MCData ID of the inviting MCData user;

4A) may display to the MCData user the functional alias of the inviting MCData user, if provided;

5) may display to the MCData user the file meta-data of the incoming file as described by the SDP included in the received SIP INVITE request;

6) if the Mandatory indication IE of the FD SIGNALLING PAYLOAD contained in the application/vnd.3gpp.mcdata-signalling MIME body received in the SIP INVITE request is set to "MANDATORY", then:

   i) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

   ii) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

iii) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [38]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

iv) shall include the g.3gpp.mcdata.fd media feature tag in the Contact header field of the SIP 200 (OK) response;

v) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" in the Contact header field of the SIP 200 (OK) response;

vi) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [5] with the clarifications given in subclause 10.2.5.2.2; and

vii) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of an SIP ACK message to the sent SIP 200 (OK) message, the MCData client shall:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 10.2.5.1.2.

On receipt of an indication from the media plane of the successful download of the file and if the received FD SIGNALLING PAYLOAD message contained an FD disposition request type IE requesting a file download completed update indication, then, the MCData client:

1) shall follow the procedures described in subclause 12.2.1.1.

10.2.5.3 Participating MCData function procedures

10.2.5.3.1 SDP offer generation

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the participating MCData function:

1) shall contain only one SDP media-level section for file distribution as contained in the received SDP offer; and

2) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value, if present in the received SDP offer.

When composing the SDP offer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the participating MCData function, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP answer.

10.2.5.3.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCData function, for the accepted media stream in the received SDP offer, if required; and

NOTE 1: Requirements can exist for the participating MCData function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

NOTE 2: If the participating MCData function and the controlling MCData function are in the same MCData server, and the participating MCData function does not have a dedicated IP address or a dedicated port number for media stream, the replacement of the IP address or the port number is omitted.

2) if the IP address is replaced shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP answer.

10.2.5.3.3 Originating participating MCData function procedures

Upon receipt of a "SIP INVITE request for file distribution for originating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is:

   a) set to a value of "group-fd", shall determine the public service identity of the controlling MCData function associated with the MCData group identity in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request; or

   b) set to a value of "one-to-one-fd", shall determine the public service identity of the controlling MCData function hosting the file distribution service for the calling user;

5) if unable to identify the controlling MCData function for file distribution, it shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID:

   a) is not allowed to initiate MCData communications as determined by step 1) of subclause 11.1, shall reject the "SIP INVITE request for file distribution for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

   b) is not allowed to initiate one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request as determined by step 7) of subclause 11.1, shall reject the "SIP INVITE request for file distribution for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "202 user not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

   c) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of clause 11.1, shall reject the "SIP INVITE request for file distribution for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData

communication not authorised to the targeted user" in a Warning header field as specified in clause 4.9 and shall not continue with the rest of the steps;

8) shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5];

9) shall include the option tag "timer" in the Supported header field;

10) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

11) shall set the Request-URI of the outgoing SIP INVITE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

12) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

12A) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element;

13) shall include in the outgoing SIP INVITE request, the application/vnd.3gpp.mcdata-signalling MIME body that was present in the incoming SIP INVITE request;

14) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

15) shall set the P-Asserted-Identity in the outgoing SIP INVITE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP INVITE request;

16) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the MCData client as specified in subclause 10.2.5.3.1; and

17) shall send the SIP INVITE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP INVITE request in step 16):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 10.2.5.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

5) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.fd media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd"; and

   c) the isfocus media feature tag;

6) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

7) shall include an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP 200 (OK) response;

8) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

9) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response; and

10) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.2.1;

11) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5]; and

12) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP INVITE request in step 16) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

10.2.5.3.4 Terminating participating MCData function procedures

Upon receipt of a "SIP INVITE request for file distribution for terminating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCData function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

4) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

4A) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [12]) and:

   i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]); and

   ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [12]);

   then:

   i) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

5) shall generate a SIP INVITE request accordance with 3GPP TS 24.229 [5];

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall include the option tag "timer" in the Supported header field;

8) shall include the following in the Contact header field:

a) the g.3gpp.mcdata.fd media feature tag;

b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

c) the isfocus media feature tag;

d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

9) shall include in the SIP INVITE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP INVITE request;

10) shall set the Request-URI of the outgoing SIP INVITE request to the public user identity associated to the MCData ID of the terminating MCData user;

11) shall populate the outgoing SIP INVITE request with the MIME bodies that were present in the incoming SIP INVITE request;

12) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for file distribution for terminating participating MCData function" as specified in subclause 10.2.5.3.1; and

14) shall send the SIP INVITE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 10.2.5.3.2;

3) shall include the option tag "timer" in a Require header field;

4) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

5) shall include the following in the Contact header field:

a) the g.3gpp.mcdata.fd media feature tag;

b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd"; and

c) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCData function;

6) if the incoming SIP response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

7) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

8) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.2.2; and

10) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];
2) shall include Warning header field(s) that were received in the incoming SIP response; and
3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

10.2.5.4 Controlling MCData function procedures

10.2.5.4.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 5547 [69] IETF RFC 6135 [19] and IETF RFC 6714 [20] the MCData client:

1) shall include an "m=message" media-level section for the MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;
   c) an "a=sendonly" attribute;
   d) an "a=path" attribute containing its own MSRP URI;
   e) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling";
   f) set the a=setup attribute as "actpass";
   g) a file-selector attribute containing:
      i) a 'name' selector;
      ii) a 'type' selector;
      iii) a 'size' selector; and
      iv) a 'hash' selector; and
   h) a file-date attribute;

10.2.5.4.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the controlling MCData function:

1) shall include an "m=message" media-level section for the accepted MCData media stream consisting of:
   a) the port number;
   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS according to the received SDP offer;
   c) a format list field set to ‘*’;
   d) an "a=recvonly" attribute;
   e) an "a=path" attribute containing its own MSRP URI;
   f) set the content type as a=accept-types:application/vnd.3gpp.mcdata-signalling; and
   g) set the a=setup attribute set to "passive", according to IETF RFC 6135 [19]; and
   h) a file-selector attribute containing:
      i) a 'name' selector;
      ii) a 'type' selector;
      iii) a 'size' selector; and

iv) a 'hash' selector.

10.2.5.4.3 Originating controlling MCData function procedures

This subclause describes the procedures for inviting an MCData user to an MCData session. The procedure is initiated by the controlling MCData function as the result of an action in subclause 10.2.5.4.4.

The controlling MCData function:

1) shall generate a SIP INVITE according to 3GPP TS 24.229 [5];

2) shall include the Supported header field set to "timer";

3) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38]. The refresher parameter shall be omitted;

4) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

5) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

6) shall include a Referred-By header field with the public user identity of the inviting MCData client;

7) shall include in the Contact header field an MCData session identity for the MCData session with the g.3gpp.mcdata.fd media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" according to IETF RFC 3840 [16];

8) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

   b) the <mcdata-calling-group-id> element set to the group identity if the request is for group file distribution ;

9) shall include in the outgoing SIP INVITE request, the application/vnd.3gpp.mcdata-signalling MIME body that was present in the incoming SIP INVITE request;

10) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

NOTE 1: How the controlling MCData function finds the address of the terminating participating MCData function is out of the scope of the current release.

11) shall set the P-Asserted-Identity header field to the public service identity of the controlling MCData function;

12) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] in the SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the originating client according to the procedures specified in subclause 10.2.5.4.1; and

14) shall send the SIP INVITE request towards the terminating client in accordance with 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.3.

NOTE 2: The procedures executed by the controlling MCData function prior to sending a response to the inviting MCData client are specified in subclause 10.2.5.4.4.

10.2.5.4.4 Terminating controlling MCData function procedures

In the procedures in this subclause:

1) MCData ID in an incoming SIP INVITE request refers to the MCData ID of the originating user from the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request;

2) group identity in an incoming SIP INVITE request refers to the group identity from the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request; and

3) MCData ID in an outgoing SIP INVITE request refers to the MCData ID of the called user in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

The procedures in this subclause are executed upon:

- receipt of a "SIP INVITE request for controlling MCData function for file distribution"; or

- a decision to now process a previously received "SIP INVITE request for controlling MCData function for file distribution" that had been queued for later transmission;

NOTE 1: The controlling MCData function may postpone the continuation of an FD using media plane procedure by queuing the received "SIP INVITE request for controlling MCData function for file distribution". The management of the queue is specified in Annex B of 3GPP TS 23.282 [2].

the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response or queue the received SIP INVITE. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4];

2) if the received SIP INVITE request has been queued for later transmission, shall include warning text set to "215 request to transmit is queued by the server" in a Warning header field as specified in subclause 4.9, in the SIP 100 (Trying) response, and shall send the SIP 100 (TRYING) response towards the originating participating MCData function according to 3GPP TS 24.229 [5] and not continue with the remaining steps in this subclause. Otherwise, continue with the rest of the steps;

3) shall determine if the media parameters are acceptable and the MSRP URI is offered in the SDP offer and if not reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

4) if the incoming SIP INVITE request does not contain an application/vnd.3gpp.mcdata-signalling MIME body with the FD SIGNALLING PAYLOAD as described in subclause 6.2.2.3, shall reject the SIP INVITE request with appropriate reject code;

5) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcdata.fd media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

6) shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported;

7) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

8) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-fd" and:

   a) the conditions in subclause 11.1 indicate that the MCData user is not allowed to initiate FD communications due to file size exceeding allowed limits as determined by step 4) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "220 user not authorised for FD communications due to file size" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

NOTE 2: The size of the file intended for transfer over the media plane is obtained from the 'size' selector of the file-selector attribute in the received SDP offer.

   b) the SIP INVITE request:

i) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "205 unable to determine targeted user for one-to-one FD " in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

ii) contains an application/resource-lists MIME body with exactly one <entry> element, shall invite the MCData user identified by the <entry> element of the MIME body, as specified in subclause 10.2.5.4.3; and

shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.3;

9) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "group-fd":

a) shall retrieve the necessary group document(s) from the group management server for the group identity contained in the SIP INVITE request and carry out initial processing as specified in subclause 6.3.3, and shall continue with the remaining steps if the procedures in subclause 6.3.3 were successful;

b) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

c) if the <entry> element of the <list> element of the <list-service> element in the group document does not contain an <mcdata-mcdata-id> element with a "uri" attribute matching the MCData ID of the originating user contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP INVITE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

d) if the <list-service> element contains a <mcdata-allow-file-distribution> element in the group document set to a value of "false", shall send a SIP 403 (Forbidden) response with the warning text set to "213 file distribution not allowed for this group" in a Warning header field as specified in subclause 4.x and shall not continue with the rest of the steps;

e) if the <supported-services> element is not present in the group document or is present and contains a <service> element containing an "enabler" attribute which is not set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd", shall send a SIP 488 (Not Acceptable) response with the warning text set to "214 FD services not supported for this group" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

f) if the user identified by the MCData ID:

i) is not allowed to initiate group MCData communications on this group identity as determined by step 2) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response, with warning text set to "201 user not authorised to transmit data on this group identity" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

ii) is not allowed to initiate group MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request as determined by step 8) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "208 user not authorised for MCData communications on this group identity due exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause; and

iii) is not allowed to initiate FD communications on this group identity due to file size exceeding the allowed limits as determined by step 6) of subclause 11.1, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "219 user not authorised for FD communications on this group identity due to file size" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause.

NOTE 3: The size of the file intended for transfer over the media plane is obtained from the 'size' selector of the file-selector attribute in the received SDP offer.

g) if the originating user identified by the MCData ID is not affiliated to the group identity contained in the SIP INVITE request, as specified in subclause 6.3.5, shall return a SIP 403 (Forbidden) response with the

warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

h) shall determine targeted group members for MCData communications by following the procedures in subclause 6.3.4;

j) if the procedures in subclause 6.3.4 result in no affiliated members found in the selected MCData group, shall return a SIP 403 (Forbidden) response with the warning text set to "198 no users are affiliated to this group" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

k) shall invite each group member determined in step h) above, to the group session, as specified in subclause 10.2.5.4.3; and

l) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.3.

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 10.2.5.4.3 and if the MCData ID in the SIP 200 (OK) response matches to the MCData ID in the corresponding SIP INVITE request the controlling MCData function:

1) shall generate SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCData function;

5) shall include a SIP URI for the MCData session identity in the Contact header field identifying the MCData session at the controlling MCData function;

6) shall include the following in the Contact header field:

a) the g.3gpp.mcdata.fd media feature tag;

b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd"; and

c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 10.2.5.4.2;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15] subclause 7.3; and

10) shall send a SIP 200 (OK) response to the inviting MCData client according to 3GPP TS 24.229 [5].

11 Transmission and Reception Control

11.1 General

The MCData functional entities (as specified in subclause 5.2 and subclause 5.3) check if the MCData user is allowed to initiate MCData communications by following the procedures specified below:

1) if the MCData user wishes to send one-to-one MCData communications and the <allow-transmit-data> element of an <actions> element is not present in the MCData user profile document or is present with the value "false" (see the MCData user profile document in 3GPP TS 24.484 [12]), , the MCData client and participating MCData function shall determine that the MCData user is not allowed to send MCData communications and shall not continue with the rest of the steps;

1A) if the MCData user wishes to initiate one-to-one MCData communications, the <One-to-One-Communication> element exists in the MCData user profile document with one more <entry> elements, and the "uri" attribute of the <entry> element of the application/resource-lists MIME body does not match with one of the <entry> elements of the <One-to-One-Communication> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]), the MCData client and participating MCData function shall determine that the MCData user is not allowed to initiate MCData communication to the targeted user and shall not continue with the rest of the steps;

2) if the MCData user wishes to send group MCData communications on an MCData group identity and the <mcdata-allow-transmit-data-in-this-group> element of an <actions> element is not present in the MCData group document or is present with the value "false" as specified in 3GPP TS 24.481 [11], the MCData client and controlling MCData function shall determine that the MCData user is not allowed to send group MCData communications on this group identity, and shall not continue with the rest of the steps;

3) if the MCData user wishes to send one-to-one SDS communications and the size of the payload is greater than the value contained in the <max-data-size-sds-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], the MCData client and controlling MCData function shall determine that the MCData user is not allowed to send SDS communications due to message size and shall not continue with the rest of the steps;

4) if the MCData user wishes to send one-to-one FD communications and the size of the data that the MCData user wishes to send is greater than the value contained in the <max-data-size-fd-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], the MCData client and controlling MCData function shall determine that the MCData user is not allowed to send FD communications due to file size and shall not continue with the rest of the steps;

5) if the MCData user wishes to send group SDS communications on an MCData group identity and the size of the data that the MCData user wishes to send is greater than the value contained in the <mcdata-on-network-max-data-size-for-SDS> element in the MCData group document for the MCData group ID as specified in 3GPP TS 24.481 [11], then the MCData client and the controlling MCData function shall determine that the MCData user is not allowed to send SDS communications on this group identity due to message size and shall not continue with the rest of the steps;

6) if the MCData user wishes to send group FD communications on an MCData group identity and the size of the data that the MCData user wishes to send is greater than the value contained in the <mcdata-on-network-max-data-size-for-FD> element in the MCData group document for the MCData group ID as specified in 3GPP TS 24.481 [11], then the MCData client and the controlling MCData function shall determine that the MCData user is not allowed to send FD communications on this group identity due to file size and shall not continue with the rest of the steps;

7) if the MCData user wishes to send one-to-one MCData communications to another MCData user and the size of the payload is greater than the maximum amount of data that the MCData user can transmit in a single request during one-to-one communications contained in the <MaxData1To1> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [12]), the MCData client and participating MCData function shall determine that the MCData user is not allowed to send one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request and shall not continue with the rest of the steps;

8) if the MCData user wishes to send group MCData communications on an MCData group identity and the size of the payload is greater than the maximum amount of data that the MCData user can transmit in a single request during group communications in the group identified by the MCData group identity in the request contained in the <mcdata-max-data-in-single-request> element of the <entry> element of the MCData group document as specified in 3GPP TS 24.481 [11], the MCData client and the controlling MCData function shall determine that the MCData user is not allowed to send group MCData communications on this group identity due to exceeding the maximum amount of data that can be sent in a single request and shall not continue with the rest of the steps;

9) if the MCData user wishes to initiate a SDS session for later use with one-to-one MCData communications there are no further checks for the MCData client which shall continue at step 11). If, for either the originating user or the terminating user, the <allow-transmit-data> element of an <actions> element is not present in the MCData user profile document or is present with the value "false" (see the MCData user profile document in 3GPP TS 24.484 [12]), the participating MCData function shall determine that the MCData user is not allowed to initiate a SDS session and shall not continue with the rest of the steps;

10) if the MCData user wishes to initiate a SDS session on an MCData group identity and the <mcdata-allow- short-data-service> element of a <list-service> element is not present in the MCData group document or is present with the value "false" as specified in 3GPP TS 24.481 [11], the MCData client and controlling MCData function shall determine that the MCData user is not allowed to initiate a SDS session on this group identity and shall not continue with the rest of the steps;

11) if the MCData user wishes to initiate an IP Connectivity session with one-to-one MCData communications and the <allow-transmit-data> element of an <actions> element is not present in the MCData user profile document or is present with the value "false" as specified in 3GPP TS 24.484 [12], the MCData client and controlling MCData function shall determine that the MCData user is not allowed to initiate an IP Connectivity session and shall not continue with the rest of the steps; and

12) the MCData functional entity shall determine that the MCData user is allowed to initiate MCData communications.

11.2 Auto-receive for File Distribution

If the controlling MCData function receives a one-to-one file distribution using HTTP or a group standalone file distribution using HTTP without the mandatory download indication the controlling MCData function:

1) if the file distribution request contained metadata, shall retrieve the filesize contained in the fileselector of the Metadata IE in the FD request;

2) if the file distribution request did not contain metadata, shall determine the size of the file referenced by the file URL contained in FD request;

3) for one-to-one file distribution using HTTP, shall determine if the filesize is less than or equal to the value contained in the <max-data-size-auto-recv-bytes> element of the MCData service configuration document as specified in 3GPP TS 24.484 [12];

4) for group standalone file distribution using HTTP, shall determine if the filesize is less than or equal to the value contained the <mcdata-on-network-max-data-size-auto-recv> element of the MCData group document associated with the MCData group identity in the request, as specified in 3GPP TS 24.481 [11]

5) ifcondition 3) or 4) is true, shall determine that the mandatory download indication needs to be included in the file distribution request sent to the terminating MCData client;

11.3 Accessing list of deferred data group communications

11.3.1 General

Accessing list of deferred data group communication allows a MCData user to request for the list of files that have been deferred for future download. The procedures are applicable for FD using HTTP.

11.3.2 MCData client procedures

11.3.2.1 Sending a request to access a list of deferred group communications

Upon receiving a request from the MCData user to access the list of deferred data group communications, the MCData client:

1) shall build the SIP MESSAGE request as specified in subclause 6.2.4.1;

2) shall generate DEFERRED DATA REQUEST message as specified in subclause 15.1.11.1;

3) shall include in the SIP request, the DEFERRED DATA GROUP COMM message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

4) shall send the SIP MESSAGE request towards the participating MCData function according to rules and procedures of 3GPP TS 24.229 [5].

11.3.2.2 Receiving a list of deferred group communications

Upon receipt of a "SIP MESSAGE response for the list of deferred group communications request", the MCData client:

1) shall generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

2) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5];

3) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body:

   a) if the application/vnd.3gpp.mcdata-signalling MIME body contains DEFERRED DATA RESPONSE message as specified in subclause 15.1.12:

      i) for each payload, if payload type is set to "FILEURL", shall store the payload data; and

4) shall present to MCData user, the list of file URLs which were deferred.

11.3.3 Participating MCData function procedures

11.3.3.1 Receiving a request to access a list of deferred group communications

Upon receipt of a "SIP MESSAGE request for the list of deferred group communications", the participating MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

2) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

3) shall follow the procedure described in subclause 11.3.3.2 to send response.

11.3.3.2 Sending a list of deferred group communications

To send the list of deferred group communications, the participating MCData function:

1) shall build the SIP MESSAGE request as specified in subclause 6.3.2.1;

2) shall generate DEFERRED DATA RESPONSE message as specified in subclause 15.1.12.1;

3) shall include in the SIP request, the DEFERRED DATA RESPONSE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

4) shall send the SIP MESSAGE request towards the participating MCData function according to rules and procedures of 3GPP TS 24.229 [5].

When generating a DEFERRED DATA RESPONSE message as specified in subclause 15.1.12, the MCData client:

1) shall set the number of payloads IE to the number of FD using HTTP communication which are deferred as per the stored file list:

   a) for each deferred file from the list, shall copy the payload IE value from the stored list to the payload IE value of the outgoing message being generated;

12 Dispositions and Notifications

12.1 General

The procedures in clause 12 describe:

- the on-network procedures for generating out-of-band dispositions for on-network SDS and on-network FD;

- the on-network procedures for generating network notifications for file distribution; and
- the off-network procedures for generating SDS dispositions.

The MCData client can send a disposition notification as a direct result of receiving an MCData message (e.g. delivery notification) or can send a disposition notification at a later time (e.g. read notification). In certain circumstances the delivery and read notification can be delivered in one notification message.

In-band dispositions are sent in the media plane as specified in 3GPP TS 24.582 [15].

12.2 On-network disposition notifications

12.2.1 MCData client procedures

12.2.1.1 MCData client sends a disposition notification message

The MCData client shall follow the procedures in this subclause to:

- indicate to an MCData client that an SDS message was delivered, read or delivered and read when the originating client requested a delivery, read or delivery and read report;
- indicate to the participating MCData function serving the MCData user that an SDS message was undelivered. The participating MCData function can store the message for later re-delivery;
- indicate to an MCData client that a request for FD was accepted, deferred or rejected; or
- indicate to an MCData client that a file download has been completed;

Before sending a disposition notification the MCData client needs to determine:

- the group identity related to an SDS or FD message request received as part of a group communication. The MCData client determines the group identity from the contents of the <mcdata-calling-group-id> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SDS or FD message request; and
- the MCData user targeted for the disposition notification. The MCData client determines the targetted MCData user from the contents of the <mcdata-calling-user-id> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SDS or FD message request.

The MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] with the clarifications given below.

The MCData client:

1) shall build the SIP MESSAGE request as specified in subclause 6.2.4.1;
2) shall follow the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message when processing the remaining steps in this subclause;
3) shall insert in the SIP MESSAGE request an application/resource-lists+xml MIME body containing the MCData ID of the targeted MCData user, according to rules and procedures of IETF RFC 5366 [18];
4) void;
5) if sending a disposition notification in response to an MCData group data request, shall include an <mcdata-calling-group-id> element set to the MCData group identity in the application/vnd.3gpp.mcdata-info+xml MIME body;
6) if requiring to send an SDS notification, shall generate an SDS NOTIFICATION message and include it in the SIP MESSAGE request as specified in subclause 6.2.3.1;
7) if requiring to send an FD notification, shall generate an FD NOTIFICATION message and include it in the SIP MESSAGE request as specified in subclause 6.2.3.2; and

8) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

12.2.1.2 MCData client receives a disposition notification message

Upon receipt of a:

"SIP MESSAGE request for SDS disposition notification for terminating MCData client"; or

"SIP MESSAGE request for FD disposition notification for terminating MCData client";

the MCData client:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body; and

2) shall deliver the notification to the user or application.

12.2.2 Participating MCData function procedures

12.2.2.1 Participating MCData function receives disposition notification from a MCData user

Upon receipt of a:

- "SIP MESSAGE request for SDS disposition notification for MCData server"; or

- "SIP MESSAGE request for FD disposition notification for MCData server";

the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE request;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) void;

5) if the SIP MESSAGE is a "SIP MESSAGE request for SDS disposition notification for MCData server" containing an SDS disposition notification type set to a value of "UNDELIVERED", shall temporarily store the message for re-delivery, shall start timer TD1 (SDS re-delivery timer) with the timer value as specified in subclause F.2.1, and shall not continue with the remaining steps;

NOTE: The participating MCData function attempts re-delivery of the SDS message after timer TD1 (SDS re-delivery timer) expiry.

6) if the SIP MESSAGE is a "SIP MESSAGE request for SDS disposition notification for MCData server " containing an SDS disposition notification type set to a value of "DELIVERED", "READ" or "DELIVERED AND READ" and the message was temporarily stored for re-delivery, shall delete the message from temporary store and shall stop TD1 (SDS re-delivery timer);

7) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

8) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCData function;

NOTE: How the participating MCData function determines the controlling MCData function to forward notification message is out of scope of the present document.

9) shall copy all MIME bodies included in the incoming SIP MESSAGE request to the outgoing SIP MESSAGE request;

10) if not already included as part of step 8) above, shall include an application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request, containing an <mcdata-calling-user-id> element set to the MCData ID of the originating user;

11) if the SIP MESSAGE is a "SIP MESSAGE request for SDS disposition notification for MCData server ", shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

12) if the SIP MESSAGE is a "SIP MESSAGE request for FD disposition notification for MCData server ", shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

13) if the SIP MESSAGE is a "SIP MESSAGE request for FD disposition notification for MCData server", and the FD disposition notification type IE is set as "FILE DOWNLOAD REQUEST ACCEPTED" or "FILE DOWNLOAD REQUEST REJECTED"as specified in subclause 15.2.6, shall remove the file from the stored file list;

14) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

15) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 202 (Accepted) response in response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP 202 (Accepted) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 202 (Accepted) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5]; and

2) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP MESSAGE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

12.2.2.2 Participating MCData function receives disposition notification from a Controlling MCData function

Upon receipt of a:

- "SIP MESSAGE request for SDS disposition notification for terminating MCData client"; or

- "SIP MESSAGE request for FD disposition notification for terminating MCData client";

the participating MCData function:

1) if unable to process the request due to a lack of resources or if a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response , optionally containing a Retry-After header field as specified in IETF RFC 3261 [4] . In this case, the participati ng MCData function shall skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request to retrieve the binding between the MCData ID and the public user identity;

3) if the binding between the MCData ID and the public user identity does not exist, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response and shall skip the rest of the steps;

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.1;

5) if sending an SDS disposition notification, shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

5) if sending an FD disposition notification, shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 2xx, 4xx, 5xx or 6xx response to the outgoing SIP MESSAGE request, the participating MCData function shall forward the SIP response to the controlling MCData function.

12.2.3 Controlling MCData function procedures

Upon receipt of a:

- "SIP MESSAGE request for SDS disposition notification for MCData server"; or

- "SIP MESSAGE request for FD disposition notification for MCData server";

the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4]. Otherwise, continue with the rest of the steps;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" or "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

3) if the incoming SIP MESSAGE request does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

4) shall attempt to correlate the disposition notification to the original SDS or FD request using the values contained in the Conversation ID and Message ID of the SDS NOTIFICATION message or FD NOTIFICATION message contained in the application/vnd.3gpp.mcdata-signalling MIME body of the SIP MESSAGE;

5) if unable to correlate the disposition notification as determined by step 4), shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "216 unable to correlate the disposition notification" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

6) if:

   a) a "SIP MESSAGE request for FD disposition notification for MCData server" has been received;

b) the FD disposition notification type IE in the FD NOTIFICATION message is set to "FILE DOWNLOAD REQUEST REJECTED"; and

c) the SIP MESSAGE does not contain an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-calling-group-id> element, or the SIP MESSAGE contains an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-calling-group-id> element and all other FD disposition notifications have been received from the invited group members and were all set to "FILE DOWNLOAD REQUEST REJECTED";

then:

a) shall delete the file stored in the media storage function that is associated with the Conversation ID and Message ID that was included in the FD NOTIFICATION message if no other file availability timers are running for a file;and

b) shall stop the running timer TDC2 (file availability timer), which is associated to the Conversation ID, Message ID, Application ID (if associated), and Extended application ID (if associated) that is included in the FD NOTIFICATION message;

7) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

8) if sending an SDS disposition notification:

a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8]] in the outgoing SIP MESSAGE request;

9) if sending an FD disposition notification:

a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

10) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

NOTE 1: How the controlling MCData function finds the address of the terminating MCData participating function is out of the scope of the current release.

11) if sending an SDS disposition notification, shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

12) if sending an FD disposition notification, shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

13) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request;

14) shall copy the MCData ID of the MCData user listed in the MIME resources body of the incoming SIP MESSAGE request, into the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

15) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-calling-group-id> element:

a) shall retrieve the group document for the MCData group id contained in the <mcdata-calling-group-id> element from the group management server, if not already cached, and identify the group members;

b) shall verify that the MCData ID contained in the <mcdata-calling-user-id> element matches to a group member. If there is no match, the controlling MCData function shall reject the SIP request with a SIP 403 (Forbidden) response including warning text set to "116 user is not part of the MCData group" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

c) if MCData disposition notifications need to be aggregated and an aggregated disposition notification has not yet been sent:

i) if timer TDC1 (disposition aggregation timer) is not running, shall start timer TDC1 (disposition aggregation timer) with the timer value as specified in subclause F.2.2;

ii) shall copy the application/vnd.3gpp.mcdata-signalling MIME body in the received SIP MESSAGE request to the outgoing SIP MESSAGE request;

NOTE 2: If the aggregated MCData disposition notifications do not fit into one SIP MESSAGE request, then the controlling MCData function needs to generate a new SIP MESSAGE request for the remaining disposition notifications.

iii) on expiry of timer TDC1 (disposition aggregation timer) shall continue with step 16; and

iv) if all MCData disposition notifications have been received from all group members shall continue with step 16; and

d) if MCData disposition notifications do not need to be aggregated, shall copy the application/vnd.3gpp.mcdata-signalling MIME body in the received SIP MESSAGE request to the outgoing SIP MESSAGE request and shall continue with step 16;

16) if the incoming SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body without an <mcdata-calling-group-id> element shall copy the application/vnd.3gpp.mcdata-signalling MIME body in the received SIP MESSAGE request to the outgoing SIP MESSAGE request;

17) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [5];

18) shall generate a SIP 202 (Accepted) response in response to the

- "SIP MESSAGE request for SDS disposition notification for MCData server"; or
- "SIP MESSAGE request for FD disposition notification for MCData server"; and

19) shall send the SIP 202 (Accepted) response towards the originating participating MCData function according to 3GPP TS 24.229 [5].

12.3 Off-network dispositions

12.3.1 General

12.3.2 Sending off-network SDS delivery notification

To send an off-network SDS delivery notification, the MCData client:

1) shall store "DELIVERED" as the disposition type;

2) shall generate a SDS OFF-NETWORK NOTIFICATION message as specified in subclause 15.1.8. In the SDS OFF-NETWORK NOTIFICATION message, the MCData client:

a) shall set the Sender MCData user ID IE to its own MCData user ID as specified in subclause 15.2.15;

b) shall set the Conversation ID IE as the stored conversation ID as specified in subclause 15.2.9;

c) shall set the Message ID IE as the stored SDS message ID as specified in subclause 15.2.10;

d) shall set the Date and time IE as the stored SDS notification time as specified in subclause 15.2.8;

e) shall set the SDS disposition notification type IE to the stored disposition type as specified in subclause 15.2.5; and

f) may set:

i) the Application ID IE to the stored SDS application ID as specified in subclause 15.2.7; or

ii) the Extended application ID IE to the stored extended SDS application ID as specified in subclause 15.2.24;

3) shall send the SDS OFF-NETWORK NOTIFICATION message to the stored notification target MCData user ID as specified in subclause 9.3.1.1;

4) shall initialise the counter CFS2 (SDS notification retransmission) with the value set to 1; and

5) shall start timer TFS2 (SDS notification retransmission).

12.3.3 Sending off-network SDS read notification

Upon receiving a display indication for the payload to the user or processing of the payload by the target application, the MCData client:

1) shall store "READ" as the disposition type;

2) shall store the current UTC time as the stored SDS notification time;

3) shall generate SDS OFF-NETWORK NOTIFICATION message as specified in subclause 15.1.8. In the SDS OFF-NETWORK NOTIFICATION message, the MCData client:

a) shall set the Sender MCData user ID IE to its own MCData user ID as specified in subclause 15.2.15;

b) shall set the Conversation ID IE as the stored conversation ID as specified in subclause 15.2.9;

c) shall set the Message ID IE as the stored SDS message ID as specified in subclause 15.2.10;

d) shall set the Data and time IE as the SDS notification time as specified in subclause 15.2.8;

e) shall set the SDS disposition notification type IE to the stored disposition type as specified in subclause 15.2.5; and

f) may set:

i) the Application ID IE set to the stored SDS application ID as specified in subclause 15.2.7; or

ii) the Extended application ID IE to the stored extended SDS application ID as specified in subclause 15.2.24;

4) shall send the SDS OFF-NETWORK NOTIFICATION message to the stored sender MCData user ID as specified in subclause 9.3.1.1;

5) shall initialise the counter CFS2 (SDS notification retransmission) with the value set to 1; and

6) shall start timer TFS2 (SDS notification retransmission).

12.3.4 Sending off-network SDS delivered and read notification

Upon receiving a display indication for the payload to the user or processing of the payload by the target application, the MCData client:

1) shall store "DELIVERED AND READ" as the disposition type and stop the timer TFS3 (display and read);

2) shall store the current UTC time as the stored SDS notification time;

3) shall generate SDS OFF-NETWORK NOTIFICATION message. In the SDS OFF-NETWORK NOTIFICATION message, the MCData client:

a) shall set the Sender MCData user ID IE to its own MCData user ID as specified in subclause 15.2.15;

b) shall set the Conversation ID IE as the stored conversation ID as specified in subclause 15.2.9;

c) shall set the Message ID IE as the stored SDS message ID as specified in subclause 15.2.10;

d) shall set the Date and time IE as the SDS notification time as specified in subclause 15.2.8;

e) shall set the SDS disposition notification type IE to the stored disposition type as specified in subclause 15.2.5; and

f) may set:

i) the Application ID IE to the stored SDS application ID as specified in subclause 15.2.7; or

ii) the Extended application ID IE to the stored extended SDS application ID as specified in subclause 15.2.24;

4) shall send the SDS OFF-NETWORK NOTIFICATION message to the stored sender MCData user ID as specified in subclause 9.3.1.1;

5) shall initialise the counter CFS2 (SDS notification retransmission) with the value set to 1; and

6) shall start timer TFS2 (SDS notification retransmission).

12.3.5 Off-network SDS notification retransmission

Upon expiry of timer TFS2 (SDS notification retransmission), the MCData client:

1) shall generate a SDS OFF-NETWORK NOTIFICATION message as specified in subclause 15.1.8. In the SDS OFF-NETWORK NOTIFICATION message, the MCData client:

a) shall set the Sender MCData user ID IE to its own MCData user ID as specified in subclause 15.2.15;

b) shall set the Conversation ID IE as the stored conversation ID as specified in subclause 15.2.9;

c) shall set the Message ID IE as the stored SDS message ID as specified in subclause 15.2.10;

d) shall set the Date and time IE as the stored SDS notification time as specified in subclause 15.2.8;

e) shall set the SDS disposition type IE to the stored disposition type as specified in subclause 15.2.5; and

f) may set:

i) the Application ID IE to the stored SDS application ID as specified in subclause 15.2.7; or

ii) the Extended application ID IE to the stored extended SDS application ID as specified in subclause 15.2.24;

2) shall send the SDS OFF-NETWORK NOTIFICATION message to the stored sender MCData user ID as specified in subclause 9.3.1.1;

3) shall increment the counter CFS2 (SDS notification retransmission) by 1; and

4) shall start timer TFS2 (SDS notification retransmission) if the associated counter CFS2 (SDS notification retransmission) has not reached its upper limit.

12.4 Network-triggered notifications for FD

12.4.1 General

12.4.1.1 File availability expiry

When the controlling MCData function receives a "SIP MESSAGE request for FD using HTTP for controlling MCData function" (referred to as FD request), it starts a timer TDC2 (file availability timer). The timer value is derived from the "file availability" information contained in metadata in the FD request (if included) or by local policy. The timer running for the file is uniquely associated to the Conversation ID and Message ID in the FD request.

The controlling MCData function tracks which MCData client(s) have downloaded the file referenced by the file URL received in an FD request which is associated to a Conversation ID and Message ID. On expiry of timer TDC2 (file availability timer), the controlling MCData function sends a FD NETWORK NOTIFICATION message with a notification type set to "FILE EXPIRED UNAVAILABLE TO DOWNLOAD". The MCData client is notified that the file associated with the Conversation ID and Message ID is no longer available to download.

12.4.2 Controlling MCData function procedures

12.4.2.1 Generation of a SIP MESSAGE request for notification

This subclause is referenced from other procedures and is not run standalone.

The controlling MCData function

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

4) shall follow the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message when processing the remaining steps in this subclause;

5) shall include in an application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request:

   - the <mcdata-request-uri> element set to the MCData ID of the MCData user; and

   - the <request-type> element set to a value of "notify";

6) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

7) shall include the public service identity of the controlling MCData function in the P-Asserted-Identity header field; and

8) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd".

12.4.2.2 Expiry of timer TDC2 (file availability timer)

When timer TDC2 (file availability timer) associated to a specific Conversation ID and Message ID expires, the controlling MCData function shall identify a target set of MCData client(s) as being:

- the MCData client that received a one-to-one file distribution using HTTP for the associated Conversation ID and Message ID, but has not yet downloaded the file; or

- each MCData client that received a group standalone file distribution using HTTP for the associated Conversation ID and Message ID, but have not yet downloaded the file;

On expiry of timer TDC2 (file availability timer), for each identified MCData client, the controlling MCData function:

NOTE: The file availability timer is associated to the Conversation ID and Message ID that was present in the initial FD request.

1) shall generate a SIP MESSAGE request as specified in subclause 12.4.2.1;

2) shall include an FD NETWORK NOTIFICATION message in an application/vnd.3gpp.mcdata-signalling MIME body of the SIP MESSAGE request with:

   a) the FD notification type IE as "FILE EXPIRED UNAVAILABLE TO DOWNLOAD" as specified in subclause 15.2.6;

   b) shall set the Date and time IE to the current time as specified in subclause 15.2.8;

   c) the Conversation ID IE set to a value identifying the conversation, as specified in subclause 15.2.9;

   d) the Message ID IE set to a value identifying the message as specified in subclause 15.2.10;

   e) if an Application ID was stored against the expired timer TDC2 (file availability timer), shall set the Application ID to the stored value as specified in subclause 15.2.7;

   f) if an Extended application ID was stored against the expired timer TDC2 (file availability timer), shall set the Extended application ID to the stored value as specified in subclause 15.2.7; and

3) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [5].

12.4.3 Participating MCData function procedures

The participating MCData function shall follow the procedures in subclause 10.2.4.3.2.

12.4.4 MCData client terminating procedures

On receipt of a SIP MESSAGE request containing an application/vnd.3gpp.mcdata-signalling MIME body with a FD NETWORK NOTIFICATION message, the MCData client:

1) may reject the SIP MESSAGE request if there are not enough resources to handle the SIP MESSAGE request;

2) if the SIP MESSAGE request is rejected in step 1), shall respond towards the participating MCData function with a SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this subclause;

3) shall generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

4) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5];

5) shall decode the contents of the FD NETWORK NOTIFICATION message contained in the application/vnd.3gpp.mcdata-signalling MIME body;

6) if the FD NETWORK NOTIFICATION message contains an Application ID or contains an Extended application ID, shall deliver the FD NETWORK NOTIFICATION message to the application; and

7) if the FD NETWORK NOTIFICATION message does not contain an Application ID and does not contain an Extended application ID, shall deliver the FD NETWORK NOTIFICATION message to the user.

13 Communication Release

13.1 General

Communication Release allows MCData user or MCData server to release MCData communications on-demand or based on policies. These procedures are applicable for SDS and FD and can be initiated by communication originator or MCData server.

13.2 On-network

13.2.1 General

13.2.1.1 Server generating message for release of communication over HTTP towards participating MCData function

This procedure is only referenced from other procedures. In order to generate a SIP MESSAGE towards the participating MCData function, the MCData server:

1) shall generate SIP MESSAGE accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];
2) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;
3) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";
4) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the participating MCData function associated to the originating MCData ID user; and
5) shall include an application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, following the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message:
    a) fill <mcdata-request-uri> element with the MCData ID of the target user.
6) shall include FD HTTP TERMINATION in application/vnd.3gpp.mcdata-signalling.

While generating an FD HTTP TERMINATION message as specified in subclause 15.1.3.1, the MCData server:

1) shall set the Conversation ID IE to a value identifying the conversation, as specified in subclause 15.2.9;
2) shall set the Message ID IE to a value identifying the message as specified in subclause 15.2.10;
3) may set:
    i) the Application ID IE to the stored value if applicable; or
    ii) the Extended application ID IE to the stored value if applicable; and
4) shall include a Payload IE with:
    a) the Payload content type set to "FILEURL" as specified in subclause 15.2.13; and
    b) Shall set the URL of the file same as of FD transmission.

13.2.1.2 Authorised user generating FD HTTP TERMINATION MESSAGE towards participating MCData function

This clause is referred from other clause only. In order to generate a SIP MESSAGE towards participating MCData function:

1) Shall generate SIP MESSAGE accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with parameters "require" and "explicit" according to IETF RFC 3841 [8] in the outgoing SIP MESSAGE request;

3) shall include a P-preferred-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

4) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the participating MCData function associated to the MCData ID user; and

5) shall include an application/vnd.3gpp.mcdata-info+xml MIME body in the SIP MESSAGE request, following the rules specified in subclause 6.4 for the handling of MIME bodies in a SIP message:

   a) set <mcdata-request-uri> element to the MCData ID of the target user; and

   b) shall include FD HTTP TERMINATION application/vnd.3gpp.mcdata-signalling. While including FD HTTP TERMINATION message according to subclause E.1.

When generating an FD HTTP TERMINATION message as specified in subclause 15.1.11, the MCData client:

1) shall set the Conversation ID IE to a value identifying the conversation, as specified in subclause 15.2.9;

2) shall set the Message ID IE to a value identifying the message as specified in subclause 15.2.10;

3) may set:

   i) the Application ID IE ID to the stored value if applicable; or

   ii) the Extended Application ID IE to the stored value if applicable; and

4) shall include a Payload IE with:

   a) the Payload content type set to "FILEURL" as specified in subclause 15.2.13; and

   b) the URL of the file same as of FD transmission.

13.2.2 MCData originating user initiated communication release

13.2.2.1 General

The MCData client can release the communication to indicate MCData service that the user no longer wants to transmit.

13.2.2.2 Release of MCData communication over media plane

13.2.2.2.1 General

The procedures described in this subclause are applicable to MCData SDS and MCData FD using media plane where originating MCData user initiates the communication release.

13.2.2.2.2 MCData client procedures

13.2.2.2.2.1 MCData client originating procedures

When the MCData client wants to release a MCData communication established over the media plane, the MCData client:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5];

2) shall set the Request-URI to the MCData session identity to be released; and

3) shall send the SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request, the MCData client shall release all media plane resources corresponding to the MCData communication being released.

13.2.2.2.2.2 MCData client terminating procedures

Upon receiving a SIP BYE request, the MCData client:

1) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

2) shall release all media plane resources corresponding to the MCData communication being released.

NOTE: Partially received data can be stored and processed.

13.2.2.2.3 Participating MCData function procedures

13.2.2.2.3.1 Originating participating MCData function procedures

Upon receiving a SIP BYE request from the MCData client, the originating participating MCData function:

1) shall generate a SIP BYE request as specified in 3GPP TS 24.229 [5];

2) shall set the Request-URI to the MCData session identity mentioned in the received SIP BYE request;

3) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP BYE request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

4) shall send the SIP BYE request toward the controlling MCData function, according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the participating MCData function;

1) shall forward the SIP 200 (OK) response to the originating MCData client and release all media plane resources corresponding to the MCData communication with the originating MCData client; and

2) shall release all media plane resources corresponding to the MCData communication with the controlling MCData function.

13.2.2.2.3.2 Terminating participating MCData function procedures

Upon receiving a SIP BYE request from the controlling MCData function, the participating MCData function:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5];

2) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP BYE request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

3) shall send the SIP BYE request to the MCData client according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the participating MCData function:

1) shall send the SIP 200 (OK) response to the SIP BYE request received from the controlling MCData function according to 3GPP TS 24.229 [5] and release all media plane resources corresponding to the MCData communication with the controlling MCData function; and

2) shall release all media plane resources corresponding to the MCData communication with the terminating MCData client.

13.2.2.2.4 Controlling MCData function procedures

13.2.2.2.4.1 Communication release policy for group MCData communication

The controlling MCData function shall release the group MCData communication, if:

1) the controlling MCData function receives an indication from the media plane that the transmission time limit has reached;

2) the controlling MCData function receives an indication from the media plane that the transmission data limit per request has reached;

3) there are only one or no participants in the MCData communication;

4) according to a local policy, the initiator of the group call leaves the MCData communication; or

5) the minimum number of affiliated MCData group members is not present;

13.2.2.2.4.2 Communication release policy for one-to-one MCData communication

The controlling MCData function shall release the one-to-one MCData communication if:

1) the controlling MCData function receives an indication from the media plane that the transmission time limit has reached;

2) the controlling MCData function receives an indication from the media plane that the transmission data limit per request has reached; or

3) there are only one or no participants in the MCData communication.

13.2.2.2.4.3 Receiving a SIP BYE request

Upon receiving a SIP BYE request the controlling MCData function:

1) shall release all media plane resources corresponding to the MCData communication with the originating participating MCData function;

2) shall generate a SIP 200 (OK) response and send the SIP response towards the originating MCData client according to 3GPP TS 24.229 [5];

3) shall check the communication release policy as specified in subclause 13.2.2.2.4.1 and subclause 13.2.2.2.4.2 whether the MCData communication needs to be released for each participant of the MCData communication; and

4) if release of the MCData communication is required, perform the procedures as specified in the subclause 13.2.2.2.4.4.

13.2.2.2.4.4 Sending a SIP BYE request

When a participant needs to be removed from the MCData communication, the controlling MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] for the MCData communication release;

2) shall generate a SIP BYE request according to 3GPP TS 24.229 [5]; and

3) shall send the SIP BYE request to the MCData client according to 3GPP TS 24.229 [5].

If group MCData communication needs to be released, the controlling MCData function shall send SIP BYE requests as described in this subclause to all the participants of the communication.

Upon receiving a SIP 200 (OK) response to a SIP BYE request, the controlling MCData function shall release all media plane resources corresponding to the MCData communication with the terminating participating MCData function.

13.2.2.3 Release of MCData communication over HTTP

13.2.2.3.1 General

The procedures described in this subclause are applicable to MCData FD using HTTP where originating MCData user initiates the communication release. This procedure applicable after file upload happened successfully and originating client sends SDS message towards server.

13.2.2.3.2 MCData client procedures

13.2.2.3.2.1 MCData client originating procedures

13.2.2.3.2.1.1 Initiating Release

When MCData client wants to release MCData communication either one-to-one FD or group-FD established over HTTP, the MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] with the clarifications given below.

The MCData client:

1) shall build the SIP MESSAGE request as specified in subclause 6.2.4.1;

2) if terminating one-to-one FD transmission, shall insert in the SIP MESSAGE request:

   a) an application/resource-lists+xml MIME body with the MCData ID of the recipient of FD transmission, according to rules and procedures of IETF RFC 4826 [9]; and

   b) an application/vnd.3gpp.mcdata-info+xml MIME body with a <request-type> element set to a value of "one-to-one-fd";

3) if terminating group FD transmission:

   a) shall insert in the SIP MESSAGE request an application/vnd.3gpp.mcdata-info+xml MIME body with:

      i) the <request-type> element set to a value of "group-fd";

      ii) the <mcdata-request-uri> element set to the MCData group identity for which FD transmission happening; and

      iii) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client;

4) shall generate a standalone FD message as specified in subclause 6.2.2.4; and

5) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards originating particiapting function.

13.2.2.3.2.1.2 Receiving Release Response Type from server

Upon receiving SIP MESSAGE from server containing application/vnd.3gpp.mcdata-signalling MIME body with HTTP TERMINATION MESSAGE and FD signalling payload message identity value set as FD HTTP TERMINATION as described in subclause 15.2.2 then

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

2) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5];

3) if FD HTTP TERMINATION message contains an Application ID or contains an Extended Application ID, shall deliver the FD HTTP TERMINATION message to the application; and

4) if Termination information type IE in HTTP TERMINATION MESSAGE is set to "TERMINATION RESPONSE" as specified in subclause 15.2.22 and If Release Response Type IE present then:

   a) set to "RELEASE SUCCESS" as described in subclause 15.2.23 the notify user that termination request is successful; or

   b) set to "RELEASE FAILED" as described in subclause 15.2.23 then notify user that termination request failed.

13.2.2.3.2.2 MCData client terminating procedures

On receipt of a SIP MESSAGE request containing an application/vnd.3gpp.mcdata-signalling MIME body with a FD NETWORK NOTIFICATION message, the MCData client shall follow the procedure as described in subclause 12.4.4.

13.2.2.3.3 Participating MCData function procedures

13.2.2.3.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for originating participating MCData function", the participating MCData function should follow the procedure as describe in subclause 10.2.4.3.1.

13.2.2.3.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for terminating participating MCData function", the participating MCData function should follow the procedure as describe in subclause 10.2.4.3.2.

13.2.2.3.4 Controlling MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for controlling MCData function", the controlling MCData function should follow the procedure as describe in subclause 10.2.4.4.2.

13.2.3 MCData server initiated communication release without prior indication

13.2.3.1 General

Based on local policies and conditions explained in subclause 13.2.2.2.4.1 and subclause 13.2.2.2.4.2, MCData server can release an ongoing MCData communication. Based on the configuration, MCData server can decide to release the communication without prior notification to MCData client.

13.2.3.2 Release of MCData communication over media plane

13.2.3.2.1 General

The procedures described in this subclause are applicable to MCData SDS and MCData FD using media plane where MCData server initiates communication release.

13.2.3.2.2 MCData client procedures

Upon receiving a SIP BYE request from the MCData server, the MCData client should follow the procedure described in subclause 13.2.2.2.2.2 with following clarification:

1) shall notify the MCData user with reason for release of communication if SIP BYE request contains reason header.

13.2.3.2.3 Participating MCData function procedures

Upon receiving SIP BYE request from controlling MCData function, the participating MCData function should follow the procedure described in subclause 13.2.2.2.3.2 with following clarification:

1) if reason header is present in the incoming SIP BYE request, shall copy the contents of the reason header field of the incoming SIP BYE request to the reason header field of the outgoing SIP BYE request.

13.2.3.2.4 Controlling MCData function procedures

Based on communication release policies and configuration, when controlling MCData function wants to release communication, the controlling MCData function should follow the procedure as described in subclause 13.2.2.2.4.4 with following clarification:

1) shall add reason header with reason-text value as appropriate (e.g. data volume limit, time limit expiry).

13.2.3.3 Release of MCData communication over HTTP

13.2.3.3.1 General

This procedure described in this subclause are applicable to MCData FD using HTTP where MCData server initiates communication release.

13.2.3.3.2 MCData client procedures

13.2.3.3.2.1 MCData client originating procedure

Upon receiving SIP MESSAGE from MCData server containing an application/vnd.3gpp.mcdata-signalling MIME body, the MCData client:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body;

2) if application/vnd.3gpp.mcdata-signalling MIME body contains a FD HTTP TERMINATION message as specified in subclause 15.1.11 and if the Termination Information Type IE is set to "TRANSMISSION STOPPED", then:

   a) shall generate a SIP 200 OK response according to 3GPP TS 24.229 [5]; and

   b) shall send the SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

3) shall notify MCData user about file transmission being stopped by identifying the corresponding file transmission local database based on conversation id, message id and FILE URL received in FD HTTP TERMINATION message, along with reason.

13.2.3.3.2.2 MCData client terminating procedure

On receipt of a SIP MESSAGE request containing an application/vnd.3gpp.mcdata-signalling MIME body with a FD NETWORK NOTIFICATION message, the MCData client shall follow the procedures as described in subclause 12.4.4.

13.2.3.3.3 Participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for terminating participating MCData function", the participating MCData function shall follow the procedure as described in subclause 10.2.4.3.2.

13.2.3.3.4 Controlling MCData function procedures

Base on communication release policies and configuration, when controlling MCData function wants to release communication, the controlling MCData function:

1) shall execute procedure as described in subclause 12.4.2.1 to delete the file and notify to participants with following clarification:

   a) shall set FD notification type IE as "FILE DELETED UNAVAILABLE TO DOWNLOAD" as specified in subclause 15.2.18; and

2) shall generate SIP MESSAGE as described in subclause 13.2.1.1 and

   a) shall add reason header with reason-text value as appropriate (e.g. data volume limit, time limit expiry);

   b) shall set Termination information type IE of FD HTTP TERMINATION MESSAGE to "TRANSMISSION STOPPED" as described in subclause 15.2.22; and

   c) shall send the SIP MESSAGE to MCData user who initiated the communication according to according to rules and procedures of 3GPP TS 24.229 [5].

13.2.4 MCData server initiated communication release with prior indication

13.2.4.1 General

Based on local policies and conditions as mentioned in subclause 13.2.2.2.4.1 and subclause 13.2.2.2.4.2, the MCData server can release an ongoing MCData communication.

If configured to, the MCData server can notify the originating MCData user about the intent to release communication and may request for more data about the communication it intends to release. The procedures described in this subclause are applicable to MCData SDS and MCData FD using media plane where the MCData server initiates the communication release.

13.2.4.2 MCData client procedures for communication over media plane

13.2.4.2.1 Receiving intent to release the communication

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the MCData client:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to “INTENT TO RELEASE”, then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

   b) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

   c) if an Data query type IE is present and set to “REMAINING AMOUNT OF DATA”, then:

      i) shall generate a DATA PAYLOAD message as described in subclause 15.1.4;

      ii) shall generate a SIP INFO request according to 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

      iii) shall include in the SIP INFO request, the DATA PAYLOAD message in an application/vnd.3gpp.mcdata-payload MIME body as specified in subclause E.2; and

         A) shall set a Content-Disposition header field to "Info-Package" value; and

      iv) shall send the SIP INFO request within the SIP dialog of the MCData communication, towards the participating MCData function according to 3GPP TS 24.229 [5]; and

3) shall notify MCData user and present the reason, if the reason header is present in incoming SIP INFO message.

When generating an DATA PAYLOAD message as specified in subclause 15.1.4, the MCData client:

1) shall set the Number of payloads IE to 1:

   a) shall set the Payload content type as "TEXT" as specified in subclause 15.2.13; and

   b) shall include the remaining amount of data in bytes to be sent in the Payload data.

Once the MCData user is notified about the MCData server's intent to release the communication, the MCData user may request for extension of communication as described in subclause 13.2.4.2.2.

13.2.4.2.2 Request for extension of communication

Upon receiving a request from MCData user for extension of the communication as a result of MCData server's intent to release the communication, the MCData client:

1) shall generate a SIP INFO request according to 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include a Info-Package with header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message as specified in subclause 15.1.10, in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

   a) shall set a Content-Disposition header field to "Info-Package" value; and

4) shall send the SIP INFO request within the SIP dialog of the MCData communication, towards the participating MCData function according to 3GPP TS 24.229 [5].

When generating an COMMUNICATION RELEASE message as specified in subclause 15.1.10, the MCData client:

1) shall set the Comm release information type to "EXTENSION REQUEST".

13.2.4.2.3 Receiving response to communication extension request

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the MCData client:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to “EXTENSION RESPONSE”, then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

   b) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

   c) shall notify user about extension response based on Extension Response Type IE.

13.2.4.3 Participating MCData function procedures for communication over media plane

13.2.4.3.1 Receiving SIP INFO request from the controlling MCData function

Upon receiving a SIP INFO request with the Info-Package header field set to g.3gpp.mcdata-com-release package, from controlling MCData function within the SIP dialog of the MCData communication, the participating MCData function:

1) shall generate a SIP INFO request according to 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall copy the contents of the Info-Package header field of the incoming SIP INFO request to the Info-Package header field of the outgoing SIP INFO request;

3) shall copy the MIME bodies present in the incoming SIP INFO request to the outgoing SIP INFO request; and

4) shall send the SIP INFO request to the MCData client within the SIP dialog of the MCData communication according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response from MCData client to the SIP INFO request, the participating MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

2) shall send a SIP 200 (OK) response to the SIP INFO request received from the controlling MCData function according to 3GPP TS 24.229 [5].

13.2.4.3.2 Receiving SIP INFO request from the MCData client

Upon receiving a SIP INFO request with the Info-Package header field set to g.3gpp.mcdata-com-release package, from MCData client within the SIP dialog of the MCData communication, the participating MCData function:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall copy the contents of the Info-Package header field of the incoming SIP INFO request to the Info-Package header field of the outgoing SIP INFO request;

3) shall copy the MIME bodies present in the incoming SIP INFO request to the outgoing SIP INFO request; and

4) shall send the SIP INFO request to the controlling MCData function, within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response from controlling MCData function to the SIP INFO request, the participating MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

2) shall send a SIP 200 (OK) response to the SIP INFO request received from the MCData client according to 3GPP TS 24.229 [5].

13.2.4.4 Controlling MCData function procedures for communication over media plane

13.2.4.4.1 Sending intent to release a communication

To send an intent to release a MCData communication, the controlling MCData function:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include the Info-Package header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1:

   a) shall set a Content-Disposition header field to "Info-Package" value;

4) may add reason header with reason-text value as appropriate (e.g. data volume limit, time limit expiry); and

5) shall send a SIP request towards participating MCData function within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

When generating a COMMUNICATION RELEASE message, the controlling MCData function:

1) shall generate a COMMUNICATION RELEASE message as defined in subclause 15.1.10. In the COMMUNICATION RELEASE message, the controlling MCData function:

   a) shall set Comm Release Information type IE to “INTENT TO RELEASE”; and

   b) if requesting for more information, shall include and set Data query type IE to the “REMAINING AMOUNT OF DATA”.

Upon receiving SIP 200 OK, the controlling MCData function:

1) shall start Timer TDC3 (request for extension).

If timer TDC3 (request for extension) expires before controlling MCData function receives a request for extension of communication from the MCData client, the controlling MCData function shall release MCData communication as described in subclause 13.2.2.2.4.4.

13.2.4.4.2 Receiving more information

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-payload MIME body associated with the Info-Package, the controlling MCData function:

1) shall decode the contents of the application/vnd.3gpp.mcdata-payload MIME body; and

2) shall identify the number of Payload IEs in the DATA PAYLOAD message from the Number of payloads IE in the DATA PAYLOAD message:

   a) For each Payload IE:

      i) shall store the contents of the Payload IE as remaining data information associated with ongoing MCData communication;

13.2.4.4.3 Receiving request for extension of communication

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the controlling MCData function:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if application/vnd.3gpp.mcdata-signalling MIME body contains COMMUNICATION RELEASE message with the comm release information type IE set to “EXTENSION REQUEST”, the controlling MCData function:

   a) shall stop the timer TDC3 (request for extension);

   b) shall generate SIP 200 (OK) response and send it towards participating MCData function according to 3GPP TS 24.229 [5]; and

   c) shall send response to communication extension request as described in subclause 13.2.4.4.4.

13.2.4.4.4 Sending response to communication extension request

To send a response to communication extension request from MCData client, the controlling MCData function:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include the Info-Package header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

   a) Shall set a Content-Disposition header field to "Info-Package" value; and

4) shall send a SIP request towards participating MCData function within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

When generating a COMMUNICATION RELEASE message, the controlling MCData function:

1) Shall generate a COMMUNICATION RELEASE message as defined in subclause 15.1.10. In the COMMUNICATION RELEASE message, the controlling MCData function:

   a) Shall set Comm Release Information type IE to “EXTENSION RESPONSE”; and

   b) shall assert the local policy along with already stored remaining data information associated with the MCData communication:

      i) If controlling MCData function decides to accept the request for extension, shall set extension request type information element to "ACCEPTED"; or

      ii) If controlling MCData function, decides to reject the request for extension, shall set extension request type information element to "REJECTED";

Upon receiving a SIP 200 (OK) response,

1) shall release the MCData communication as described in subclause 13.2.2.2.4.4, if controlling MCData function, decides to reject the request for extension.

13.2.4.5 Release of MCData communication over HTTP

13.2.4.5.1 General

Based on communication release policies and configuration, the MCData server can release an ongoing MCData communication.

If configured, the MCData server can notify the originating MCData user about the intent to release communication and may request for more data about the communication it intends to release. The procedures described in this subclause are applicable to MCData FD using HTTP where the MCData server initiates the communication release.

13.2.4.5.2 MCData client procedures

13.2.4.5.2.1 Receiving intent to release the communication

Upon receiving a SIP MESSAGE request containing an application/vnd.3gpp.mcdata-signalling MIME body; the MCData client:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a FD HTTP TERMINATION message as specified in subclause 15.1.11, with the Termination information type IE set to "INTENT TO RELEASE COMM OVER HTTP" then:

   a) shall identify file transmission request with Conversation ID, Message ID, and FILE URL in FD HTTP TERMINATION message, if identified any transmission:

      i) shall generate SIP 200 (OK) according to 3GPP TS 24.229 [5];

      ii) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5];

      iii) shall store the public service identity of the controlling MCData function from <mcdata-controller-psi> element of application/vnd.3gpp.mcdata-signalling MIME body; and

      iv) shall notify MCData user and present the reason; if the reason header is present in SIP MESSAGE.

Once the MCData user is notified about the MCData server's intent to release the communication, the MCData user may request for extension of communication as described in subclause 13.2.4.5.2.2

13.2.4.5.2.2 Request for extension of communication

Upon receiving a request from MCData user for extension of the communication as a result of MCData server's intent to release the communication, the MCData client:

1) shall generate SIP MESSAGE request according to 3GPP TS 24.229 [5];

2) shall generated a standalone FD message as specified in subclause 6.2.2.4 with following clarifications:

   a) shall set Termination information type IE to "EXTENSION REQUEST FOR COMM OVER HTTP";

3) shall include an application/vnd.3gpp.mcdata-info+xml MIME body:

   a) shall set <mcdata-controller-psi> element to the store public service identity of controlling MCData function; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards originating participating function.

13.2.4.5.2.3 Receiving response to communication extension request

Upon receiving a SIP MESSAGE request from MCData server containing application/vnd.3gpp.mcdata-signalling MIME body, the MCData client:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a FD HTTP TERMINATION message as specified in subclause 15.1.11, with the Termination information type IE set to "EXTENSION RESPONSE FOR COMM OVER HTTP", then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

   b) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and

3) shall notify user about extension response based on Extension response type IE.

13.2.4.5.3 Participating MCData function procedures

13.2.4.5.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for originating participating MCData function", the participating MCData function shall follow the procedure described in subclause 10.2.4.3.1.

13.2.4.5.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function", the participating MCData function shall follow the procedure described in subclause 10.2.4.3.2

13.2.4.5.4 Controlling MCData function procedures

13.2.4.5.4.1 Sending intent to release a communication

To send an intent to release a MCData communication, the controlling MCData function:

1) shall generate a SIP MESSAGE as described in subclause 13.2.1.1;

2) shall include <mcdata-controller-psi> element in application/vnd.3gpp.mcdata-info+xml MIME body with public service identity of controlling function;

3) shall set Termination information type IE in FD HTTP TERMINATION of application/vnd.3gpp.mcdata-signalling MIME body to "INTENT TO RELEASE COMM OVER HTTP";

4) may add reason header with reason-text value as appropriate (e.g. data volume limit, time limit expiry); and

5) shall send a SIP request towards participating MCData function according to 3GPP TS 24.229 [5].

Upon receiving SIP 200 OK, the controlling MCData function:

1) shall start Timer TDC3 (request for extension).

If timer TDC3 (request for extension) expires before controlling MCData function receives a request for extension of communication from the MCData client, the controlling MCData function shall release MCData communication as described in subclause 13.2.3.3.4.

13.2.4.5.4.2 Receiving request for extension of communication

Upon receiving a SIP MESSAGE request, the controlling MCData function:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if application/vnd.3gpp.mcdata-signalling MIME body contains FD HTTP TERMINATION message with the Termination information type IE set to "EXTENSION REQUEST FOR COMM OVER HTTP", the controlling MCData function:

   a) shall stop the timer TDC3 (request for extension) for file transmission identified by Conversation ID and Message ID and FILE URL;

   b) shall generate SIP 200 (OK) response and send it towards participating MCData function according to 3GPP TS 24.229 [5]; and

3) shall send response to communication extension request as described in subclause 13.2.4.5.4.3.

13.2.4.5.4.3 Sending response to communication extension request

To send a response to communication extension request from MCData client, the controlling MCData function:

1) shall generate a SIP MESSAGE as described in subclause 13.2.1.1;

2) shall set Termination information type IE in FD HTTP TERMINATION of application/vnd.3gpp.mcdata-signalling MIME body to "EXTENSION RESPONSE FOR COMM OVER HTTP";

3) shall assert the local policy associated with the MCData communication:

   a) If controlling MCData function decides to accept the request for extension, shall set Extension response type IE to "ACCEPTED"; or

   b) If controlling MCData function, decides to reject the request for extension, shall set Extension response type IE to "REJECTED"; and

4) shall send SIP MESSAGE towards participating MCData function according 3GPP TS 24.229 [5];

Upon receiving 200 OK response:

1) shall release the MCData communication as described in subclause 13.2.3.3.4; if controlling MCData function decides to reject the request for extension.

13.2.5 Authorized MCData user initiated communication release without prior indication

13.2.5.1 General

An authorized MCData user at any point of time during an ongoing MCData communication decides to release communication. An authorized MCData user should be part of the ongoing MCData communication. The procedure in this subclause describes the case where an authorized MCData user decides to release the communication without providing prior indication to originator MCData user.

13.2.5.2 Release of MCData communication over media plane

13.2.5.2.1 General

The procedures described in this subclause are applicable to MCData SDS and MCData FD established using media plane.

13.2.5.2.2 Authorized MCData client procedures

13.2.5.2.2.1 Sending communication release request

Upon receiving request from an authorized MCData user to release the communication without prior indication to originating MCData user, the MCData client:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include the Info-Package header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1:

   a) shall set a Content-Disposition header field to "Info-Package" value;

4) shall insert in the SIP INFO request an application/vnd.3gpp.mcdata-info+xml MIME body with

a) the <mcdata-client-id> element set to the MCData client ID of the authorized MCData client;

5) may add reason header with reason-text value as appropriate; and

6) shall send a SIP request towards participating MCData function within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

When generating a COMMUNICATION RELEASE message, the MCData client:

1) shall generate a COMMUNICATION RELEASE message as defined in subclause 15.1.10. In the COMMUNICATION RELEASE message, the MCData client:

a) shall set Comm Release Information type IE to "AUTH USER RELEASE REQ".

Upon receiving a SIP 200 (OK) response from participating MCData function to the SIP INFO request, the MCData client should inform the authorized MCData user about acceptance of communication release request by MCData server.

Upon receiving a SIP 403 (Forbidden) response from participating MCData function to the SIP INFO request, the MCData client should inform the authorized MCData user about rejection of communication release request by MCData server.

13.2.5.2.3 Participating MCData function procedures

13.2.5.2.3.1 Receiving SIP INFO request from the authorized MCData client

Upon receiving a SIP INFO request with the Info-Package header field set to g.3gpp.mcdata-com-release package, from MCData client within the SIP dialog of the MCData communication, the participating MCData function should follow the procedure described in subclause 13.2.4.3.2.

Upon receiving a SIP 403 (Forbidden) response from controlling MCData function to the SIP INFO request, the participating MCData function:

1) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5]; and

2) shall send a SIP 403 (Forbidden) response to the SIP INFO request received from the MCData client according to 3GPP TS 24.229 [5].

13.2.5.2.4 Controlling MCData function procedures

13.2.5.2.4.1 Receiving request to release the communication from authorized MCData user

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the controlling MCData function:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to "AUTH USER RELEASE REQ", then:

a) shall validate whether MCData user from which communication release request is received is authorized or not based on configuration;

3) if MCData user validation is not successful,

a) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5];

b) shall send SIP 403 (Forbidden) response towards participating MCData function according to 3GPP TS 24.229 [5];

c) shall skip further steps;

4) if MCData user validation is successful,

a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

b) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5];

5) shall follow the procedure as described in subclause 13.2.3.2.4 to terminate the ongoing communication;

13.2.5.3 Release of MCData communication over HTTP

13.2.5.3.1 General

The procedures described in this subclause are applicable to MCData FD over HTTP.

13.2.5.3.2 Authorized MCData client procedures

13.2.5.3.2.1 Sending communication release request

Upon receiving request from an authorized MCData user to release the communication without prior indication to originating MCData user, the MCData client

1) shall generate a SIP MESSAGE as specified in subclause 13.2.1.2, then:

   a) shall set the Termination information type IE if FD HTTP TERMINATION message to "AUTH USER TERMINATION REQUEST FOR COMM OVER HTTP" as specified in subclause 15.2.22;

2) shall add application/vnd.3gpp.mcdata-info+xml MIME body in SIP MESSAGE with:

   a) shall set <mcdata-controller-psi> element to the value received in incoming SIP MESSAGE; and

   b) shall add <mcdata-client-id> element set to the MCData client ID of the authorized MCData client;

3) may add reason header with reason-text value as appropriate; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards originating participating function.

Upon receiving a SIP 200 (OK) response from participating MCData function to the SIP MESSAGE request, the MCData client should inform the authorized MCData user about acceptance of communication release request by MCData server.

Upon receiving a SIP 403 (Forbidden) or SIP 404 (Not found) response from participating MCData function to the SIP MESSAGE request, the MCData client should inform the authorized MCData user about rejection of communication release request by MCData server.

13.2.5.3.2.2 Receiving Release Response Type from server

Upon receiving SIP MESSAGE from server containing application/vnd.3gpp.mcdata-signalling MIME body with HTTP TERMINATION MESSAGE and FD signalling payload message identity value set as FD HTTP TERMINATION as described in subclause 15.2.2, the authorized MCData client shall follow the procedure as described in subclause 13.2.2.3.2.1.2.

13.2.5.3.3 Participating MCData function procedures

13.2.5.3.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for originating participating MCData function", the participating MCData function shall follow the procedure as described in subclause 10.2.4.3.1.

13.2.5.3.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function", the participating MCData function shall follow the procedure as described in subclause 10.2.4.3.2.

13.2.5.3.4 Controlling MCData function procedures

13.2.5.3.4.1 Receiving request to release the communication from authorized MCData user

Upon receiving a SIP MESSAGE request and containing an application/vnd.3gpp.mcdata-signalling MIME body, the controlling MCData function:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;
2) if the application/vnd.3gpp.mcdata-signalling MIME body contains FD HTTP TERMINATION message as specified in subclause 15.1.11 then:
   a) if Termination information type IE set to "AUTH USER TERMINATION REQUEST FOR COMM OVER HTTP", then:
      i) shall validate whether MCData user identified in <mcdata-calling-userid> element of application/vnd.3gpp.mcdata-info+xml, is authorized or not based on configuration;
   b) if MCData user validation is not successful:
      i) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5];
      ii) shall send SIP 403 (Forbidden) response towards participating MCData function according to 3GPP TS 24.229 [5]; and
      iii) shall skip further steps;
   c) if MCData user validation is successful:
      i) if not able to identify file transmission using the Conversation ID, Message ID and file URL, shall send SIP 404 (Not Found) with reason with waring text set to "224 No transmission available" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps;
      ii) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and
      ii) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and
   d) shall follow the procedure as described in subclause 13.2.3.3.4 to terminate the ongoing communication.

The controlling MCData function should follow procedure as described in subclause 6.3.6.1 to generate response to the authorized user initiated request for release of MCData communication with following clarifications:

1) shall set Release response type IE to:
   a) "RELEASE SUCCESS" if communication release request is successful; or
   b) "RELEASE FAILED" if communication release request is not successful; and
2) shall send the SIP MESSAGE request towards the authorized MCData client as specified in 3GPP TS 24.229 [5].

13.2.6 Authorized MCData user initiated communication release with prior indication

13.2.6.1 General

An authorized MCData user at any point of time during an ongoing MCData communication decides to release communication. An authorized MCData user should be part of the ongoing MCData communication. The procedure in this subclause describes the case where an authorized MCData user decides to release the communication with providing prior indication to originator MCData user.

13.2.6.2 Release of MCData communication over media plane

13.2.6.2.1 General

The procedures described in this subclause are applicable to MCData SDS and MCData FD established using media plane.

13.2.6.2.2 Authorized MCData client procedures

13.2.6.2.2.1 Sending intent to release a communication

Upon receiving request from an authorized MCData user to release the communication without prior indication to originating MCData user, the MCData client:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include the Info-Package header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1:

   a) shall set a Content-Disposition header field to "Info-Package" value;

4) shall insert in the SIP INFO request an application/vnd.3gpp.mcdata-info+xml MIME body with:

   a) the <mcdata-client-id> element set to the MCData client ID of the authorized MCData client;

5) may add reason header with reason-text value as appropriate; and

6) shall send a SIP request towards participating MCData function within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

When generating a COMMUNICATION RELEASE message, the MCData client:

1) shall generate a COMMUNICATION RELEASE message as defined in subclause 15.1.10. In the COMMUNICATION RELEASE message, the MCData client:

   a) shall set Comm Release Information type IE to "INTENT TO RELEASE"; and

   b) if requesting for more information, shall include and set Data query type IE to the "REMAINING AMOUNT OF DATA".

Upon receiving a SIP 200 (OK) response from participating MCData function to the SIP INFO request, the MCData client should inform the authorized MCData user about acceptance of communication release request by MCData server.

Upon receiving a SIP 403 (Forbidden) response from participating MCData function to the SIP INFO request, the MCData client should inform the authorized MCData user about rejection of communication release request by MCData server.

13.2.6.2.2.2 Receiving more information

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-payload MIME body associated with the Info-Package, the authorized MCData client:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

2) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5];

3) shall decode the contents of the application/vnd.3gpp.mcdata-payload MIME body; and

4) shall identify the number of Payload IEs in the DATA PAYLOAD message:

a) for each Payload IE:

i) shall store the contents of the Payload IE as remaining data information associated with ongoing MCData communication.

13.2.6.2.2.3 Receiving request for extension of communication

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the authorized MCData client:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if application/vnd.3gpp.mcdata-signalling MIME body contains COMMUNICATION RELEASE message with the comm release information type IE set to "EXTENSION REQUEST", the MCData client:

a) shall generate SIP 200 (OK) response and send it towards participating MCData function according to 3GPP TS 24.229 [5]; and

b) shall notify authorized MCData user about extension request and also present more information received previously to authorized MCData user; and

3) based on authorized MCData user's response, shall send response to communication extension request as described in subclause 13.2.6.2.4.

13.2.6.2.2.4 Sending response to communication extension request

To send a response to communication extension request from originator MCData client, the authorized MCData client:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include the Info-Package header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1;

a) Shall set a Content-Disposition header field to "Info-Package" value; and

4) shall send a SIP request towards participating MCData function within the SIP dialog of the MCData communication, according to 3GPP TS 24.229 [5].

When generating a COMMUNICATION RELEASE message, the MCData client:

1) shall generate a COMMUNICATION RELEASE message as defined in subclause 15.1.10. In the COMMUNICATION RELEASE message, the MCData client:

a) shall set Comm Release Information type IE to "EXTENSION RESPONSE"; and

b) shall set extension request type information element as follows:

i) if authorized MCData user decides to accept the request for extension, shall set extension request type information element to "ACCEPTED"; or

ii) if authorized MCData user decides to reject the request for extension, shall set extension request type information element to "REJECTED".

13.2.6.2.3 Participating MCData function procedures

13.2.6.2.3.1 Receiving SIP INFO request from the authorized MCData client

Upon receiving a SIP INFO request with the Info-Package header field set to g.3gpp.mcdata-com-release package, from MCData client within the SIP dialog of the MCData communication, the participating MCData function should follow the procedure described in subclause 13.2.4.3.2.

Upon receiving a SIP 403 (Forbidden) response from controlling MCData function to the SIP INFO request, the participating MCData function:

1) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5]; and

2) shall send a SIP 403 (Forbidden) response to the SIP INFO request received from the MCData client according to 3GPP TS 24.229 [5].

13.2.6.2.3.2 Receiving SIP INFO request from the controlling MCData function

Upon receiving a SIP INFO request with the Info-Package header field set to g.3gpp.mcdata-com-release package, from controlling MCData function within the SIP dialog of the MCData communication, the participating MCData function shall follow the procedure described in subclause 13.2.4.3.1.

13.2.6.2.4 Controlling MCData function procedures

13.2.6.2.4.1 Receiving request to release the communication from authorized MCData user

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the controlling MCData function:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to AUTH USER RELEASE REQ, then:

   a) shall validate whether MCData user, from which communication release request is received, is authorized or not based on configuration;

3) if MCData user is not authorized to release the MCData communication,

   a) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5];

   b) shall send SIP 403 (Forbidden) response towards participating MCData function according to 3GPP TS 24.229 [5]; and

   c) shall skip further steps;

4) if MCData user is authorized to release the MCData communication,

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

   b) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5]; and

5) shall follow the procedure as described in subclause 13.2.4.4.1 with following clarifications;

   a) shall copy reason header from SIP INFO message received from participant MCData function.

The controlling MCData function should store the information related to initiator of MCData communication release process.

13.2.6.2.4.2 Receiving more information

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-payload MIME body associated with the Info-Package, the controlling MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];

2) shall send SIP 200 (OK) response towards participating MCData server according to 3GPP TS 24.229 [5].

If controlling MCDta function is not the initiator of the MCData communication release process, the controlling MCData function should send more information received in SIP INFO message to authorized MCData user who is the initiator of the MCData communication release process. The controlling MCData function:

1) shall generate a SIP INFO request according to 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall generate a DATA PAYLOAD message as described in subclause 15.1.4;

3) shall include in the SIP INFO request, the DATA PAYLOAD message in an application/vnd.3gpp.mcdata-payload MIME body as specified in subclause E.2;

   a) shall set a Content-Disposition header field to "Info-Package" value;

4) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the authorized MCData user; and

5) shall send the SIP INFO request within the SIP dialog of the MCData communication, towards the participating MCData function according to 3GPP TS 24.229 [5].

When generating an DATA PAYLOAD message as specified in subclause 15.1.4, the MCData client:

1) shall set the Number of payloads IE to the same number which it received in SIP INFO message from participating function:

   a) shall copy every payload IE from SIP INFO message received from participating function.

13.2.6.2.4.3 Receiving request for extension of communication

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the controlling MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

2) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5].

If controlling MCDta function is not the initiator of the MCData communication release process, the controlling MCData function should send request for extension of communication received in SIP INFO message to authorized MCData user who is the initiator of the MCData communication release process. The controlling MCData function:

1) shall generate a SIP INFO request according to 3GPP TS 24.229 [5] and IETF RFC 6086 [21];

2) shall include a Info-Package with header field set to g.3gpp.mcdata-com-release;

3) shall include in the SIP INFO request, a COMMUNICATION RELEASE message as specified in subclause 15.1.10, in an application/vnd.3gpp.mcdata-signalling MIME body as specified in subclause E.1; and

   a) shall set a Content-Disposition header field to "Info-Package" value;

4) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the authorized MCData user;

5) shall send the SIP INFO request within the SIP dialog of the MCData communication, towards the participating MCData function according to 3GPP TS 24.229 [5].

When generating an COMMUNICATION RELEASE message as specified in subclause 15.1.10, the MCData client:

1) shall set the Comm release information type to "EXTENSION REQUEST".

13.2.6.2.4.4 Receiving response to communication extension request

Upon receiving a SIP INFO request within the SIP dialog of a MCData communication, with the Info-Package header field set to g.3gpp.mcdata-com-release package and containing an application/vnd.3gpp.mcdata-signalling MIME body associated with the Info-Package, the controlling MCData function:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to "EXTENSION RESPONSE", then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

   b) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5].

If controlling MCDta function is not the initiator of the MCData communication release process, the controlling MCData function should send response to request for extension of communication received in SIP INFO message to originator MCData user. The controlling MCData function should follow procedure described in subclause 13.2.4.4.4 with following clarification:

1) while generating a COMMUNICATION RELEASE message;

   a) shall copy the extension request type information element from SIP INFO message received from authorized MCData client.

After sending response to originator MCData user, the controlling MCData function:

1) shall release the MCData communication as described in subclause 13.2.2.2.4.4, if authorized MCData user has rejected the request for extension.

13.2.6.3 Release of MCData communication over HTTP

13.2.6.3.1 General

The procedures described in this subclause are applicable to MCData FD over HTTP.

13.2.6.3.2 Authorized MCData client procedures

13.2.6.3.2.1 Sending intent to release a communication

Upon receiving request from an authorized MCData user to release the communication without prior indication to originating MCData user, the MCData client:

1) shall generate a SIP MESSAGE as specified in subclause 13.2.1.2, then:

   a) shall set the Termination information type IE of FD HTTP TERMINATION message to "INTENT TO RELEASE COMM OVER HTTP";

2) shall add application/vnd.3gpp.mcdata-info+xml MIME body in SIP MESSAGE with:

   a) shall set <mcdata-controller-psi> element to the value received in incoming SIP MESSAGE; and

   b) shall add <mcdata-client-id> element set to the MCData client ID of the authorized MCData client;

3) may add reason header with reason-text value as appropriate; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards originating participating function.

Upon receiving a SIP 200 (OK) response from participating MCData function to the SIP MESSAGE request, the MCData client should inform the authorized MCData user about acceptance of communication release request by MCData server.

Upon receiving a SIP 403 (Forbidden) or SIP 404 (Not found) response from participating MCData function to the SIP MESSAGE request, the MCData client should inform the authorized MCData user about rejection of communication release request by MCData server.

13.2.6.3.2.2 Receiving request for extension of communication

Upon receiving a SIP MESSAGE containing application/vnd.3gpp.mcdata-signalling MIME body then MCData client:

1) shall decode contents of application/vnd.3gpp.mcdata-signalling;

2) if application/vnd.3gpp.mcdata-signalling MIME body contains FD HTTP TERMINATION message with the Termination information type IE set to "EXTENSION REQUEST FOR COMM OVER HTTP", the authorized MCData client:

   a) shall generate SIP 200 (OK) response and send it towards participating MCData function according to 3GPP TS 24.229 [5]; and

   b) shall notify authorized MCData user about extension request to authorized MCData user; and

3) based on authorized MCData user's response, shall send response to communication extension request as described in subclause 13.2.6.3.2.3.

13.2.6.3.2.3 Sending response to communication extension request

To send a response to communication extension request from originator MCData client, the authorized MCData client:

1) shall generate a SIP MESSAGE as specified in subclause 13.2.1.2, then:

   a) shall set the Termination information type IE if FD HTTP TERMINATION message to "EXTENSION RESPONSE FOR COMM OVER HTTP";

   b) shall set Extension response type IE as follows:

      i) if authorized MCData user decides to accept the request for extension, shall set to "ACCEPTED"; or

      ii) if authorized MCData user decides to reject the request for extension, shall set to "REJECTED";

2) shall add application/vnd.3gpp.mcdata-info+xml MIME body in SIP MESSAGE with:

   a) shall set <mcdata-controller-psi> element to the value received in incoming SIP MESSAGE of FD transmission message; and

   b) shall add <mcdata-client-id> element set to the MCData client ID of the authorized MCData client;

3) may add reason header with reason-text value as appropriate; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards originating participating function.

13.2.6.3.2.4 Receiving Release Response from server

Upon receiving SIP MESSAGE from server containing application/vnd.3gpp.mcdata-signalling MIME body with HTTP TERMINATION MESSAGE and FD signalling payload message identity value set as FD HTTP TERMINATION as described in subclause 15.2.2, the authorized MCData client shall follow the procedure as described in subclause 13.2.2.3.2.1.2.

13.2.6.3.3 Participating MCData function procedures

13.2.6.3.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for FD using HTTP for originating participating MCData function", the originating participating MCData function shall follow the procedure as described in subclause 10.2.4.3.1.

13.2.6.3.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE network notification for FD using HTTP for terminating participating MCData function", the terminating participating MCData function shall follow the procedure as described in subclause 10.2.4.3.2.

13.2.6.3.4 Controlling MCData function procedures

13.2.6.3.4.1 Receiving request to release the communication from authorized MCData user

Upon receiving SIP MESSAGE from authorized MCData client containing an application/vnd.3gpp.mcdata-signalling MIME body; the controlling MCData function:

1) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body;

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a FD HTTP TERMINATION message as specified in subclause 15.1.11, with the Termination information type IE set to "INTENT TO RELEASE FOR COMM OVER HTTP", then:

   a) shall get authorized MCData user identity from <mcdata-calling-userid> element of application/vnd.3gpp.mcdata-info+xml MIME body and validate whether authorized MCData user, from which communication release request is received, is authorized or not based on configuration;

3) if MCData user is not authorized to release the MCData communication,

   a) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [5];

   b) shall send SIP 403 (Forbidden) response towards participating MCData function according to 3GPP TS 24.229 [5]; and

   c) shall skip further steps;

4) if MCData user is authorized to release the MCData communication:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

   b) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5]; and

5) shall follow the procedure as described in subclause 13.2.4.5.3.1 with following clarifications;

   a) shall copy reason header from SIP MESSAGE received from participant MCData function.

The controlling MCData function should store the information related to initiator of MCData communication release process.

13.2.6.3.4.2 Receiving request for extension of communication

Upon receiving SIP MESSAGE containing an application/vnd.3gpp.mcdata-signalling MIME body, the Controlling MCData function:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a COMMUNICATION RELEASE message as specified in subclause 15.1.10, with the Comm release information type IE set to "EXTENSION REQUEST FOR COMM OVER HTTP", then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

   b) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5].

If controlling MCData function is not the initiator of the MCData communication release process, the controlling MCData function should send request for extension of communication received in SIP MESSAGE to authorized MCData user who is the initiator of the MCData communication release process. The controlling MCData function:

1) shall generate SIP MESSAGE as described in subclause 13.2.1.1;

2) shall include application/vnd.3gpp.mcdata-info+xml MIME body, then:

   a) shall set <mcdata-request-uri> element to authorized user MCData id;

3) shall set Termination information type IE of FD HTTP TERMINATION message to "EXTENSION REQUEST FOR COMM OVER HTTP" as specified in subclause 15.2.22; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5] towards participating function.

13.2.6.3.4.3 Receiving response to communication extension request

Upon receiving a SIP MESSAGE containing an application/vnd.3gpp.mcdata-signalling MIME body, the controlling MCData function:

1) shall decode the contents of application/vnd.3gpp.mcdata-signalling MIME body; and

2) if the application/vnd.3gpp.mcdata-signalling MIME body contains a FD HTTP TERMINATION message as specified in subclause 15.1.11, with the Termination information type IE set to "EXTENSION RESPONSE FOR COMM OVER HTTP", then:

   a) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5]; and

   b) shall send SIP 200 (OK) response towards participating MCData function according to 3GPP TS 24.229 [5].

If controlling MCData function is not the initiator of the MCData communication release process, the controlling MCData function should send response to request for extension of communication received in SIP MESSAGE to originator MCData user. The controlling MCData function should follow procedure described in subclause 13.2.4.2.3.2 with following clarification:

1) while generating a FD HTTP TERMINATION message;

   a) shall copy the Extension response type information element from SIP MESSAGE received from authorized MCData client.

After sending response to originator MCData user, the controlling MCData function:

1) shall release the MCData communication as described in subclause 13.2.3.3.4, if authorized MCData user has rejected the request for extension.

The controlling MCData function should follow procedure as described in subclause 6.3.6.1 to generate response to the authorized user initiated request for release of MCData communication with following clarifications:

1) shall set Release response type IE to:

   a) "RELEASE SUCCESS" if communication release request is successful; or

   b) "RELEASE FAILED" if communication release request is not successful.

2) shall send the SIP MESSAGE request towards the authorized MCData client as specified in 3GPP TS 24.229 [5].

14. Enhanced Status (ES)

14.1 General

14.2 On-network ES

14.2.1 MCData client procedures

14.2.1.1 MCData client originating procedures

Upon receiving a request from the MCData user to send an enhanced status to an MCData group and the <mcdata-allow-enhanced-status> element under the <list-service> element as defined in 3GPP TS 24.481 [11] is set to "true", the MCData client:

1) shall use the "id" attribute of the MCData user selected operation value from <mcdata-enhanced-status-operational-values> element under <list-service> element as defined in 3GPP TS 24.481 [11], to generate a group standalone SDS message by following the procedure described in subclause 9.2.2.2.1.

14.2.1.2 MCData client terminating procedures

Upon receiving a "SIP MESSAGE request for standalone SDS for terminating MCData client", the MCData client:

1) shall follow the procedure defined in subclause 9.2.2.2.2;

2) shall match the received value with an "id" attribute of the operational values from the <mcdata-enhanced-status-operational-values> element of the MCData group document as defined in 3GPP TS 24.481 [11]; and

3) if a match is found, shall render the operational value as enhanced status to the MCData user. Otherwise shall discard the received message.

14.2.2 Participating MCData function procedures

14.2.2.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for originating participating MCData function", the participating MCData function should follow the procedure described in subclause 9.2.2.3.1.

14.2.2.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for terminating participating MCData function", the participating MCData function should follow the procedure described in subclause 9.2.2.3.2.

14.2.3 Controlling MCData function procedures

14.2.3.1 Originating controlling MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for controlling MCData function", the controlling MCData function should follow the procedure described in subclause 9.2.2.4.1.

14.2.3.2 Terminating controlling MCData function procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for controlling MCData function", the controlling MCData function should follow the procedure described in subclause 9.2.2.4.2.

14.3 Off-network ES

14.3.1 Sending enhanced status message

Upon receiving request from MCData user to share enhanced for selected group:

1) if the value of "/<x>/<x>/Common/MCData/AllowedEnhSvc" leaf node present in the group configuration as specified in 3GPP TS 24.483 [4] is set to "true" for the MCData group, the MCData client:

   a) shall use "/<x>/<x>/Common/MCData/EnhSvcOpValues/<x>/EnhSvcOpID" leaf node associated with user selected enhanced status operation value present in the group configuration as specified in 3GPP TS 24.483 [4] to generate a group standalone SDS message by following the procedure described in subclause 9.3.2.2.

14.3.2 Receiving enhanced status message

Upon receipt of a SDS OFF-NETWORK MESSAGE message, the MCData client:

1) shall follow the procedure defined in subclause 9.3.2.4;

2) shall attempt to match the received value with a "/<x>/<x>/Common/MCData/EnhSvcOpValues/<x>/EnhSvcOpID" leaf node present in the group configuration as specified in 3GPP TS 24.483 [4]; and

3) if a match is found, shall render the associated operational value from "/<x>/<x>/Common/MCData/EnhSvcOpValues/<x>/EnhSvcOpValue" leaf node as enhanced status to the MCData user.

15 Message Formats

15.1 MCData message functional definitions and contents

15.1.1 General

The following subclauses describe the MCData message functional definitions and contents. Each message consist of a series of information elements. The standard format of an MCData message and the encoding rules for each type of information element follow that defined for the MCPTT Off-Network Protocol (MONP) as documented in Annex I of 3GPP TS 24.379 [10]. The associated MIME types and related considerations are documented in Annex E of the present document.

For off-network transport, the MCData messages are transported in a MONP MCDATA CARRIER message defined in TS 24.379 [10].

15.1.2 SDS SIGNALLING PAYLOAD message

15.1.2.1 Message definition

This message is sent by the UE to other UEs when sending an SDS data payload. This message provides the signalling content related to the SDS data payload. For the contents of the message see Table 15.1.2.1-1.

Message type: SDS SIGNALLING PAYLOAD

Direction: UE to other UEs (can be via network)

Table 15.1.2.1-1: SDS SIGNALLING PAYLOAD message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS signalling payload message identity	Message type 15.2.2	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
21	InReplyTo message ID	InReplyTo message ID 15.2.11	O	TV	17
22	Application ID	Application ID 15.2.7	O	TV	2
8-	SDS disposition request type	SDS disposition request type 15.2.3	O	TV	1
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x
7E	User location	User location 15.2.25	O	TLV-E	4-x
51	Sender MCData user ID	MCData user ID 15.2.15	O	TLV-E	4-x

15.1.3 FD SIGNALLING PAYLOAD message

15.1.3.1 Message definition

This message is sent by the UE to other UEs when sending an FD data payload. This message provides the signalling content related to the FD data payload. For the contents of the message see Table 15.1.3.1-1.

Message type: FD SIGNALLING PAYLOAD

Direction: UE to other UEs (via the network)

Table 15.1.3.1-1: FD SIGNALLING PAYLOAD message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	FD signalling payload message identity	Message type 15.2.2	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
21	InReplyTo message ID	InReplyTo message ID 15.2.11	O	TV	17
22	Application ID	Application ID 15.2.7	O	TV	2
9-	FD disposition request type	FD disposition request type 15.2.4	O	TV	1
A-	Mandatory download	Mandatory download 15.2.16	O	TV	1
78	Payload	Payload 15.2.13	O	TLV-E	3-x
79	Metadata	Metadata 15.2.17	O	TLV-E	3-x
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x
51	Sender MCData user ID	MCData user ID 15.2.15	O	TLV-E	4-x

15.1.4 DATA PAYLOAD message

15.1.4.1 Message definition

This message is sent by the UE to other UEs when sending an SDS data payload or an FD data payload. This message provides the data to be delivered to the user or application. For the contents of the message see Table 15.1.4.1-1.

Message type: DATA PAYLOAD

Direction: UE to other UEs (can be via the network for SDS and always via the network for FD)

Table 15.1.4.1-1: DATA PAYLOAD message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Data payload message identity	Message type 15.2.2	M	V	1
	Number of payloads	Number of payloads 15.2.12	M	V	1
7A	Security parameters and Payload	MCData Protected Payload message 3GPP TS 33.180 [26]	O	TLV-E	32-x
78	Payload	Payload 15.2.13	O	TLV-E	3-x

NOTE 1: The Number of payloads IE dictates the number of Payload IEs that are included in the message by the sender. Multiple Payload IEs can be part of Security parameters and Payload IE if end-to-end security is required.

NOTE 2: If end-to-end security is required for a one-to-one communication, Security parameters and Payload IE is included. Otherwise, if end-to-end security is not required for a one-to-one communication, Payload IE is included. For group communication, Payload IE is included.

NOTE 3: Formatting of payloads as part of the Security parameters and Payload IE is specified in subclause 15.2.13.

15.1.5 SDS NOTIFICATION message

15.1.5.1 Message definition

This message is sent by the UE to another other UE to share SDS disposition information. For the contents of the message see Table 15.1.5.1-1.

Message type: SDS NOTIFICATION

Direction: UE to other UEs (can be via network)

Table 15.1.5.1-1: SDS NOTIFICATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS notification message identity	Message type 15.2.2	M	V	1
	SDS disposition notification type	SDS disposition notification type 15.2.5	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
22	Application ID	Application ID 15.2.7	O	TV	2
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x
51	Sender MCData user ID	MCData user ID 15.2.15	O	TLV-E	4-x

15.1.6 FD NOTIFICATION message

15.1.6.1 Message definition

This message is sent by the UE to another other UE to share FD disposition information. For the contents of the message see Table 15.1.6.1-1.

Message type: FD NOTIFICATION

Direction: UE to other UEs (via the network)

Table 15.1.6.1-1: FD NOTIFICATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	FD notification message identity	Message type 15.2.2	M	V	1
	FD disposition notification type	FD disposition notification type 15.2.6	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
22	Application ID	Application ID 15.2.7	O	TV	2
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x
51	Sender MCData user ID	MCData user ID 15.2.15	O	TLV-E	4-x

15.1.7 SDS OFF-NETWORK MESSAGE message

15.1.7.1 Message definition

This message is sent by the UE to other UEs to share application or user payload in a SDS message. For contents of the message see Table 15.1.7.1-1.

Message type: SDS OFF-NETWORK MESSAGE

Direction: UE to other UEs

Table 15.1.7.1-1: SDS OFF-NETWORK MESSAGE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS off-network message message identity	Message Type 15.2.2	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Number of payloads	Number of payloads 15.2.12	M	V	1
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
	Sender MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x
21	InReplyTo message ID	InReplyTo message ID 15.2.11	O	TV	17
22	Application ID	Application ID 15.2.7	O	TV	2
8-	SDS disposition request type	SDS disposition request type 15.2.3	O	TV	1
23	Security parameters	MCData Protected Payload message 3GPP TS 33.180 [26]	O	TV	32
7B	MCData group ID	MCData group ID 15.2.14	O	TLV-E	4-x
7C	Recipient MCData user ID	MCData user ID 15.2.15	O	TLV-E	4-x
78	Payload	Payload 15.2.13	O	TLV-E	4-x
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x
7E	User location	User location 15.2.25	O	TLV-E	4-x

15.1.8 SDS OFF-NETWORK NOTIFICATION message

15.1.8.1 Message definition

This message is sent by the UE to other UEs to share disposition status of a SDS message. For contents of the message see Table 15.1.8.1-1.

Message type: SDS OFF-NETWORK NOTIFICATION

Direction: UE to other UEs

Table 15.1.8.1-1: SDS OFF-NETWORK NOTIFICATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS off-network notification message identity	Message type 15.2.2	M	V	1
	SDS disposition notification type	SDS disposition notification type 15.2.5	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
	Sender MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x
22	Application ID	Application ID 15.2.7	O	TV	2
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x

15.1.9 FD NETWORK NOTIFICATION message

15.1.9.1 Message definition

This message is sent from the network to the UE to provide the UE a file availability indication. For the contents of the message see Table 15.1.9.1-1.

Message type: FD NETWORK NOTIFICATION

Direction: network to UE

Table 15.1.9.1-1: FD NETWORK NOTIFICATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	FD network notification message identity	Message type 15.2.2	M	V	1
	FD notification type	Notification type 15.2.18	M	V	1
	Date and time	Date and time 15.2.8	M	V	5
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
22	Application ID	Application ID 15.2.7	O	TV	2
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x

15.1.10 COMMUNICATION RELEASE message

15.1.10.1 Message definition

This message is sent by the MCData server to MCData UE to indicate about intension to release the MCData communication. This message is also sent by the MCData UE to MCData server to request extension for the MCData communication. The MCData server response back about the request using this message. For the contents of the message see Table 15.10.1-1.

Message type: COMMUNICATION RELEASE

Direction: Server to UE, UE to server

Table 15.1.10.1-1: COMMUNICATION RELEASE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Comm Release message identity	Message type 15.2.2	M	V	1
	Comm Release Information type	Comm Release Information type 15.2.20	M	V	1
B-	Data query type	Data query type 15.2.19	O	TV	1
C-	Extension response type	Extension response type 15.2.21	O	TV	1

15.1.11 DEFERRED DATA REQUEST message

15.1.11.1 Message definition

This message is sent by the MCData UE to MCData server to request the list of group communications which was deferred by the MCData user.

Message type: DEFERRED DATA REQUEST

Direction: UE to server

Table 15.1.11.1-1: DEFERRED DATA REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Deferred data request message identity	Message type 15.2.2	M	V	1

15.1.12 DEFERRED DATA RESPONSE message

15.1.12.1 Message definition

This message is sent by the MCData server to the MCData UE as response to the list of deferred group communications request from the MCData UE.

Message type: DEFERRED DATA RESPONSE

Direction: Server to UE

Table 15.1.12.1-1: DEFERRED DATA RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Deferred data response message identity	Message type 15.2.2	M	V	1
	Number of payloads	Number of payloads 15.2.12	M	V	1
7A	Security parameters and Payload	MCData Protected Payload message 3GPP TS 33.180 [26]	O	TLV-E	32-x
78	Payload	Payload 15.2.13	O	TLV-E	3-x

15.1.13 FD HTTP TERMINATION

15.1.13.1 Message definition

This message is sent by the UE to server or server to UE when trying to release FD communication over HTTP. This message provides the signalling content to identify the MESSAGE where FILE URL is shared. For the contents of the message see table 15.1.13.1-1.

Message type: FD HTTP TERMINATION

Direction: UE to server or server to UE

Table 15.1.13.1-1: FD HTTP TERMINATION content

IEI	Information Element	Type/Reference	Presence	Format	Length
	FD signalling payload message identity	Message type 15.2.2	M	V	1
	Conversation ID	Conversation ID 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
	Termination Information Type	Termination information type 15.2.22	M	V	1
22	Application ID	Application ID 15.2.7	O	TV	2
C-	Extension Response Type	Extension response type 15.2.21	O	TV	1
D-	Release Response Type	Release response type 15.2.23	O	TV	1
78	Payload	Payload 15.2.13	O	TLV-E	3-x
7D	Extended application ID	Extended application ID 15.2.24	O	TLV-E	3-x

15.1.14 GROUP EMERGENCY ALERT message

15.1.14.1 Message definition

This message is sent by the UE to other UEs to indicate an emergency situation. For contents of the message see table 15.1.14.1-1.

Message type: GROUP EMERGENCY ALERT

Direction: UE to other UEs

Table 15.1.14.1-1: GROUP EMERGENCY ALERT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert message identity	Message type 15.2.2	M	V	1
	MCData group ID	MCData group ID 15.2.14	M	LV-E	3-x
	Originating MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x
7F	Organization name	Organization name 15.2.26	O	TLV-E	4-x
7E	User location	User location 15.2.25	O	TLV-E	4-x

15.1.15 GROUP EMERGENCY ALERT ACK message

15.1.15.1 Message definition

This message is sent by the UE to other UEs to indicate receipt of emergency alert. For contents of the message see table 15.1.15.1-1.

Message type: GROUP EMERGENCY ALERT ACK

Direction: UE to other UEs

Table 15.1.15.1-1: GROUP EMERGENCY ALERT ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert ack message identity	Message type 15.2.2	M	V	1
	MCData group ID	MCData group ID 15.2.14	M	LV-E	3-x
	Originating MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x
	Sending MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x

15.1.16 GROUP EMERGENCY ALERT CANCEL message

15.1.16.1 Message definition

This message is sent by the UE to other UEs to indicate end of emergency situation. For contents of the message see table 15.1.16.1-1.

Message type: GROUP EMERGENCY ALERT CANCEL

Direction: UE to other UEs

Table 15.1.16.1-1: GROUP EMERGENCY ALERT CANCEL message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert cancel message identity	Message type 15.2.2	M	V	1
	MCData group ID	MCData group ID 15.2.14	M	LV-E	3-x
	Originating MCData user ID	MCData User ID 15.2.15	M	LV-E	3-x

15.1.17 GROUP EMERGENCY ALERT CANCEL ACK message

15.1.17.1 Message definition

This message is sent by the UE to other UEs to indicate receipt of emergency alert cancel. For contents of the message see table 15.1.17.1-1.

Message type: GROUP EMERGENCY ALERT CANCEL ACK

Direction: UE to other UEs

Table 15.1.17.1-1: GROUP EMERGENCY ALERT CANCEL ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert cancel ack message identity	Message type 15.2.2	M	V	1
	MCData group ID	MCData group ID 15.2.14	M	LV-E	3-x
	Originating MCData user ID	MCData User ID 15.2.15	M	LV-E	3-x
	Sending MCData user ID	MCData user ID 15.2.15	M	LV-E	3-x

15.2 General message format and information elements coding

15.2.1 General

The least significant bit of a field is represented by the lowest numbered bit of the highest numbered octet of the field. When the field extends over more than one octet, the order of bit values progressively decreases as the octet number increases.

Figure 15.2.1-1 shows an example of a field where the most significant bit of the field is marked MSB and the least significant bit of the field is marked LSB.

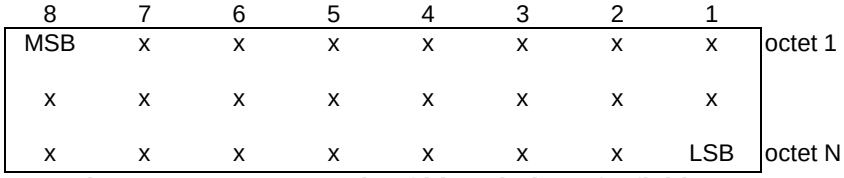

Figure 15.2.1-1: Example of bit ordering of a field

Within the protocols defined in the present document, the message consists of the following parts:

a) message type information element; and

b) other information elements, as required.

The organization of a message is illustrated in the example shown in Figure 15.2.1-2.

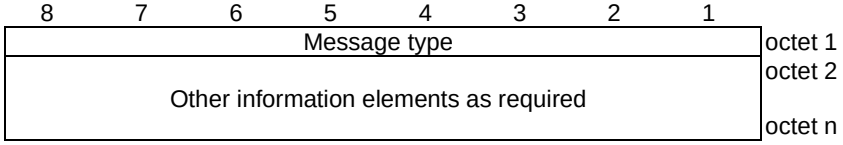

Figure 15.2.1-2: General message organization example

Unless specified otherwise in the message descriptions of subclause 15.1, a particular information element shall not be present more than once in a given message.

The sending entity shall set value of a spare bit to zero. The receiving entity shall ignore value of a spare bit

The sending entity shall not set a value of an information element to a reserved value. The receiving entity shall discard message containing an information element set to a reserved value.

15.2.2 Message type

The purpose of the Message type information element is to identify the type of the message.

The value part of the Message type information element is coded as shown in Table 15.2.2-1.

The Message type information element is a type 3 information element with a length of 1 octet.

Table 15.2.2-1: Message types

Bits 8	7	6	5	4	3	2	1	
x	x	0	0	0	0	0	1	SDS SIGNALLING PAYLOAD
x	x	0	0	0	0	1	0	FD SIGNALLING PAYLOAD
x	x	0	0	0	0	1	1	DATA PAYLOAD
x	x	0	0	0	1	0	1	SDS NOTIFICATION
x	x	0	0	0	1	1	0	FD NOTIFICATION
x	x	0	0	0	1	1	1	SDS OFF-NETWORK MESSAGE
x	x	0	0	1	0	0	0	SDS OFF-NETWORK NOTIFICATION
x	x	0	0	1	0	0	1	FD NETWORK NOTIFICATION
x	x	0	0	1	0	1	0	COMMUNICATION RELEASE
x	x	0	0	1	0	1	1	DEFERRED LIST ACCESS REQUEST
x	x	0	0	1	1	0	0	DEFERRED LIST ACCESS RESPONSE
x	x	0	0	1	1	0	1	FD HTTP TERMINATION
x	x	0	1	0	0	0	1	GROUP EMERGENCY ALERT
x	x	0	1	0	0	1	0	GROUP EMERGENCY ALERT ACK
x	x	0	1	0	0	1	1	GROUP EMERGENCY ALERT CANCEL
x	x	0	1	0	1	0	0	GROUP EMERGENCY ALERT CANCEL ACK
All other values are reserved.								

Bit 7 of the above defined messages is set as follows:

- '0' – if the message is not protected as defined in 3GPP TS 33.180 [26]; or
- '1' – if the message is protected as defined in 3GPP TS 33.180 [26].

Bit 8 of the above defined messages is set as follows:

- '0' – if the message is not authenticated as defined in 3GPP TS 33.180 [26]; or
- '1' – if the message is authenticated as defined in 3GPP TS 33.180 [26].

15.2.3 SDS disposition request type

The purpose of the SDS disposition request type information element is to identify the type of SDS disposition notification that the sender requires from the receiver.

The value part of the SDS disposition request type information element is coded as shown in Table 15.2.3-1.

The SDS disposition request type information element is a type 1 information element.

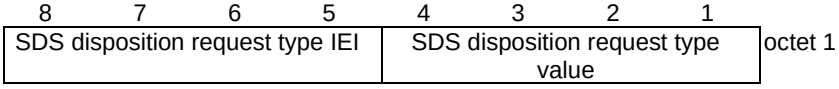

Figure 15.2.3-1: SDS disposition request type

Table 15.2.3-1: SDS disposition request type

SDS disposition request type value (octet 1) Bits 4	3	2	1	
0	0	0	1	DELIVERY
0	0	1	0	READ
0	0	1	1	DELIVERY AND READ
All other values are reserved.				

15.2.4 FD disposition request type

The purpose of the FD disposition request type information element is to identify the type of FD disposition notification that the sender requires from the receiver.

The value part of the FD disposition request type information element is coded as shown in Table 15.2.4-1.

The FD disposition request type information element is a type 1 information element.

8	7	6	5	4	3	2	1	
FD disposition request type IEI				FD disposition request type value				octet 1

Figure 15.2.4-1: FD disposition request type

Table 15.2.4-1: FD disposition request type

FD disposition request type value (octet 1)				
Bits				
4	3	2	1	
0	0	0	1	FILE DOWNLOAD COMPLETED UPDATE
All other values are reserved.				

15.2.5 SDS disposition notification type

The purpose of the SDS disposition notification type information element is to identify the type of SDS disposition notification sent from receiver to the sender.

The value part of the SDS disposition notification type information element is coded as shown in Table 15.2.5-1.

The SDS disposition notification type information element is a type 3 information element with a length of 1 octet.

Table 15.2.5-1: SDS disposition notification type

Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	UNDELIVERED
0	0	0	0	0	0	1	0	DELIVERED
0	0	0	0	0	0	1	1	READ
0	0	0	0	0	1	0	0	DELIVERED AND READ
All other values are reserved.								

15.2.6 FD disposition notification type

The purpose of the FD disposition notification type information element is to identify the type of FD disposition notification sent from receiver to the sender.

The value part of the FD disposition notification type information element is coded as shown in Table 15.2.6-1.

The FD disposition notification type information element is a type 3 information element with a length of 1 octet.

Table 15.2.6.1: FD disposition notification type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	FILE DOWNLOAD REQUEST ACCEPTED
0 0 0 0 0 0 1 0	FILE DOWNLOAD REQUEST REJECTED
0 0 0 0 0 0 1 1	FILE DOWNLOAD COMPLETED
0 0 0 0 0 1 0 0	FILE DOWNLOAD DEFERRED
All other values are reserved.	

15.2.7 Application ID

The purpose of the Application ID information element is to uniquely identify the application for which the payload is intended.

The Application ID information element is coded as shown in figure 15.2.7-1 and table 15.2.7-1

The Application ID information element is a type 3 information element with a length of 2 octets.

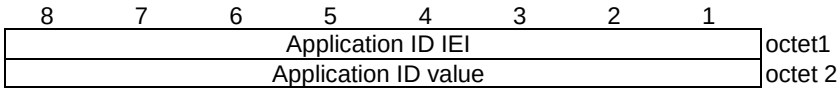

Figure 15.2.7-1: Application ID value

Table 15.2.7-1: Application ID value

Application ID value (octet 1) The Application ID contains a number that uniquely identifies the destination application.

15.2.8 Date and time

The Date and time information element is used to indicate the UTC time when a message or file was sent.

The Date and time information element is coded as shown in Figure 15.2.8-1 and Table 15.2.8-1.

The Date and time information element is a type 3 information element with a length of 5 octets.

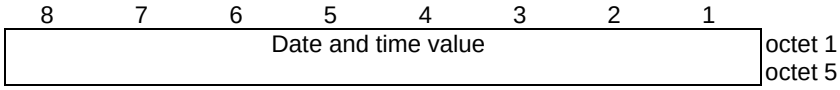

Figure 15.2.8-1: Date and time value

Table 15.2.8-1: Date and time value

Date and time value (octet 1 to 5) The Date and time value is an unsigned integer containing UTC time of the time when a message was sent, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).

15.2.9 Conversation ID

The Conversation ID information element uniquely identifies the conversation.

The Conversation ID information element is coded as shown in Figure 15.2.9-1 and Table 15.2.9-1.

The Conversation ID information element is a type 3 information element with a length of 16 octets.

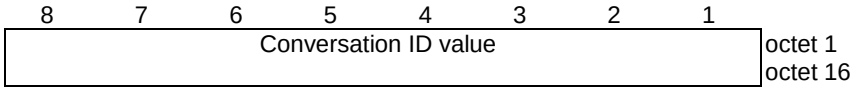

Figure 15.2.9-1: Conversation ID value

Table 15.2.9-1: Conversation ID value

Conversation identifier value (octet 1 to 16) The Conversation ID contains a number uniquely identifying the conversation. The value is a universally unique identifier as specified in IETF RFC 4122 [14].

15.2.10 Message ID

The Message ID information element uniquely identifies a message within a conversation.

The Message ID information element is coded as shown in Figure 15.2.10-1 and Table 15.2.10-1.

The Message ID information element is a type 3 information element with a length of 16 octets.

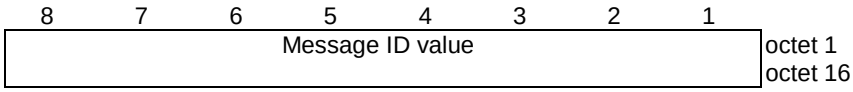

Figure 15.2.10-1: Message ID value

Table 15.2.10-1: Message ID value

Message ID value (octet 1 to 16) The Message ID contains a number uniquely identifying a message. The value is a universally unique identifier as specified in IETF RFC 4122 [14].

15.2.11 InReplyTo message ID

The InReplyTo message ID information element is used to associate a message within a conversation that is a reply to an existing message in a conversation.

The InReplyTo message ID information element is coded as shown in Figure 15.2.11-1 and Table 15.2.11-1.

The InReplyTo message ID information element is a type 3 information element with a length of 17 octets.

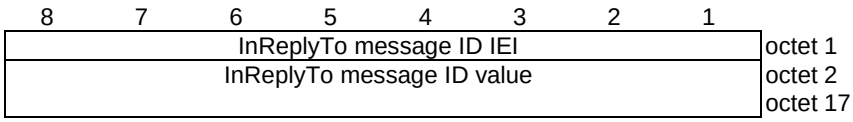

Figure 15.2.11-1: InReplyTo message ID value

Table 15.2.11-1: InReplyTo Message ID value

InReplyTo message ID value (octet 2 to 17) The InReplyTo message ID contains a number uniquely identifying a message. The value is a universally unique identifier as specified in IETF RFC 4122 [14].

15.2.12 Number of payloads

The Number of payloads information element identifies the number of payloads contained in the message.

The Number of payloads information element is coded as shown in Figure 15.2.12-1, Table 15.2.12-1

The Number of payloads information element is a type 3 information element with a length of 1 octet

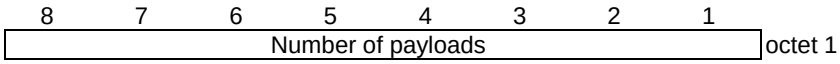

Figure 15.2.12-1: Number of payloads information element

Table 15.2.12-2: Number of payloads information element

Number of payloads value (octet 1) The Number of payloads contains a value from 1 to 255.

15.2.13 Payload

The Payload information element contains the payload intended for the recipient user or application;

The Payload information element is coded as shown in Figure 15.2.13-1, Table 15.2.13-1, Table 15.2.13-2 and Table 15.2.13-3.

The Payload information element is a type 6 information element.

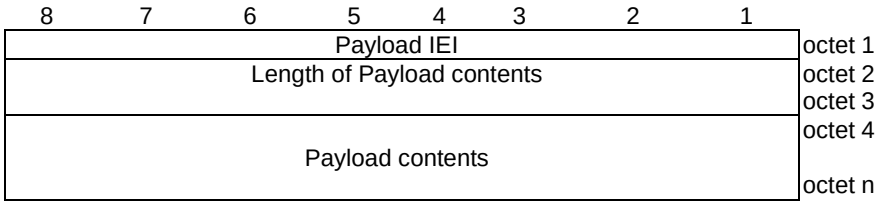

Figure 15.2.13-1: Payload information element

Table 15.2.13-1: Payload contents

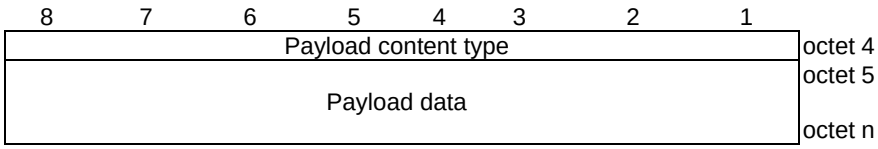

Table 15.2.13-2: Payload content type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	TEXT
0 0 0 0 0 0 1 0	BINARY
0 0 0 0 0 0 1 1	HYPERLINKS
0 0 0 0 0 1 0 0	FILEURL
0 0 0 0 0 1 0 1	LOCATION
0 0 0 0 0 1 1 0	ENHANCED STATUS
0 0 0 0 0 1 1 1	Value allocated for use in interworking (NOTE)
All other values are reserved.	
NOTE: Usage of this value is described in 3GPP TS 29.582 [48].	

Table 15.2.13-3: Payload data

Payload data is included in octet 5 to octet n; Max value of 65535 octets. Payload data contains the payload destined for the user or application. A file URL is encoded as specified in IETF RFC 1738 [70]. The length of location information payload content is 6 bytes. First 3 bytes contain the latitude information and next 3 bytes contain the longitude information.

15.2.14 MCData group ID

The MCData group ID information element is used to indicate the destination MCData group identifier;

The MCData group ID information element is coded as shown in Figure 15.2.14-1 and Table 15.2.14-1.

The MCData group ID information element is a type 6 information element.

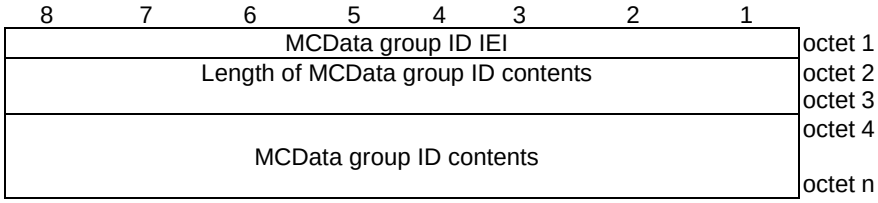

Figure 15.2.14-1: MCData group ID information element

Table 15.2.14-1: MCData group ID information element

MCData group ID is contained in octet 4 to octet n; Max value of 65535 octets.

15.2.15 MCData user ID

The MCData user ID information element is used to indicate an MCData user ID.

The MCData user ID information element is coded as shown in Figure 15.2.15-1 and Table 15.2.15-1.

The MCData user ID information element is a type 6 information element.

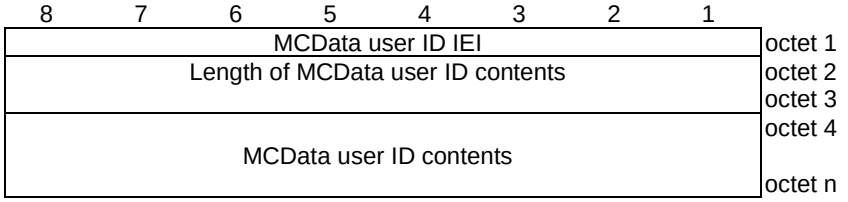

Figure 15.2.15-1: MCData user ID information element

Table 15.2.15-1: MCData user ID information element

MCData user ID is contained in octet 4 to octet n if the IE is used as an optional IE. If used as a mandatory IE, MCData user ID IEI is omitted and MCData user ID is contained in octet 3 to octet n; Max value of 65535 octets.

15.2.16 Mandatory download

The purpose of the Mandatory download information element is for the originating client to inform the terminating client that a file must be downloaded immediately.

The value part of the Mandatory download information element is coded as shown in Figure 15.2.16-1 and Table 15.2.16-1.

The Mandatory download information element is a type 1 information element.

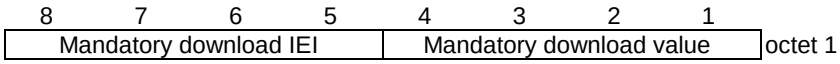

Figure 15.2.16-1: Mandatory download

Table 15.2.16-1: Mandatory download

Mandatory download value (octet 1) Bits 4 3 2 1 0 0 0 1 MANDATORY DOWNLOAD All other values are reserved.

15.2.17 Metadata

The Metadata information element is data that is used to describe a file.

The Metadata information element is coded as shown in Figure 15.2.17-1 and Table 15.2.17-1.

The Metadata information element is a type 6 information element.

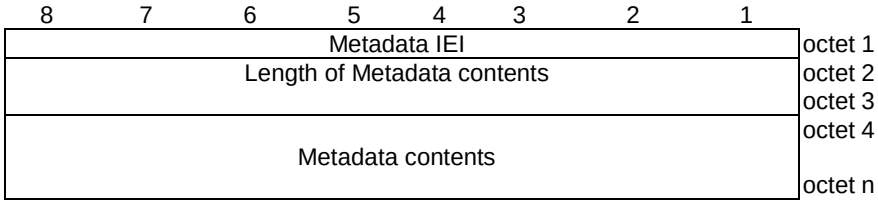

Figure 15.2.17-1: Metadata information element

Table 15.2.17-1: Metadata information element

Metadata is contained in octet 4 to octet n; Max value of n is 65535 octets.

Metadata contains a concatenation of the following data:
- **fileselector** (which is a concatenation of filename, filesize, filetype and hash)
- **file-date** (which is set to "creation", "modification" or "read" with a date/time, to indicate date/time file was created, last modified or last read)
- **file-availability** (set to a date and time that the file is available until)
- **file-description** (which is set to text specifying description of file)

The **file-selector** is encoded as shown in the "file-selector-attr" ABNF specified in IETF RFC 5547 [69].

The **file-date** is encoded as shown in the "file-date-attr" ABNF specified in IETF RFC 5547 [69].

The **file-availability** is encoded as

file-availability = "file-availability:" date-time
;date-time is defined in IETF RFC 5322 [34]

The **file-description** is encoded as

file-description = “file-description:” <text to describe file>

15.2.18 Notification type

The purpose of the Notification type information element is to identify the type of notification sent from receiver to the sender.

The value part of the Notification type information element is coded as shown in Table 15.2.18-1.

The notification type information element is a type 3 information element with a length of 1 octet.

Table 15.2.18.1: Notification type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	FILE EXPIRED UNAVAILABLE TO DOWNLOAD
0 0 0 0 0 0 1 0	FILE DELETED UNAVAILABLE TO DOWNLOAD
All other values are reserved.	

15.2.19 Data query type

The purpose of the data query type information element is to identify the type of data information that the sender requires from the receiver.

The value part of the data query request type information element is coded as shown in Figure 15.2.19-1 and Table 15.2.19-1.

The data query request type information element is a type 1 information element with a length of 1 octet

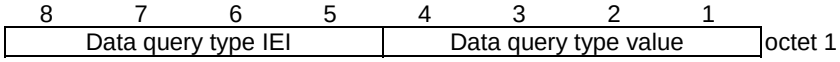

Figure 15.2.19-1: Data query type

Table 15.2.19-1: Data query type

Data query type value (octet 1) Bits 4 3 2 1	
0 0 0 1	REMAINING AMOUNT OF DATA
All other values are reserved.	

15.2.20 Comm release Information type

The purpose of the comm release information type information element is to identify the type of communication release information that the sender wants to inform to the receiver.

The value part of the comm release information type information element is coded as shown in Table 15.2.20-1.

The comm release information type information element is a type 3 information element with a length of 1 octet

Table 15.2.20-1: Comm release Information type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	INTENT TO RELEASE
0 0 0 0 0 0 1 0	EXTENSION REQUEST
0 0 0 0 0 0 1 1	EXTENSION RESPONSE
0 0 0 0 0 1 0 0	AUTH USER RELEASE REQ
All other values are reserved.	

15.2.21 Extension response type

The purpose of the extension request type information element is to inform MCData server's response towards MCData client's request for extension of the MCData communication. This information element is used only when comm release information type IE takes "EXTENSION RESPONSE" value. The receiver can ignore Extension response type information element value if comm release information type IE takes any other value.

The value part of the Extension response type information element is coded as shown in Figure 15.2.21.1 and Table 15.2.21-1.

The Extension response type information element is a type 1 information element.

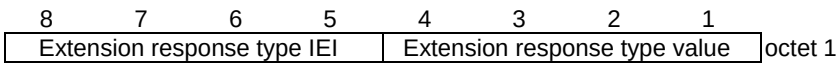

Figure 15.2.21-1: Extension response type

Table 15.2.21-1: Extension response type

Extension response type value (octet 1)				
Bits				
4	3	2	1	
0	0	0	1	ACCEPTED
0	0	1	0	REJECTED
All other values are reserved.				

15.2.22 Termination Information type

The purpose of the Termination information type is to identify the type of termination request that the sender wants to inform to the receiver.

The value part of the Termination information type element is coded as shown in table 15.2.22-1.

The Termination information type is a type 3 information element with a length of 1 octet.

Table 15.2.22-1: Termination Information type

Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	TERMINATION REQUEST
0	0	0	0	0	0	1	0	TERMINATION RESPONSE
0	0	0	0	0	0	1	1	TRANSMISSION STOPPED
0	0	0	0	0	1	0	0	INTENT TO RELEASE COMM OVER HTTP
0	0	0	0	0	1	0	1	EXTENSION REQUEST FOR COMM OVER HTTP
0	0	0	0	0	1	1	0	EXTENSION RESPONSE FOR COMM OVER HTTP
0	0	0	0	0	1	1	1	AUTH USER TERMINATION REQUEST FOR COMM OVER HTTP
All other values are reserved.								

15.2.23 Release Response Type

The purpose of the Release Response Type information element is to inform MCData server's response towards MCData client's request for termination of the MCData communication. This information element is used only when Termination information type IE takes "TERMINATION RESPONSE" value. The receiver can ignore Release response type information element value if Termination information type IE takes any other value

The value part of the Release response type information element is coded as shown in figure 15.2.23.1 and table 15.2.23-1.

The Release Response Type information element is a type 1 information element.

8	7	6	5	4	3	2	1	
Release Response Type IEI				Release Response Type value				octet 1

Figure 15.2.23-1: Release Response Type

Table 15.2.23-1: Release Response Type

Release Response Type value (octet 1)				
Bits				
4	3	2	1	
0	0	0	1	RELEASE SUCCESS
0	0	1	0	RELEASE FAILED
All other values are reserved.				

15.2.24 Extended application ID

The purpose of the Extended application ID information element is to uniquely identify the application for which the payload is intended when the format of the identifier used is not the format available in the Application ID.

The Extended application ID information element is coded as shown in figure 15.2.24-1, table 15.2.24-1, table 15.2.24-2 and table 15.2.24-3.

The Extended application ID information element is a type 6 information element.

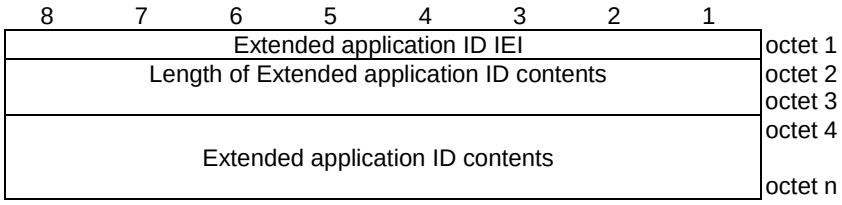

Figure 15.2.24-1: Extended application ID value

Table 15.2.24-1: Extended application ID contents

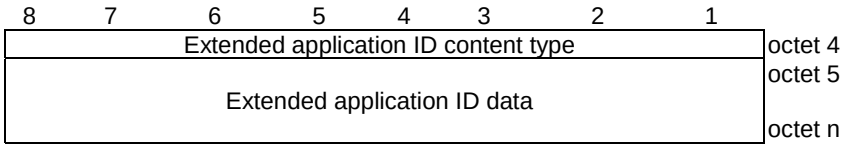

Table 15.2.24-2: Extended application ID content type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	TEXT
0 0 0 0 0 0 1 0	URI
All other values are reserved.	

Table 15.2.24-3: Extended application ID data

Extended application ID data is included in octet 5 to octet n; Max length 65534 octets. Extended application ID data contains a value that uniquely identifies the destination application, encoded in the format specified by Extended application ID content type. A URI is encoded as specified in IETF RFC 3986 [46].

15.2.25 User location

The User location information element is used to indicate the current location of the MCData client;

The User location information element is coded as shown in figure 15.2.25-1 and table 15.2.25-1.

The User location information element is a type 6 information element.

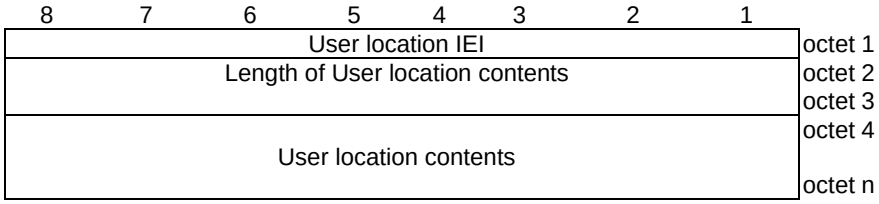

Figure 15.2.25-1: User location information element

Table 15.2.25-1: User location information element

User location is contained in octet 4 to octet n; Max value of 65535 octets.

The User location information element contains the LocationInfo structure defined in subclause 7.4 of 3GPP TS 29.199-09 [65].

15.2.26 Organization name

The Organization name information element is used to indicate the name of the organization to which the user belongs.

The Organization name information element is coded as shown in figure 15.2.26-1 and table 15.2.26-1.

The Organization name information element is a type 6 information element.

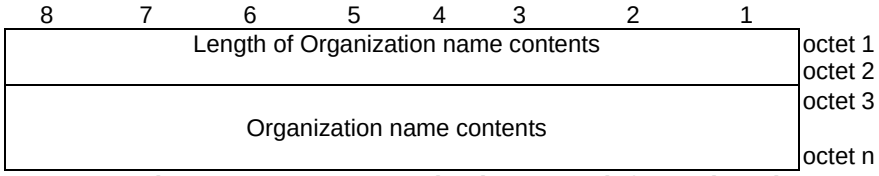

Figure 15.2.26-1: Organization name information element

Table 15.2.26-1: Organization name information element

Organization name is contained in octet 3 to octet n; Max value of 65535 octets.

16 Emergency Alert

16.1 General

This clause describes the emergency alert procedures for on-network.

For on-network emergency alert, the procedures for originating and terminating MCData clients, participating MCData function and controlling MCData function are specified in subclause 16.2.

For off-network emergency alert, the procedures for each functional entity is specified in subclause 16.3.

16.2 On-network emergency alert

16.2.1 Client procedures

16.2.1.1 Emergency alert origination

Upon receiving a request from the MCData user to send an MCData emergency alert, the MCData client shall determine whether or not it is authorised to originate an emergency alert, as follows:

1) if the <allow-activate-emergency-alert> element of the <actions> element of a <rule> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index associated with MCData user (see 3GPP TS 24.484 [12]) is present and is set to a value of "true", then the MCData emergency alert request shall be considered to be an authorised request for an MCData emergency alert. In all other cases, the MCData client shall indicate to the MCData user that the request for sending an MCData emergency alert is unauthorised and shall terminate this procedure.

If the request was authorised, but the MCData user has not indicated the identity of the MCData group to receive the emergency alert, the MCData client shall use, in descending order of preference, one of the following: the value of the <entry> element of the <GroupEmergencyAlert> element of the <Common> element in the MCData user profile, if present; if not, the identity of the MCData group to which the most recent communication or affiliation request was made by the MCData client since last acquiring the MCData service. If an MCData group identity cannot be determined, the MCData client shall indicate the fact to the MCData user and shall terminate this procedure.

The MCData client shall generate a SIP MESSAGE as an out-of-dialog request, in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6], and:

1) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

2) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [5];

4) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element (see clause D.1) with:

   a) the <mcdata-request-uri> element set to the MCData group identity;

   b) the <alert-ind> element set to a value of "true";

   c) the <mcdata-client-id> element set to the MCData client ID of the originating MCData client; and

   d) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> element set to the URI of the used functional alias;

5) shall include an application/vnd.3gpp.mcdata-location-info+xml MIME body with a <Report> element included in the <location-info> root element (see clause D.x);

6) shall include in the <Report> element the specific location information configured for the MCData emergency alert location trigger;

7) shall set the MCData emergency state if not already set;

8) shall set the MCData emergency alert state to "MDEA 2: emergency-alert-confirm-pending";

9) shall set the Request-URI to the public service identity identifying the participating MCData function serving the group identity; and

10) shall send the SIP MESSAGE request according to rules and procedures of 3GPP 24.229 [5];

On receiving a SIP 2xx response to the SIP MESSAGE request, the MCData client shall set the MCData emergency alert state to "MDEA 3: emergency-alert-initiated" and shall give the MCData user an indication of success.

On receiving a SIP 4xx response a SIP 5xx response or a SIP 6xx response to the SIP MESSAGE request, the MCData client shall set the MCData emergency alert state to "MDEA 1: no-alert" and shall indicate the failure to the MCData user.

NOTE: If no response is received after an implementation dependent amount of time or if there is an indication of communication failure, the MCData client can inform the user, and can clear the MCData emergency alert state or can retry sending the emergency alert to the MCData participating server. The MCData emergency state is left unchanged, as the MCData user presumably is in the best position to determine whether or not there still is an emergency situation and can use manual clearing, as necessary.

16.2.1.2 Emergency alert cancellation

Upon receiving a request from the MCData user to send an MCData emergency alert cancellation, the MCData client shall determine whether or not it is authorised to cancel an emergency alert, as follows:

1) if the MCData emergency cancellation request is for an MCData emergency alert originated by this MCData user, then the request shall be considered authorised if <allow-cancel-emergency-alert> element of the <actions> element of a <rule> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index associated with MCData user (see 3GPP TS 24.484 [12]) is present and is set to a value of "true"; and

2) if the MCData emergency cancellation request is for an MCData emergency alert originated by a different MCData user, then the request shall be considered authorised if <allow-cancel-emergency-alert-any-user> element of the <actions> element of a <rule> element of the <ruleset> element of the MCData user profile document identified by the MCData ID and profile index associated with MCData user (see 3GPP TS 24.484 [12]) is present and is set to a value of "true".

If the MCData emergency cancellation request is not considered authorised, the MCData client shall indicate this fact to the requesting MCData user and shall terminate this procedure.

If the authorised MCData emergency cancellation request is for an MCData emergency alert originated by this MCData user and if there are more than one outstanding emergency alerts from this MCData user and the MCData user has not indicated which one to cancel, the MCData client shall terminate this procedure after giving an indication of the condition to the MCData user.

The MCData client shall generate a SIP MESSAGE out-of dialog request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] and:

1) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

2) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) may include a P-Preferred-Identity header field containing a public user identity as specified in 3GPP TS 24.229 [5];

4) if the MCData emergency alert was originated by this MCData user, shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element (see clause D.1) with:

   a) the <mcdata-request-uri> element set to the MCData group identity;

   b) the <alert-ind> element set to a value of "false";

   c) the <mcdata-client-id> element set to the MCData client ID of this MCData client; amd

   d) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> element set to the URI of the used functional alias;

5) if the MCData emergency alert was originated by a different MCData user, shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element (see clause D.1) with:

   a) the <mcdata-request-uri> element set to the MCData group identity;

   b) the <alert-ind> element set to a value of "false";

   c) the <originated-by> element set to the MCData ID of the MCData user who originated the MCData emergency alert; and

   d) if the MCData client is aware of active functional aliases, and an active functional alias is to be included in the SIP MESSAGE request, the <functional-alias-URI> set to the URI of the used functional alias;

6) shall set the Request-URI to the public service identity identifying the participating MCData function serving the group identity;

7) if the generated SIP MESSAGE request does not contain an <originated-by> element in the application/vnd.3gpp.MCData-info+xml MIME body, shall set the MCData emergency alert state to "MDEA 4: emergency-alert-cancel-pending"; and

8) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of a SIP MESSAGE request containing an application/vnd.3gpp.mcdata-info+xml MIME body with an <alert-ind-rcvd> element set to "true" and an <mcdata-client-id> matching the MCData client ID included in the sent SIP MESSAGE request and if the sent SIP MESSAGE request did not contain an <originated-by> element in its application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall:

1) if the <alert-ind> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the received SIP MESSAGE request is set to a value of "false":

   a) set the MCData emergency alert state to "MDEA 1: no-alert"; and

   b) clear the MCData emergency state if not already cleared; and

2) if the <alert-ind> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the received SIP MESSAGE request is set to a value of "true" and if the MCData emergency alert state is set to "MDEA 4: emergency-alert-cancel-pending":

   a) set the MCData emergency alert state to "MDEA 1: no-alert".

NOTE: It would appear to be an unusual situation for the initiator of an MCData emergency alert to not be able to clear their own alert. Nevertheless, an MCData user can be configured to be authorised to initiate MCData emergency alerts but not have the authority to clear them. Hence, the case is covered here.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the sent SIP MESSAGE emergency alert cancellation request, if the sent SIP MESSAGE request did not contain an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body and the MCData emergency alert state is set to "MDEA 4: emergency-alert-cancel-pending":

1) if the received SIP 4xx response, SIP 5xx response or SIP 6xx response does not contain an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element containing the <alert-ind> element OR if it contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <alert-ind> element set to a value of "true" (see clause D.1), the MCData client shall set the MCData emergency alert state to "MDEA 3: emergency-alert-initiated".

16.2.1.3 MCData client receives an MCData emergency alert or communication notification

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

Upon receipt of a "SIP MESSAGE request for emergency notification", the MCData client:

1) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "true", should display to the MCData user an indication of the MCData emergency alert and associated information, including:

   a) the MCData group identity contained in <mcdata-calling-group-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body;

   b) the originator of the MCData emergency alert contained in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body; and

   c) the mission critical organization of the MCData emergency alert originator contained in the <mc-org> element of the application/vnd.3gpp.mcdata-info+xml MIME body;

NOTE 1: This is the case of the MCData client receiving the notification of another MCData user's emergency alert.

2) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "false":

   a) should display to the MCData user an indication of the MCData emergency alert cancellation and associated information, including:

      i) the MCData group identity contained in the <mcdata-calling-group-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body; and

      ii) the originator of the MCData emergency alert contained in:

         A) if present, the <originated-by> element of the application/vnd.3gpp.mcdata-info+xml MIME body; or

         B) the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body;

   b) if the MCData ID contained in the <originated-by> element is the MCData ID of the receiving MCData user, shall set the MCData emergency alert state to "MDEA 1: no-alert"; and

   c) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <emergency-ind> element is set to a value of "false":

      i) shall set the MCData emergency group state to "MDEG 1: no-emergency"; and

      ii) shall set the MCData emergency group communication state to "MDEGC 1: emergency-gc-capable";

NOTE 2: This is the case of the MCData client receiving the notification of the cancellation by a third party of an MCData emergency alert. This can be the MCData emergency alert of another MCData user or the MCData emergency alert of the recipient, as determined by the contents of the <originated-by> element. Optionally, notification of the cancellation of the in-progress emergency state of the MCData group can be included.

3) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <emergency-ind> element set to a value of "true":

   a) should display to the MCData user an indication of the additional emergency MCData user participating in the MCData emergency group communication including the following, if not already displayed as part of step 1):

      i) the MCData group identity contained in the <mcdata-calling-group-id> element application/vnd.3gpp.mcdata-info+xml MIME body; and

      ii) the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body; and

   b) shall set the MCData emergency group state to "MDEG 2: in-progress" if not already set to that value;

NOTE 3: This is the case of the MCData client receiving notification of an additional MCData user in an MCData emergency state (i.e., not the MCData user that originally triggered the in-progress emergency state of the group) joining the in-progress emergency group communication. An emergency alert indication, if included, is handled in step 1).

4) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <emergency-ind> element set to a value of "false":

   a) should display to the MCData user an indication of the cancellation of the in-progress emergency state of the MCData group communication including the following if not already displayed as part of step 2):

      i) the MCData group identity contained in the <mcdata-calling-group-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body; and

      ii) the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body;

   b) shall set the MCData emergency group state to "MDEG 1: no-emergency"; and

   c) shall set the MCData emergency group communication state to "MDEGC 1: emergency-gc-capable";

NOTE 4: This is the case of the MCData client receiving the notification of the cancellation of the in-progress emergency state of the MCData group. In this case, the receiving MCData client is affiliated with the MCData group but not participating in the session. An emergency alert cancellation, if included, is handled in step 2).

5) shall generate a SIP 200 (OK) response according to rules and procedures of TS 24.229 [5]; and

6) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of TS 24.229 [5].

16.2.2 Participating MCData function procedures

16.2.2.1 Receipt of a SIP MESSAGE request for emergency notification from the served MCData client

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

Upon receipt of a "SIP MESSAGE request for emergency notification for originating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field in the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

NOTE 1: if the SIP MESSAGE request contains an emergency indication set to a value of "true" or an alert indication set to a value of "true", the participating MCData function can, according to local policy, choose to accept the request.

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE request, and shall authorise the calling user;

NOTE 2: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in clause 7.3.

3) if the MCData user is not affiliated with the MCData group as determined by clause 8.3.2.11, shall perform the actions specified in clause 8.3.2.12 for implicit affiliation;

4) if the actions for implicit affiliation specified in step 3) above were performed but not successful in affiliating the MCData user due to the MCData user already having N2 simultaneous affiliations, shall reject the "SIP MESSAGE request for emergency notification for originating participating MCData function" with a SIP 486 (Busy Here) response with the warning text set to "102 too many simultaneous affiliations" in a Warning header field as specified in clause 4.9 and skip the rest of the steps;

NOTE 3: N2 is the total number of MCData groups that an MCData user can be affiliated to simultaneously as specified in 3GPP TS 23.282 [2].

NOTE 4: As this is a request for MCData emergency services, the participating MCData function can choose to accept the request.

5) shall determine the public service identity of the controlling MCData function associated with the group identity in the received SIP MESSAGE request;

6) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

7) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCData function associated with the group identified by the <mcdata-request-uri> element contained in the <mcdatainfo> element containing the <mcdata-Params> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the incoming SIP MESSAGE request;

8) shall copy the contents of the application/vnd.3gpp.mcdata-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcdata-info+xml MIME body as specified in clause D.1 included in the outgoing SIP MESSAGE request;

9) shall set the <mcdata-calling-user-id> element of the <mcdatainfo> element containing the <mcdata-Params> element to the MCData ID determined in step 2) above;

10) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-location-info+xml MIME body as specified in clause D.4, shall copy the contents of the application/vnd.3gpp.mcdata-location-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcdata-location-info+xml MIME body included in the outgoing SIP MESSAGE request;

11) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

12) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 2xx response in response to the SIP MESSAGE request sent in step 12):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5] with the follow clarifications:

   a) shall include the public user identity received in the P-Asserted-Identity header field of the incoming SIP 2xx response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response;

2) if the procedures of clause 8.3.2.12 for implicit affiliation were performed in the present subclause, shall complete the implicit affiliation by performing the procedures of clause 8.3.2.13; and

3) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the sent SIP MESSAGE request and if the implicit affiliation procedures of clause 8.3.2.12 were invoked in the present subclause, the participating MCData function shall perform the procedures of subclause 8.3.2.14.

16.2.2.2 Receipt of a SIP MESSAGE request for emergency notification for terminating MCData client

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

In the procedures in this subclause:

1) emergency indication in an incoming SIP MESSAGE request refers to the <emergency-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body; and

2) alert indication in an incoming SIP MESSAGE request refers to the <alert-ind> element of the application/vnd.3gpp.mcdata-info+xml MIME body.

Upon receipt of a "SIP MESSAGE requests for emergency notification for terminating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field in the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

NOTE 1: if the SIP MESSAGE request contains an emergency indication set to a value of "true" or an alert indication set to a value of "true", the participating MCData function can, by means beyond the scope of this specification, choose to accept the request.

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request to retrieve the binding between the MCData ID and public user identity;

3) if the binding between the MCData ID and public user identity does not exist, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response and skip the rest of the steps. Otherwise, continue with the rest of the steps;

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.1; and

5) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCData function shall follow the procedures specified in TS 24.229 [5].

16.2.2.3 Receipt of a SIP MESSAGE request indicating successful delivery of emergency notification

Upon receipt of a SIP MESSAGE request routed to the terminating participating MCData function with the Request-URI set to the public service identity of the terminating participating MCData function and the SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with an <alert-ind-rcvd> element present, the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field in the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request to retrieve the binding between the MCData ID and public user identity;

3) if the binding between the MCData ID and public user identity does not exist, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response and skip the rest of the steps. Otherwise, continue with the rest of the steps;

4) shall generate an outgoing SIP MESSAGE request in accordance with TS 24.229 [5] and IETF RFC 3428 [6] and:

   a) shall include in the SIP MESSAGE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP MESSAGE request;

   b) shall set the Request-URI of the outgoing SIP MESSAGE request to the public user identity associated to the MCData ID of the MCData user that was in the Request-URI of the incoming SIP MESSAGE request;

   c) shall copy the contents of the application/vnd.3gpp.mcdata-info+xml MIME body received in the incoming SIP MESSAGE request into an application/vnd.3gpp.mcdata-info+xml MIME body included in the outgoing SIP MESSAGE request; and

   d) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP MESSAGE request to the P-Asserted-Identity header field of the outgoing SIP MESSAGE request; and

5) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCData function shall follow the procedures specified in 3GPP TS 24.229 [5].

16.2.3 Controlling MCData function procedures

16.2.3.1 Handling of a SIP MESSAGE request for emergency notification

Upon receipt of a "SIP MESSAGE request for emergency notification for controlling MCData function", the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field in the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps. Otherwise, continue with the rest of the steps;

NOTE: If the SIP MESSAGE request contains an alert indication set to a value of "true", the controlling MCData function can, according to local policy, choose to accept the request.

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata", "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" or "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd";

3) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "false", shall perform the procedures specified in clause 16.2.3.2 and skip the rest of the steps;

4) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "true":

   a) if the received SIP MESSAGE request is an unauthorised request for an MCData emergency alert as specified in subclause 6.3.7.2.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [5] with the following clarifications:

      i) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcdata-info+xml MIME body as specified in clause D.1 with the <mcdatainfo> element containing the <mcdata-Params> element with the <alert-ind> element set to a value of "false"; and

      ii) shall send the SIP 403 (Forbidden) response as specified in TS 24.229 [5] and skip the rest of the steps; and

   b) if the received SIP MESSAGE request is an authorised request for an MCData emergency alert as specified in subclause 6.3.7.2.1:

      i) if the sending MCData user identified by the <mcdata-calling-user-id> element included in the application/vnd.3gpp.mcdata-info+xml MIME body is not affiliated with the MCData group identified by the <mcdata-request-uri> element of the MIME body as determined by the procedures of subclause 6.3.5:

         I) shall check if the MCData user is eligible to be implicitly affiliated with the MCData group as determined by subclause 8.3.3.6;

         II) if the MCData user is determined not to be eligible to be implicitly affiliated to the MCData group shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.9 and skip the rest of the steps below; or

         III) if the procedures of clause 8.3.3.6 determined the MCData user to be eligible to be implicitly affiliated to the MCData group, shall perform the implicit affiliation as specified in clause 8.3.3.7;

      ii) for each of the other affiliated members of the group:

         A) generate an outgoing SIP MESSAGE request notification of the MCData user's emergency alert indication as specified in subclause 6.3.7.1.2 with the clarifications of subclause 6.3.7.1.3;

B) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-calling-user-id> element set to the value of the <mcdata-calling-user-id> element in the received SIP MESSAGE request; and

C) send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [5];

iii) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [5] with the following clarifications:

A) shall cache the information that the MCData user has initiated an MCData emergency alert;

iv) shall send the SIP 200 (OK) response to the received SIP MESSAGE according to rules and procedures of 3GPP TS 24.229 [5].

v) shall generate a SIP MESSAGE request as described in subclause 6.3.7.1.5 to indicate successful receipt of an emergency alert, and shall include in the application/vnd.3gpp.mcdata-info+xml MIME body:

A) the <alert-ind> element set to a value of "true";

B) the <alert-ind-rcvd> element set to a value of "true"; and

C) the <mcdata-client-id> element with the MCData client ID that was included in the incoming SIP MESSAGE request; and

vi) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCData function shall follow the procedures specified in 3GPP TS 24.229 [5].

16.2.3.2 Handling of a SIP MESSAGE request for emergency alert cancellation

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

Upon receipt of a "SIP MESSAGE request for emergency notification for controlling MCData function" containing an application/vnd.3gpp.mcdata-info+xml MIME body with the <alert-ind> element set to a value of "false", the controlling MCData function:

1) if the received SIP MESSAGE request is an unauthorised request for an MCData emergency alert cancellation as specified in clause 6.3.7.2.1:

a) and if the received SIP MESSAGE request does not contain an <emergency-ind> element or is an unauthorised request for an MCData emergency communication cancellation as specified in clause 6.3.7.2.3, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [5] with the following clarifications:

i) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcdata-info+xml MIME body as specified in clause D.1 with the <mcdatainfo> element containing the <mcdata-Params> element with the <alert-ind> element set to a value of "true";

ii) if the received SIP MESSAGE request contains an <emergency-ind> element of the <mcdatainfo> element set to a value of "false" and if the in-progress emergency state of the group is set to a value of "true" and this is an unauthorised request for an MCData emergency communication cancellation as determined in step i) above, shall include an <emergency-ind> element set to a value of "true" in the application/vnd.3gpp.mcdata-info+xml MIME body in the SIP 403 (Forbidden) response; and

iii) shall send the SIP 403 (Forbidden) response according to rules and procedures of 3GPP TS 24.229 [5] and skip the rest of the steps; and

b) and if the received SIP MESSAGE request contains an <emergency-ind> element and is an authorised request for an MCData emergency communication cancellation as specified in clause 6.3.7.2.3 and the in-progress emergency state of the MCData group is set to a value of "true":

i) shall set the in-progress emergency state of the group to a value of "false";

ii) shall clear the cache of the MCData ID of the MCData user that triggered the setting of the in-progress emergency state of the MCData group;

iii) shall generate SIP re-INVITE requests to the other affiliated and joined members of the MCData group as specified in clause 6.3.7.1.1, and

A) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCData client as specified in 3GPP TS 24.229 [5];

iv) for each of the affiliated but not joined members of the group, shall:

A) generate a SIP MESSAGE request notification of the cancellation of the MCData user's emergency communication as specified in clause 6.3.7.1.2;

B) include in the application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-calling-user-id> element set to the value of the <mcdata-calling-user-id> element in the received SIP MESSAGE request; and

C) include an <emergency-ind> element set to a value of "false" in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request;

D) send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5];

v) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in TS 24.229 [5];

vi) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [5];

vii) shall generate a SIP MESSAGE request as described in clause 6.3.7.1.5 to indicate successful emergency communication cancellation;

viii) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP MESSAGE request:

A) the <alert-ind> element set to a value of "true";

B) the <alert-ind-rcvd> element set to a value of “true”;

C) the <emergency-ind> element set to a value of "false"; and

D) the <mcdata-client-id> element with the MCData client ID that was included in the incoming SIP MESSAGE request; and

ix) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5]; and

2) if the received SIP MESSAGE request is an authorised request for an MCData emergency alert cancellation as specified in clause 6.3.7.2.2:

a) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body, shall clear the cache of the MCData ID of the MCData user identified by the <originated-by> element as having an outstanding MCData emergency alert;

b) if the received SIP MESSAGE request does not contain an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body, clear the cache of the MCData ID of the sender of the SIP MESSAGE request as having an outstanding MCData emergency alert;

c) if the received SIP MESSAGE request does not contain an <emergency-ind> element or is an unauthorised request for an MCData emergency communication cancellation as specified in slause 6.3.7.2.3, for each of the affiliated but not joined members of the group shall:

i) generate a “SIP MESSAGE request for emergency notification for terminating participating MCData function” to cancel the MCData user's emergency alert as specified in clause 6.3.7.1.2;

ii) include in the application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-calling-user-id> element set to the value of the <mcdata-calling-user-id> element in the received SIP MESSAGE request;

iii) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request;

iv) include an <alert-ind> element set to a value of "false" in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request; and

v) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5];

d) if the received SIP MESSAGE request contains an <emergency-ind> element and is an authorised request for an MCData emergency communication cancellation as specified in clause 6.3.7.2.3 and the in-progress emergency state of the MCData group is set to a value of "true":

i) shall set the in-progress emergency state of the group to a value of "false";

ii) shall cache the information that the MCData user has cancelled the outstanding in-progress emergency state of the group;

iii) shall generate SIP re-INVITE requests to the other affiliated and joined members of the MCData group as specified in clause 6.3.7.1.1, and

A) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCData client as specified in 3GPP TS 24.229 [5];

iv) for each of the affiliated but not joined members of the group, shall:

A) generate a SIP MESSAGE request notification of the cancellation of the MCData user's emergency communication as specified in clause 6.3.7.1.2;

B) include in the application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with the <mcdata-calling-user-id> element set to the value of the <mcdata-calling-user-id> element in the received SIP MESSAGE request;

C) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request;

D) include in the application/vnd.3gpp.mcdata-info+xml MIME body an <alert-ind> element set to a value of "false";

E) include an <emergency-ind> element set to a value of "false" in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request; and

F) send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [5];

e) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [5];

f) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [5].

g) shall generate a SIP MESSAGE request as described in clause 6.3.7.1.5 to indicate successful receipt of the request for emergency alert cancellation;

h) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body, the <alert-ind> element set to a value of "false" and the <alert-ind-rcvd> set to "true";

i) shall populate the <mcdata-client-id> element with the MCData client ID that was included in the incoming SIP MESSAGE request;

j) if the received SIP MESSAGE request contains an <emergency-ind> element of the <mcdatainfo> element set to a value of "false":

   i) if this is an authorised request for an MCData emergency communication cancellation as specified in clause 6.3.7.2.3, shall include an <emergency-ind> element set to a value of "false" in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request; and

   ii) otherwise, if this is an unauthorised request for an MCData emergency communication cancellation as specified in clause 6.3.7.2.3, and the in-progress emergency state of the group is set to a value of "true", shall include an <emergency-ind> element set to a value of "true" in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP MESSAGE request;

k) shall send the SIP MESSAGE request according to according to the rules and procedures of TS 24.229 [5].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCData function shall follow the procedures specified in 3GPP TS 24.229 [5].

16.3 Off-network emergency alert

16.3.1 General

16.3.2 Basic state machine

16.3.2.1 General

16.3.2.2 Emergency alert state machine

The figure 16.3.2.2-1 gives an overview of the main states and transitions on the UE for emergency alert.

Each emergency alert state machine is per MCData group.

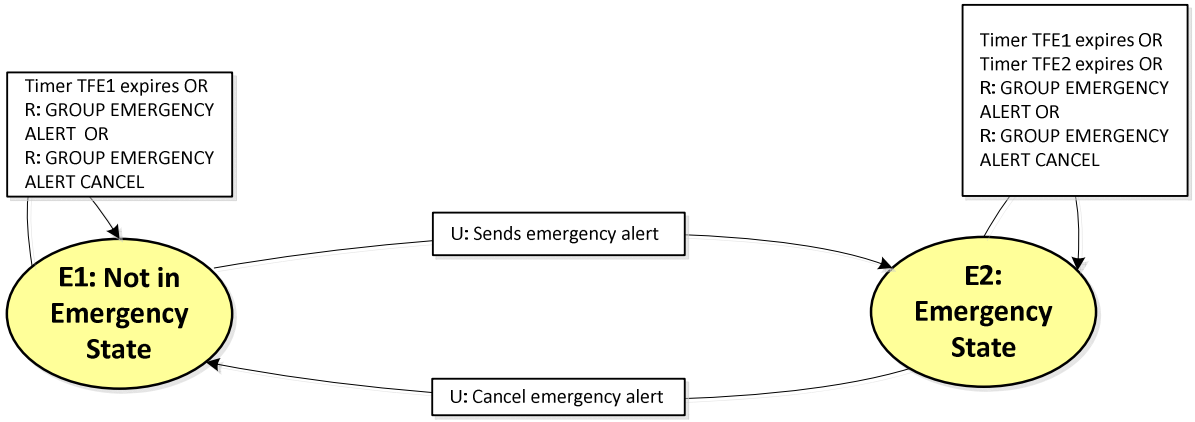

Figure 16.3.2.2-1: Emergency alert state machine

The following piece of information is associated with the emergency alert state machine:

a) the stored emergency state of the MCData group.

NOTE: The emergency alert state machine is referred by the MCData off-network group call and MCData off-network private call procedures.

16.3.2.3 Emergency alert states

16.3.2.3.1 E1: Not in emergency state

This state is the start state of this state machine.

The UE stays in this state while not in emergency state.

16.3.2.3.2 E2: Emergency state

This state exists for UE, when the UE has sent a GROUP EMERGENCY ALERT message.

16.3.3 Procedures

16.3.3.1 Originating user sending emergency alert

When in state "E1: Not in emergency state", upon receiving an indication from the MCData user to transmit an emergency alert for an MCData group ID and the value of "/<*x*>/<*x*>/Common/AllowedActivateAlert" leaf node present in the user profile as specified in 3GPP TS 24.483 [42] is set to "true", the MCData client:

1) shall set the stored emergency state as "true";
2) shall set the stored MCData group ID to the indicated MCData group ID;
3) shall generate a GROUP EMERGENCY ALERT message as specified in subclause 15.1.14. In the GROUP EMERGENCY ALERT message, the MCData client:
   a) shall set the MCData group ID IE to the stored MCData group ID;
   b) shall set the Originating MCData user ID IE to own MCData user ID;
   c) may set the Organization name IE to own organization name; and
   d) may set the User location IE with client's current location, if requested;
4) shall send the GROUP EMERGENCY ALERT message as specified in subclause 9.3.1.2;
5) shall start timer TFE2 (emergency alert retransmission); and
6) shall enter "E2: Emergency state" state.

16.3.3.2 Emergency alert retransmission

When in state "E2: Emergency state", upon expiry of timer TFE2 (emergency alert retransmission), the MCData client:

1) shall generate a GROUP EMERGENCY ALERT message as specified in subclause 15.1.14. In the GROUP EMERGENCY ALERT message, the MCData client:
   a) shall set the MCData group ID IE to the stored MCData group ID;
   b) shall set the originating MCData user ID IE to own MCData user ID;
   c) may set the Organization name IE to own organization name; and
   d) may set the Location IE with client's current location, if requested;
2) shall send the GROUP EMERGENCY ALERT message as specified in subclause 9.3.1.2;
3) shall start the timer TFE2 (emergency alert retransmission); and
4) shall remain in the current state.

16.3.3.3 Terminating user receiving emergency alert

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT message with the Originating MCData user ID IE not stored in the list of users in emergency, the MCData client:

1) shall store the Originating MCData user ID IE and location IE in the list of users in emergency;

2) shall generate a GROUP EMERGENCY ALERT ACK message as specified in subclause 15.1.15. In the GROUP EMERGENCY ALERT ACK message, the MCData client:

   a) shall set the MCData group ID IE to the MCData group ID IE of the received GROUP EMERGENCY ALERT message;

   b) shall set the Sending MCData user ID IE to own MCData user ID;

   c) shall set the Originating MCData user ID IE to the Originating MCData user ID IE of the received GROUP EMERGENCY ALERT message; and

3) shall send the GROUP EMERGENCY ALERT ACK message as specified in subclause 9.3.1.2;

4) shall start timer TFE1 (Emergency Alert); and

5) shall remain in the current state.

NOTE: Each instance of timer TFE1 is per MCData user ID.

Editor's Note: [CR 0095, WI eMCData2] Use of timer TFE1 in case of several emergency alerts from multiple users is FFS.

16.3.3.4 Terminating user receiving retransmitted emergency alert

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT message with the Originating MCData user ID IE stored in the list of users in emergency and Location IE different than the stored location of the user, the MCData client:

1) may update the stored location of the user with the received Location IE;

2) shall restart the associated timer TFE1 (Emergency Alert); and

3) shall remain in the current state.

16.3.3.5 Originating user cancels emergency alert

When in "E2: Emergency state", upon receiving an indication from the MCData user to cancel an emergency alert and the value of "/<*x*>/<*x*>/Common/AllowedCancelAlert" leaf node present in the user profile as specified in 3GPP TS 24.483 [42] is set to "true", the MCData client:

1) shall set the stored emergency state as "false";

2) shall generate a GROUP EMERGENCY ALERT CANCEL message as specified in subclause 15.1.16. In the GROUP EMERGENCY ALERT CANCEL message, the MCData client:

   a) shall set the MCData group ID IE to the stored MCData group ID; and

   b) shall set the Originating MCData user ID IE to own MCData user ID;

3) shall send the GROUP EMERGENCY ALERT CANCEL message as specified in subclause 9.3.1.2;

4) shall stop timer TFE2 (emergency alert retransmission); and

5) shall enter "E1: Not in emergency state" state.

16.3.3.6 Terminating user receives GROUP EMERGENCY ALERT CANCEL message

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT CANCEL message with the Originating MCData user ID IE stored in the list of users in emergency, the MCData client:

1) shall remove the MCData user ID and associated location information from the stored list of users in emergency;

2) shall generate a GROUP EMERGENCY ALERT CANCEL ACK message as specified in subclause 15.1.17. In the GROUP EMERGENCY ALERT CANCEL ACK message, the MCData client:

   a) shall set the MCData group ID IE to the MCData group ID IE of the received GROUP EMERGENCY ALERT CANCEL message;

   b) shall set the Sending MCData user ID IE to own MCData user ID; and

   c) shall set the Originating MCData user ID IE to the Originating MCData user ID IE of the received GROUP EMERGENCY ALERT message;

3) shall send the GROUP EMERGENCY ALERT CANCEL ACK message as specified in subclause 9.3.1.2;

4) shall stop the associated timer TFE1 (Emergency Alert); and

5) shall remain in the current state.

16.3.3.7 Implicit emergency alert cancel

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon expiry of timer TFE1 (Emergency Alert) associated with a stored MCData user ID, the MCData client:

1) shall remove the MCData user ID and associated location information from the stored list of users in emergency; and

2) shall remain in the current state.

17 Location procedures

17.1 General

If the participating MCData function needs to obtain location information, the participating MCData function configures the MCData client upon successful MCData service authorization. The configuration contains information the MCData client uses to set up filter criteria for when the MCData client shall send location reports to the participating MCData function.

The participating MCData function can also explicitly request the MCData client to send a location report.

The MCData client will, based on the received configuration or when explicitly requested, send location reports.

The location information can be used by the participating MCData function to determine whether to use MBMS bearers or not.

17.2 Participating MCData function location procedures

17.2.1 General

The participating MCData function has procedures to:

- configure the location reporting at the UE;

- request the UE to report the location of the UE; and
- receive a location information report from the UE.

17.2.2 Location reporting configuration

The participating MCData function may configure the location reporting in the MCData client by generating a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. The participating MCData function:

1) shall include a Request-URI set to the URI from MCData service authorization corresponding to the MCData ID of the MCData user;
2) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" in accordance with IETF RFC 3841 [8];
3) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-request-uri> element containing the MCData ID of the MCData user to receive the configuration;
4) shall include an application/vnd.3gpp.mcdata-location-info+xml MIME body with the <Configuration> element contained in the <location-info> root element set to the desired configuration;
5) shall include the TriggerId attribute where defined for the sub-elements defining the trigger criterion;
6) shall include the public service identity of the participating MCData function in the P-Asserted-Identity header field;
7) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and
8) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

17.2.3 Location information request

If the participating MCData function needs to request the MCData client to report its location, the participating MCData functions shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. The participating MCData function:

1) shall include a Request-URI set to the URI from MCData service authorization corresponding to the MCData ID of the MCData user;
2) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" in accordance with IETF RFC 3841 [8];
3) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with an <mcdata-request-uri> element containing the MCData ID of the MCData user;
4) shall include an application/vnd.3gpp.mcdata-location-info+xml MIME body with a <Request> element contained in the <location-info> root element;
5) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and
6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

17.2.4 Location information report

If the participating MCData function receives a SIP request containing:

1) a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml"; and
2) an application/vnd.3gpp.mcdata-location-info+xml MIME body with a <Report> element included in the <location-info> root element;

then the participating MCData function shall authorise the location report based on the MCData ID received. If the MCData user is authorised to send a location report the participating MCData function:

1) shall use the location information as needed.

NOTE: The <Report> element contains the event triggering identity in the location information report from the UE, and can contain location information.

17.2.5 Abnormal cases

Upon receipt of a SIP request:

1) where the P-Asserted-Identity identifies a public user identity not associated with an MCData user served by the participating MCData function; or

2) with a MIME body with Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and with a <mcdata-request-URI> element containing an MCData ID that identifies an MCData user served by the participating MCData function;

then, when the SIP request contains:

1) an Accept-Contact header field with the g.3gpp.mcdata media feature tag;

2) an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and

3) an application/vnd.3gpp.mcdata-location-info+xml MIME body containing a <Request> element or a <Configuration> element;

the participating MCData function shall remove the application/vnd.3gpp.mcdata-location-info+xml MIME body when sending a SIP request.

17.3 MCData client location procedures

17.3.1 General

The MCData client sends a location report when one of the trigger criteria is fulfilled or when it receives a request from the participating MCData function to send a location report. To send the location report the MCData client can use an appropriate SIP message that it needs to send for other reasons, or it can include the location report in a SIP MESSAGE request.

To send a location report, the MCData client includes in the SIP MESSAGE request an application/vnd.3gpp.mcdata-location-info+xml MIME body as specified in clause D.4. The MCData client populates the elements in accordance with its reporting configuration. Further location information may also be included in the P-Access-Network-Info header field.

17.3.2 Location reporting configuration

Upon receiving a SIP MESSAGE request containing:

1) an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

2) a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml"; and

3) an application/vnd.3gpp.mcdata-location-info+xml MIME body with a <Configuration> root element included in the <location-info> root element;

the MCData client:

1) shall store the contents of the <Configuration> elements;

2) shall set the location reporting triggers accordingly; and

3) shall start the minimumReportInterval timer.

17.3.3 Location information request

Upon receiving a SIP MESSAGE request containing:

1) an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

2) a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml"; and

3) an application/vnd.3gpp.mcdata-location-info+xml MIME body with a <Request> element included in the <location-info> root element;

the MCData client:

1) shall send a location report as specified in subclause 17.3.4; and

2) shall reset the minimumReportInterval timer.

17.3.4 Location information report

17.3.4.1 Report triggering

If a location reporting trigger fires, the MCData client checks if the minimumReportInterval timer is running. If the timer is running the MCData client waits until the timer expires. When the minimumReportInterval timer expires, the MCData client:

1) shall, if any of the reporting triggers are still true, send a location information report as specified in subclause 17.3.4.2.

If the MCData client receives a location information request as specified in subclause 17.3.3, the MCData client shall send a location report as specified in subclause 17.3.4.2.

17.3.4.2 Sending location information report

If the MCData client needs to send a SIP request anyway (i.e. for reasons other than explicit location reporting request or the firing of a configured location trigger), the MCData client:

1) shall include an application/vnd.3gpp.mcdata-location-info+xml MIME body and in the <location-info> root element the MCData client shall include:

   a) a <Report> element and, if the Report was triggered by a location request, include the <ReportID> attribute set to the value of the <RequestID> attribute in the received Request;

   b) <TriggerId> child elements, if triggers have fired, where each element is set to the value of the <Trigger-Id> attribute associated with the triggers that have fired; and

   c) the location reporting elements corresponding to the triggers that have fired, if at least one trigger has fired;

2) shall set the minimumReportInterval timer to the minimumReportInterval time and start the timer; and

3) shall reset all triggers.

If the MCData client does not need to send a SIP request for reasons other than explicit location reporting request or the firing of a configured location trigger, the MCData client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6]. The MCData client;

1) shall include in the Request-URI, the SIP URI received in the P-Asserted-Identity header field in the received SIP MESSAGE request for location report configuration;

2) shall include a Content-Type header field set to "application/vnd.3gpp.mcdata-location-info+xml";

3) shall include an application/vnd.3gpp.mcdata-location-info+xml MIME body and in the <location-info> root element include:

   a) a <Report> element and if the Report was triggered by a location request include the <ReportID> attribute set to the value of the <RequestID> attribute in the received Request;

   b) <TriggerId> child elements, if triggers have fired, where each element is set to the value of the <Trigger-Id> attribute associated with the triggers that have fired; and

   c) the location reporting elements corresponding to the triggers that have fired, if at least one trigger has fired;

4) shall include an Accept-Contact header field with the media feature tag g.3gpp.mcdata along with parameters "require" and "explicit" in accordance with IETF RFC 3841 [8];

5) shall set the minimumReportInterval timer to the minimumReportInterval time and start the timer;

6) shall reset all triggers; and

7) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [5].

18 Pre-established session

18.1 General

The MCData client may establish one or more pre-established sessions to the participating MCData function at any time after SIP registration and setting the service settings as defined in subclause 7.2.2 or subclause 7.2.3.

The MCData client may use the pre-established session for originating standalone SDS using media plane or SDS session after pre-established session establishment.

The participating MCData function may use the pre-established session for terminating standalone SDS using media plane or SDS session after pre-established session establishment.

The use of a pre-established session requires the use of resource sharing as specified in 3GPP TS 29.214 [49] and 3GPP TS 24.229 [5] by the participating MCData function. The participating MCData function use of resource sharing is defined in subclause 18.2.

18.2 Participating MCData function use of resource sharing

The participating MCData function utilizes resource sharing either:

1) via the SIP core as specified in 3GPP TS 24.229 [5]; or

2) by directly interfacing to PCC to control resource sharing via the Rx reference point as specified in 3GPP TS 29.214 [49].

If resource sharing is supported then the participating MCData function may allow the use of pre-established sessions by the MCData client.

The participating MCData function can determine that the SIP core supports resource sharing from the received third-party SIP REGISTER request if the Resource-Share header field with the value "supported" is contained in the "message/sip" MIME body of the third-party SIP REGISTER request as specified in 3GPP TS 24.229 [5].

When using resource sharing the participating MCData function uses the "+g.3gpp.registration-token" header field parameter in the Contact header field of the third-party REGISTER request to identify the MCData UE that is registering and to identify whether resource sharing and pre-established sessions can be used with a specific MCData UE.

18.3 Pre-established session for MCData SDS communication

18.3.1 General

This subclause describes the procedures to establish pre-established MCData session which may be used for originating standalone SDS using media plane or SDS session. The MCData client or the participating MCData function may initiate the release of a pre-established session as defined in subclause 18.3.3.

18.3.1.1 SDP offer generation

When composing an SDP offer according to 3GPP TS 24.229 [5], IETF RFC 4975 [17], IETF RFC 6135 [19] and IETF RFC 6714 [20] the MCData client:

1) shall include an "m=message" media-level section for the MCData media stream consisting of:

   a) the port number;

   b) a protocol field value of "TCP/MSRP" or "TCP/TLS/MSRP" for TLS;

   c) an "a=sendrecv" attribute;

   d) an "a=path" attribute containing its own MSRP URI;

   e) set the content type as "a=accept-types:application/vnd.3gpp.mcdata-signalling application/vnd.3gpp.mcdata-payload"; and

   f) set the a=setup attribute as "actpass".

18.3.1.2 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [5], the participating MCData function:

1) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCData function, for the accepted media stream in the received SDP offer, if required; and

2) if the IP address is replaced shall insert its MSRP URI before the MSRP URI in the "a=path" attribute in the SDP answer.

18.3.2 Session establishment

18.3.2.1 MCData client procedures

When the MCData client initiates a pre-established session the MCData client shall:

1) gather ICE candidates according to IETF RFC 5245 [50]; and

NOTE: ICE candidates are only gathered on interfaces that the MCData UE uses to obtain MCData service.

2) generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [5], with the clarifications given below.

The MCData client:

1) shall set the Request-URI of the SIP INVITE request to the public service identity of the participating MCData function serving the MCData user;

2) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

3) shall include the g.3gpp.mcdata.sds media feature tag in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

4) shall include an Accept-Contact header field with the media feature tag g.3gpp.mcdata.sds along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

5) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP INVITE request;

6) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

7) shall include the "timer" option tag in the Supported header field;

8) should include the Session-Expires header field according to IETF RFC 4028 [38] and should not include the "refresher" header field. The "refresher" header field parameter shall be set to "uac" if included;

9) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdataInfo> element containing the <mcdata-Params> element with the <anyExt> element an <pre-established-session-ind> element set to a value of "true";

10) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 18.3.1.1, and include ICE candidates in the SDP offer as per IETF RFC 5245 [50]; and

11) shall send the SIP INVITE request according to 3GPP TS 24.229 [5].

Upon receiving a SIP 2xx response to the SIP INVITE request the MCData client:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

18.3.2.2 Participating MCData function procedures

Upon receipt of a "SIP INVITE request for establishing a pre-established session" the participating MCData function:

1) shall check whether the public service identity is allocated and if it is not allocated, shall return a SIP 404 (Not Found) response and skip the rest of the steps;

2) shall determine the MCData ID of the MCData user establishing the pre-established session and perform actions to verify the MCData ID of the MCData client and authorise the request according to local policy, and if not authorised, the participating MCData function shall return a SIP 403 (Forbidden) response with the warning text set to "225 User not authorized to initiate pre-established session" as specified in subclause 4.9 and skip the rest of the steps;

3) shall determine whether resource sharing is supported (see subclause 18.2);

4) if resource sharing is supported by the SIP core, determine that there is a binding between the MCData ID of the MCData user establishing the pre-established session and the MCData UE identified by the "+g.3gpp.registration-token" header field parameter in the Contact header field of the third-party REGISTER request (see subclause 18.2) and that this UE identity matches the identity in the "+g.3gpp.registration-token" header field parameter in the Feature-Caps header field in the "SIP INVITE request for establishing a pre-established session";

5) if resource sharing is not supported or if there is no binding between the MCData ID of the MCData user and the identity of the MCData UE identified by the "+g.3gpp.registration-token" header field parameter in the Feature-Caps header field or the participating MCData function does not support the pre-established session, then the participating MCData function shall return a SIP 403 (Forbidden) response with the warning text set to "226 function not allowed due to pre-established session not supported" as specified in subclause 4.9 and skip the rest of the steps;

6) shall determine if the media parameters are acceptable and the MSRP URI is offered in the SDP offer and if not reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

7) shall verify that the media resources are available to support the media parameters and if not shall reject the request with a SIP 500 (Server Internal Error) response, and skip the rest of the steps;

8) shall allocate a URI to be used to identify the pre-established session;

9) shall generate a SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5]; and

   a) shall include a Contact header field containing the URI that identifies the pre-established session;

   b) shall include the public service identity in the P-Asserted-Identity header field;

   c) shall include a Supported header field containing the "norefersub" option tag;

   d) shall if the SIP core supports resource sharing, include a Resource-Share header field answer as specified in 3GPP TS 24.229 [5] with:

      A) the value "media-sharing";

      B) an "origin" header field parameter set to "session-initiator";

      C) a "timestamp" header field parameter; and

      D) a "rules" header field parameter with one resource sharing rule per media stream in the same order the corresponding m-line appears in the SDP. Each resource sharing rule is constructed as follows:

         - a "new-sharing-key" part; and

         - a "directionality" part indicating the direction of the pre-established media stream; and

   e) shall include an SDP answer as specified in 3GPP TS 24.229 [5] with the clarifications in subclause 18.3.1.2 and include ICE candidates in the SDP answer as per IETF RFC 5245 [50];

10) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

11) shall send the SIP 200 (OK) response towards the MCData client according to the rules and procedures of the 3GPP TS 24.229 [5]; and

12) shall evaluate the ICE candidates according to IETF RFC 5245 [50].

NOTE: If ICE candidate evaluation results in candidate pairs other than the default candidate pair being selected a further offer answer exchange using the procedures in subclause 18.3.4 will be needed.

18.3.3 Session release

18.3.3.1 MCData client procedures

18.3.3.1.1 MCData client initiated release

NOTE: The MCData client needs to be prepared to release the pre-established session when receiving a SIP BYE request generated by the SIP core (e.g. due to network release of media plane resources).

When a MCData client needs to release a pre-established session as created in subclause 18.3.2, the MCData client shall perform the procedure as described in subclause 13.2.2.2.2.1.

18.3.3.1.2 Participating MCData function initiated release

Upon receiving a SIP BYE request from the participating MCData function within a pre-established session the MCData client shall check whether there are any MCData sessions using the pre-established session, and:

1) if there is an established MCData session then the MCData client shall remove the MCData client from the MCData session by performing the procedures for session release for each MCData session as specified in 3GPP TS 24.582 [15]; and

2) if there is no MCData session using the pre-established session, then the MCData client shall follow the procedure described in subclause 13.2.3.2.2.

18.3.3.2 Participating MCData function procedures

18.3.3.2.1 MCData client initiated release

Upon receiving a SIP BYE request from the MCData client within a pre-established session the participating MCData function:

1) shall check whether there is a MCData session using the pre-established session, and:

   a) if there is an established MCData session then the participating MCData function shall remove the MCData client from the MCData session by performing the procedures as specified in subclause 13.2.2.2.3.1;

   b) if there is a MCData session in the process of being established, then the participating MCData function:

      i) shall send a SIP CANCEL request to cancel the MCData session in the process of being established as specified in 3GPP TS 24.229 [5]; and

      ii) shall release the MCData session as specified in the subclause 13.2.2.2.3.1, if a SIP 200 (OK) response for the SIP INVITE request is received from the remote side; and

   c) if there is no MCData session using the pre-established session, then the participating MCData function shall:

      i)_ interact with the media plane as specified in 3GPP TS 24.582 [15] for disconnecting the media plane resources towards the MCData client; and

      ii) shall generate and send a SIP 200 (OK) response to the SIP BYE request according to rules and procedures of 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response to the SIP BYE request from the remote side, the participating MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15] for releasing media plane resources towards the remote side;

2) shall interact with the media plane as specified in 3GPP TS 24.582 [15] for releasing media plane resources towards the MCData client; and

3) shall send a SIP 200 (OK) response to the SIP BYE request to the MCData client.

18.3.3.2.2 Participating MCData function initiated release

When a participating MCData function needs to release a pre-established session as created in subclause 8.2.2, the participating MCData function:

1) shall first release any participants of all MCData calls that are using the pre-established session. The participating MCData function shall remove the MCData client from the MCData session by performing the procedures as specified in subclause 13.2.2.2.3.1;

2) shall generate a SIP BYE request according to rules and procedures of 3GPP TS 24.229 [5];

3) shall set the Request-URI of the SIP BYE request to the URI that identifies the pre-established session;

4) shall send the SIP BYE request towards the MCData client within the SIP dialog of the pre-established session according to rules and procedures of the 3GPP TS 24.229 [5]; and

5) shall, upon receiving a SIP 200 (OK) response to the SIP BYE request interact with the media plane as specified in 3GPP TS 24.582 [15].

18.3.4 Session modification

18.3.4.1 MCData client procedures

18.3.4.1.1 MCData client initiated

When the MCData client needs to modify the pre-established session outside of an MCData session, the MCData client:

1) shall generate a SIP UPDATE request or a SIP re-INVITE request according to 3GPP TS 24.229 [5];

2) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 18.3.1.1, and include ICE candidates in the SDP offer as per IETF RFC 5245 [50], if required; and

3) shall send the SIP request towards the MCData server according to the rules and procedures of 3GPP TS 24.229 [5].

On receipt of the SIP 200 (OK) response the MCData client:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15], if there is a change in media parameters in the received SDP answer, compared to those in the previously agreed SDP; and

2) shall interact with the media plane as specified in 3GPP TS 24.582 [15], if there is a media stream, that is currently used in the pre-established session and is removed in the received SDP answer.

NOTE: The MCData client keeps resources for previously agreed media stream and media parameters until it receives a SIP 200 (OK) response.

18.3.4.1.2 MCData client receives SIP UPDATE or SIP re-INVITE request

Upon receiving a SIP UPDATE request or a SIP re-INVITE request to modify an existing pre-established session without associated MCData session, the MCData client:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and the MSRP URI is acceptable by the MCData client and if not reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps;

2) shall generate a SIP 200 (OK) response as follows:

   a) shall include an SDP answer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 18.3.1.2, and include ICE candidates in the SDP answer as per IETF RFC 5245 [50], if required; and

3) shall send the SIP 200 (OK) response towards the MCPTT server according to the rules and procedures of 3GPP TS 24.229 [5].

18.3.4.2 Participating MCData function procedures

18.3.4.2.1 Reception of a SIP UPDATE or SIP re-INVITE request from served MCData client

Upon receiving a SIP UPDATE request or a SIP re-INVITE request to modify an existing pre-established session without associated MCData session, the participating MCData function:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and the MSRP URI is acceptable by the participating MCData function and if not reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps; and

2) shall generate a SIP 200 (OK) response as follows:

   a) include an SDP answer according to 3GPP TS 24.229 [5] based on the received SDP offer with the clarifications given in the subclause 18.3.1.2, and include ICE candidates in the SDP answer as per IETF RFC 5245 [50], if required; and

b) include a Contact header field containing the URI that identifies the pre-established session and send a SIP 200 (OK) response according to the rules and procedures of 3GPP TS 24.229 [5].

18.3.4.2.2 Participating MCData function initiated

When the participating MCData function needs to modify the pre-established session outside of an MCData session, the participating MCData function:

1) shall generate a SIP UPDATE request or a SIP re-INVITE request according to 3GPP TS 24.229 [5];

2) shall include an SDP offer according to 3GPP TS 24.229 [5], and include ICE candidates in the SDP offer as per IETF RFC 5245 [50], if required; and

3) shall send the SIP request towards the MCData client according to the rules and procedures of 3GPP TS 24.229 [5].

On receipt of the SIP 200 (OK) response, the participating MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15], if there is change in media parameters or the MSRP URI in the received SDP answer, compared to those in the previously agreed SDP;

2) shall interact with the media plane as specified in 3GPP TS 24.582 [15], if there is a media stream, that is currently used in the pre-established session, is removed in the received SDP answer; and

3) shall interact with the media plane as specified in 3GPP TS 24.582 [15], if there is a media stream accepted in the received SDP answer, that is not currently used by the participant in the pre-established session.

NOTE: The participating MCData function keeps resources for previously agreed media stream, media parameters and the MSRP URI until it receives a SIP 200 (OK) response.

19 MBMS transmission usage procedure

19.1 General

This clause describes the participating MCData function and the MCData client procedure for:

1) MBMS bearer announcements;

2) MBMS bearer listening status; and

3) MBMS bearer suspension status.

This clause contains references to the MBMS Subchannel control messages Map Group To Bearer and Unmap Group To Bearer defined in 3GPP TS 24.582 [15].

19.2 Participating MCData function MBMS usage procedures

19.2.1 General

This subclause describes the procedures in the participating MCData function for:

1) sending an MBMS bearer announcements to the MCData client;

2) receiving an MBMS bearer listening status from the MCData client; and

3) receiving an MBMS bearer suspension status from the MCData client.

19.2.2 Sending MBMS bearer announcement procedures

19.2.2.1 General

The availability of a MBMS bearer is announced to MCData clients by means of an MBMS bearer announcement message. One or more MBMS bearer announcement elements are included in an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body.

An MBMS bearer announcement message can contain new MBMS bearer announcements, updated MBMS bearer announcements or cancelled MBMS bearer announcements or a mix of all of them at the same time in an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body. Each initial MBMS bearer announcement message announces one MBMS bearer intended to carry a general purpose MBMS subchannel used for application level multicast signalling in a specified MBMS service area and additionally, the message could also announce zero or more extra MBMS bearers intended to carry additional media plane traffic.

NOTE: A new MBMS bearer announcement does not implicitly remove previously sent MBMS bearer announcements if the previously sent MBMS bearer announcement is not included in an MBMS bearer announcement message. However, the application/sdp MIME body, if included in the new MBMS bearer announcement message, fully replaces the existing application/sdp MIME body (which includes the MSCCK security key used to protect the general purpose MBMS subchannel).

When and to whom the participating MCData function sends the MBMS bearer announcement is based on local policy in the participating MCData function.

The following subclauses describe how the participating MCData function:

1. sends an initial MBMS bearer announcement message;
2. updates a previously sent announcement of MBMS bearer(s);
3. cancels a previously sent announcement of MBMS bearer(s); and
4. keys, re-keys or un-keys MCData groups using Multicast Signalling Key (MuSiK) via a key download procedure.

Prior to the participating MCData function transmitting on an MBMS bearer, the participating MCData function:

1. if necessary, shall instruct the local key management client to request keying material from the key management server as described in 3GPP TS 33.180 [26];
2. shall generate MSCCK(s) with the corresponding MSCCK-ID(s) and MuSiK(s) with the corresponding MuSiK-ID(s) as necessary; and
3. shall distribute MSCCKs, MSCCK-IDs, MuSiKs and MuSiK-IDs to the MCData clients, as needed, using the keying material received from the key management server for security protection, as described in 3GPP TS 33.180 [26].

19.2.2.2 Sending an initial MBMS bearer announcement procedure

For each MCData client that the participating MCData function is sending an MBMS bearer announcement to, the participating MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];
2) shall set the Request-URI to the URI received in the To header field in a third-party SIP REGISTER request;
3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];
4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";
5) shall include one application/sdp MIME body conforming to 3GPP TS 24.229 [5] where the application/sdp MIME body:

a) shall include the Content-Disposition header field with the value "render";

b) should include one or more "m=message" media lines and media line attributes conforming to IETF RFC 4566 [71] and IETF RFC 5888 [72], to be used as the MBMS subchannel for media only. Additionally, the participating MCData function:

NOTE 0: Unciphered packets (i.e. using RTP/UDP/IP encapsulation) and ciphered packets (i.e. using SRTP/UDP/IP encapsulation) need separate media lines, with different transport protocols.

i) shall set the c-line to the unspecified address (0.0.0.0), if IPv4, or to a domain name within the ".invalid" DNS top-level domain, if IPv6; and

ii) shall set the port number of the media line to 9; and

iii) shall set the <proto> sub-field of the media line to RTP/AVP for unciphered traffic or to RTP/SAVP for ciphered traffic, to be used for the MBMS subchannel associated to the media line; and

c) shall include one "m=application" media line to be used for the general purpose MBMS subchannel. The media line shall include a valid multicast IP address and a valid port number. If the protection of MBMS subchannel control messages sent over this MBMS subchannel of the MBMS bearer is required, the participating MCData function also includes an "a=key-mgmt" media-level attribute. The participating MCData function:

i) shall encrypt the MSCCK to a UID associated to the targeted MCData ID and a time related parameter as described in 3GPP TS 33.180 [26];

ii) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated MSCCK and MSCCK-ID as specified in 3GPP TS 33.180 [26];

iii) shall add the public service identity of the participating MCData function to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26];

iv) shall sign the MIKEY-SAKKE I_MESSAGE using the public service identity of the participating MCData function signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [26]; and

v) shall include the "mikey" key management and protocol identifier and the signed MIKEY-SAKKE I_MESSAGE in the value of the a=key-mgmt" media-level attribute according to IETF RFC 4567 [45]; and

6) shall include an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body defined in clause D.5 with the <version> element set to "1" and one or more <announcement> elements associated with the pre-activated MBMS bearers. Each set of an <announcement> element:

a) shall include a TMGI value in the <TMGI> element;

NOTE 2: The same TMGI value can only appear in one <announcement> element. The TMGI value is also used to identify the <announcement> when updating or cancelling the <announcement> element.

NOTE 3: The security key active for the general purpose MBMS subchannel on which the mapping (i.e. the Map Group To Bearer message) of media to this MBMS bearer was indicated, is used for MBMS subchannels on this MBMS bearer, unless a different key or an indication of not using encryption is in place.

b) shall include the QCI value in the <QCI> element;

c) if multiple carriers are supported, shall include the frequency to be used in the <frequency> element;

NOTE 4: In the current release, if the <frequency> element is included, the frequency in the <frequency> element is the same as the frequency used for unicast.

d) shall include one or more MBMS service area IDs in <mbms-service-area-id> elements in the <mbms-service-areas> element;

NOTE 5: Initial mappings of groups to MBMS subchannels on an MBMS bearer for the purpose of carrying media can occur only where the MBMS service area for this bearer and the MBMS service area for the bearer carrying the general purpose MBMS subchannel on which the Map Group To Bearer message is sent intersect. However, once the mapping to this bearer was successful, the reception by the MCData client can continue (until Unmap Group To Bearer is received or until timeout) throughout the entire MBMS service area of this bearer.

e) may include the <report-suspension> element and set it to "true" value or the "false" value;

NOTE 6: The participating function can choose to direct some clients not to send an MBMS bearer suspension report when notified by RAN, by including the <report-suspension> element set to "false". The purpose is to prevent an avalanche of identical reports sent by clients roughly at the same time, to report the suspension of the same MBMS bearer. The way the participation function determines which clients are to send or not to send the report is outside the scope of the present document.

f) if the MBMS bearer is carrying the general purpose MBMS subchannel, shall include one <GPMS>element, giving the number of the "m=application" media line in the application/sdp MIME body generated in step 5 above to be used for the general purpose MBMS subchannel; and

g) if the packet headers are compressed with ROHC specified in RFC 5795 [60] in this MBMS bearer, the <anyExt> element in the <announcement> element in the <mcdata-mbms-usage-info> element shall include the <mcdata-mbms-rohc> element defined in subclause D.5.3.

7) shall include the MBMS public service identity of the participating MCData function in the P-Asserted-Identity header field;

8) shall include in a MIME body with Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml", the <mcdata-request-uri> element set to the MCData ID of the user; and

9) shall send the SIP MESSAGE request towards the MCData client according to 3GPP TS 24.229 [5].

19.2.2.3 Updating an announcement

When the participating MCData function wants to update a previously sent announcement, the participating MCData function sends an MBMS bearer announcement in an SIP MESSAGE request as specified in subclause 19.2.2.2 where the participating MCData function in the <announcement> element to be updated:

1) shall include the same TMGI value as in the MBMS bearer announcement to be updated in the <TMGI> element;

NOTE 1: TMGI value is used to identify the <announcement> when updating or cancelling the <announcement> element and can't be changed.

2) shall include the same or an updated value of the QCI in the <QCI> element;

3) if a frequency was included in the previously sent announcement, shall include the same value in the <frequency> element;

NOTE 2: In the current release if the <frequency> element is included, the frequency in the <frequency> element is the same as the frequency used for unicast.

4) shall include the same list of MBMS service area IDs or an updated list of MBMS service area IDs in <mbms-service-area-id> elements in the <mbms-service-areas> element;

5) may include the same or an updated value in the <report-suspension> element;

6) shall include the <GPMS> element with the same value as in the initial <announcement> element; and

7) shall include the same application/sdp MIME body as included in the initial MBMS announcement.

19.2.2.4 Cancelling an MBMS bearer announcement

When the participating MCData function wants to cancel an MBMS bearer announcement associated with an <announcement> element, the participating MCData function sends an MBMS bearer announcement as specified in subclause 19.2.2.2 where the participating MCData function in the <announcement> element to be cancelled:

1) shall include the same TMGI value as in the <announcement> element to be cancelled in the <TMGI> element;

2) shall not include an <mbms-service-areas> element;

3) if the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body only contains <announcement> elements that are to be cancelled, shall not include an <GPMS> element; and

4) if the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body only contains <announcement> elements that are to be cancelled, shall not include an application/sdp MIME body.

19.2.2.5 Sending a MuSiK download message

For each MCData client that the participating MCData function is intending to use a Multicast Signalling Key (MuSiK), the participating MCData function shall perform a key download procedure for a MuSiK and its corresponding MuSiK-ID. Two kinds of MuSiK download are possible: default MuSiK download and explicit MuSiK download. The default MuSiK download is used to set, reset or unset a MuSiK and its corresponding MuSiK-ID and is applicable to all groups supported by the MCData client, except for certain identified groups for which MuSiKs and MUSiK-IDs are assigned, reassigned or unassigned separately via explicit MuSiK download. The default MuSiK and MUSiK-ID can apply to all the MCData clients supported by the participating MCData function and can be overridden by the explicit MuSiK download which is selectively applied only to the MCData clients using the explicitly identified groups. A group subject to explicit MuSiK download, can be switched to the default MuSiK protection via a default MuSiK download identifying that group. The participating MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6];

2) shall set the Request-URI to the URI received in the To header field in a third-party SIP REGISTER request;

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

5) shall include an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body defined in subclause D.5 with the <version> element set to "1", and either

   a) containing an <mbms-explicitMuSiK-download> element with at least one <group> element associated with the MuSiK being downloaded; or

   b) containing an <mbms-defaultMuSiK-download> element with zero or more <group> elements associated with the MuSiK being downloaded;

6) if protection for the group(s) in the specified list is to be provided using the MuSiK, shall include an application/mikey MIME body with the MIKEY message containing the encrypted MuSiK and the corresponding MuSiK-ID, constructed as described in subclauses 5.8.1 and 5.2.2 of 3GPP TS 33.180 [26];

NOTE: Subclause 9.2.1.3 of 3GPP TS 33.180 [26] shows an example on how to include an application/mikey MIME body in a SIP message.

7) shall send the SIP MESSAGE request towards the MCData client according to 3GPP TS 24.229 [5].

The participating MCData function shall consider the key download successful on receipt of a 200 OK message in response to the SIP MESSAGE request sent in step 7).

A participating MCData function that does not receive a 200 OK message from a specific MCData client shall use unicast with that MCData client, for the groups for which the MuSiK was intended.

19.2.3 Receiving an MBMS bearer listening status from an MCData client

Upon receiving a "SIP MESSAGE request for an MBMS listening status update", the participating MCData function shall handle the request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6].

If the SIP MESSAGE request contains:

1) an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body with an <mbms-listening-status> element; and

2) an application/vnd.3gpp.mcdata-info+xml MIME body containing an MCData ID in the <mcdata-request-uri> served by the participating MCData function;

then the participating MCData function:

1) shall verify that the public user identity in the P-Asserted-Identity header field is bound to the MCData ID in the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body, and if that is the case:

   a) if the <mbms-listening-status> element is set to "listening":

      i) if a <session-id> element is included, shall indicate to the media plane that the MCData client in the session identified by the <session-id> element is now listening to the MBMS subchannel; and

      ii) if <general-purpose> element is included with the value "true", shall indicate to the media plane that the MCData client is now listening to the general purpose MBMS subchannel; and

   b) if the <mbms-listening-status> element is set to "not-listening":

      i) if a <session-id> element is included, shall indicate to the media plane that the MCData client in the sessions identified by the <session-id> elements is not listening to the MBMS subchannel;

      ii) if <general-purpose> element is included with the value "false", shall indicate to the media plane that the MCData client is no longer listening to the general purpose MBMS bearer; and

      iii) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

NOTE 1: If the MCData client reports that the MCData client is no longer listening to the general purpose MBMS subchannel it is implicitly understood that the MCData client no longer listens to any MBMS subchannel in ongoing conversations that the MCData client previously reported status "listening".

If the SIP MESSAGE request contains:

1) an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body with an <mbms-suspension-status> element; and

2) an application/vnd.3gpp.mcdata-info+xml MIME body containing an MCData ID in the <mcdata-request-uri> served by the participating MCData function;

then the participating MCData function:

1) shall verify that the public user identity in the P-Asserted-Identity header field is bound to the MCData ID in the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body, and if that is the case:

   a) if the <mbms-suspension-status> element is set to "suspending":

      i) shall consider that the bearer identified by the <suspended-TMGI> element is about to be suspended and that the reduction or elimination of traffic on that bearer and/or on some of the bearers indicated in the <other-TMGI> elements can potentially avoid the suspension; and

NOTE 2: An MBMS bearer is about to be suspended when RAN has notified the clients of the decision to suspend the bearer, but the actual suspension, which would occur at the end of the MCCH modification period, has not taken place yet because the MCCH modification period has not yet expired.

      ii) may take implementation/configuration specific immediate action for the MCData client that reports the suspension as well as other MCData clients that listen to the same bearer (e.g. moving traffic to unicast bearer(s)), reducing transmission rate, eliminating traffic, modifying pre-emption priority); or

   b) if the <mbms-suspension-status> element is set to "not-suspending":

      i) shall consider that the bearer identified by the <suspended-TMGI> element is no longer about to be suspended; and

NOTE 3: An MBMS bearer is no longer about to be suspended when RAN has notified the clients of the decision to no longer suspend the bearer after having previously notified the clients that the bearer would be suspended at the end of the MCCH modification period. The RAN notifications to first suspend and subsequently not to suspend the same MBMS bearer would have to come within the same MCCH modification period.

ii) may take implementation/configuration specific immediate action for the MCData client that reports the suspension as well as other MCData clients that listen to the same bearer (e.g. restoring traffic previously reduced or eliminated from MBMS bearers upon reception of suspension information).

NOTE 4: If the MCData client reports that the MCData client is no longer listening to MBMS subchannels associated with the MBMS bearer indicated in the suspension information, it is implicitly understood that the suspension of that MBMS bearer has actually occurred.

19.2.4 Abnormal cases

Upon receipt of a SIP MESSAGE request with an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

1) where the P-Asserted-Identity identifies a public user identity not associated with MCData user served by the participating MCData function; or

2) with an application/vnd.3gpp.mcdata-info+xml MIME body and with a <mcdata-request-uri> element containing an MCData ID that identifies an MCData user served by the participating MCData function and an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body containing one or more <announcement> elements;

then the participating MCData function shall send a SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [5].

19.3 MCData client MBMS usage procedures

19.3.1 General

This subclause describes the procedures in the MCData client for:

1) receiving an MBMS bearer announcement from the participating MCData function;

2) sending an MBMS bearer listening status report to the participating MCData function; and

3) sending an MBMS bearer suspension status report to the participating MCData function.

19.3.2 Receiving an MBMS bearer announcement

The MCData client associates each received application/sdp MIME body and each received security key with a general purpose MBMS subchannel announced in the same MBMS Bearer Announcement message. When receiving a Map Group To Bearer message, the MCData client interprets its content (e.g. the m= line number) in the context of the application/sdp MIME body associated with the general purpose MBMS subchannel on which the Map Group To Bearer message was received.

When the MCData client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and

2) an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body containing one or more an <announcement> element(s);

then the MCData client for each <announcement> element in the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

1) if the <mbms-service-areas> element is present:

   a) if an <announcement> element with the same value of the <TMGI> element is already stored:

i) shall replace the old <announcement> element with the <announcement> element received in the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body;

b) if there is no <announcement> element with the same value of the <TMGI> element stored:

i) shall store the received <announcement> element;

c) shall associate the received announcement with the received application/sdp MIME body;

d) shall associate the received announcement with the received <GPMS> element;

e) shall store the MBMS public service identity of the participating MCData function received in the P-Asserted-Identity header field and associate the MBMS public service identity with the new <announcement> element;

f) if a "a=key-mgmt" media-level attribute with the "mikey" key management and protocol identifier and a MIKEY-SAKKE I_MESSAGE is included for the general purpose MBMS subchannel defined in the "m=application" media line in the application/sdp MIME body in the received SIP MESSAGE request,

i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]. If the initiator URI deviates from the public service identity of the participating MCData function serving the MCData user, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps;

ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.180 [26];

iii) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [26];

iv) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

v) shall extract and decrypt the encapsulated MSCCK using the participating MCData function's (KMS provisioned) UID key as described in 3GPP TS 33.180 [26]; and

vi) shall extract the MSCCK-ID, from the payload as specified in 3GPP TS 33.180 [26];

NOTE: With the MSCCK successfully shared between the participating MCData function and the served UEs, the participating MCData function is able to securely send MBMS subchannel control messages to the MCData clients.

g) shall listen to the general purpose MBMS subchannel defined in the "m=application" media line in the application/sdp MIME body in the received SIP MESSAGE request when entering an MBMS service area where the announced MBMS bearer is available; and

h) shall check the condition for sending a listening status report as specified in the subclause 19.3.3; and

2) if no <mbms-service-areas> element is present:

a) shall discard a previously stored <announcement> element identified by the value of the <TMGI>;

b) shall remove the association with the stored application/sdp MIME body and stop listening to the general purpose MBMS subchannel;

c) if no more <announcement> elements associated with the stored application/sdp MIME body are stored in the MCData client, shall remove the stored application/sdp MIME body; and

d) check the condition for sending a listening status report as specified in the subclause 19.3.3.

19.3.3 The MBMS bearer listening status and suspension report procedures

19.3.3.1 Conditions for sending an MBMS listening status report

If one of the following conditions is fulfilled:

1) if the MCData client:
   a) receives a Map Group To Bearer message over the general purpose MBMS channel;
   b) participates in a group session identified by the Map Group To Bearer message; and
   c) the status "listening" is not already reported; or
2) if the MCData client:
   a) receives an announcement as described in subclause 19.3.2;
   b) enters an MBMS service area where a general purpose MBMS is available; and
   c) experiences good MBMS bearer radio condition;

then the MCData client shall report that the MCData client is listening to the MBMS bearer as specified in subclause 19.3.3.2.

If one of the following conditions is fulfilled:

1) if the MCData client:
   a) receives an MBMS bearer announcement as described in the subclause 19.3.2;
   b) the MBMS bearer announcement contains a cancellation of an <announcement> element identified by the same TGMI value as received in a Map Group To Bearer message in an ongoing conversation; and
   c) the status "not-listening" is not already reported;
2) if the MCData client:
   a) receives an MBMS bearer announcement as described in the subclause 19.3.2;
   b) the MBMS bearer announcement contains a cancellation of an <announcement> element;
   c) does not participate in an ongoing conversation;
   d) the MCData client has reported the "listening" status due to the availability of the general purpose MBMS subchannel in the <announcement> element; and
   e) the status "not-listening" is not already reported; or
3. if the MCData client:
   a) suffers from bad MBMS bearer radio condition,

then the MCData client shall report that the MCData client is not listening to the MBMS subchannels as specified in subclause 19.3.3.2.

If all the following conditions are fulfilled:

1) the MCData client has reported "listening" as the most recent listening status relative to an MBMS bearer;
2) the MCData client is notified that the MBMS bearer is about to be suspended by the RAN; and
3) the MCData client has not received a MBMS bearer announcement containing a <report-suspension> element set to "false",

then the MCData client shall report that the MBMS bearer is about to be suspended, as specified in subclause 19.3.3.2.

If all the following conditions are fulfilled:

1) the MCData client has reported "listening" as the most recent listening status relative to an MBMS bearer;

2) the MCData client has reported that the MBMS bearer is about to be suspended, but the suspension of the bearer has not been detected yet by the MCData client;

3) the MCData client is notified that the MBMS bearer is no longer to be suspended by the RAN; and

4) the MCData client has not received a MBMS bearer announcement containing a <report-suspension> element set to "false",

then the MCData client shall report that the MBMS bearer is no longer to be suspended, as specified in subclause 19.3.3.2.

19.3.3.2 Sending the MBMS bearer listening or suspension status report

When the MCData client wants to report the MBMS bearer listening status, the MCData client:

NOTE 1: The application/vnd.3gpp.mcdata-mbms-usage-info+xml can contain both the listening status "listening" and "not listening" at the same time.

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] and

   a) shall include in the Request-URI the MBMS public service identity of the participating MCData function received in the P-Asserted-Identity header field of the announcement message;

   b) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

   c) should include a public user identity in the P-Preferred-Identity header field as specified in 3GPP TS 24.229 [5];

   d) shall include a P-Preferred-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

   e) shall include an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body with the <version> element set to "1";

   f) if the MCData client is listening to the MBMS bearer, the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

      i) shall include an <mbms-listening-status> element set to "listening";

      ii) if the intention is to report that the MCData client is listening to the MBMS subchannel for an ongoing conversation in a session (e.g. as the response to the Map Group To Bearer message), shall include the MCData session identity of the ongoing conversation in a <session-id> element;

      iii) shall include one or more <TGMI> elements for which the listening status applies; and

      iv) if the intention is to report that the MCData client is listening to the general purpose MBMS subchannel, shall include the <general-purpose> element set to "true";

   g) if the MCData client is not listening, the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

      i) shall include an <mbms-listening-status> element set to "not-listening";

      iii) shall include one or more <TGMI> elements for which the listening status applies;

      iii) if the intention is to report that the MCData client is no longer listening to the MBMS subchannel in an ongoing session (e.g. as the response to Unmap Group to Bearer message), shall include the MCData session identity in a <session-id> element; and

      iv) if the intention is to report that the MCData client is no longer listening to general purpose MBMS subchannel, shall include the <general-purpose> element set to "false"; and

NOTE 2: If the MCData client reports that the MCData client is no longer listening to the general purpose MBMS subchannel, it is implicitly understood that the MCData client no longer listens to any MBMS subchannel in ongoing conversations that the MCData client previously reported status "listening".

h) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdata-request-uri> set to the MCData ID; and

2) shall send the SIP MESSAGE request according to 3GPP TS 24.229 [5].

When the MCData client meets all the conditions specified in subclause 19.3.3.1 for reporting a change in an MBMS bearer suspension status, the MCData client:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [5] and IETF RFC 3428 [6] and

a) shall include in the Request-URI the MBMS public service identity of the participating MCData function received in the P-Asserted-Identity header field of the announcement message;

b) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

c) should include a public user identity in the P-Preferred-Identity header field as specified in 3GPP TS 24.229 [5];

d) shall include a P-Preferred-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata";

e) shall include an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body with the <version> element set to "1";

f) if at least one MBMS bearer is about to be suspended, the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

i) shall include an <mbms-suspension-status> element set to "suspending";

ii) shall set the <number-of-reported-bearers> element to the total number of the included <suspended-TMGI> elements and <other-TMGI> elements;

iii) shall include <suspended-TMGI> element(s) set to the TMGI value for each of the MTCHs on the same MCH corresponding to the MBMS bearers about to be suspended; and

iv) may include <other-TMGI> elements, if available, corresponding to the TMGI values for other MTCHs on the same MCH as the MBMS bearers to be suspended

NOTE 3: To report the suspension of MTCHs on different MCHs, the MCData client sends a separate message for each of the involved MCHs.

g) if the MBMS bearer is no longer about to be suspended, the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body:

i) shall include an <mbms-suspension-status> element set to "not-suspending";

ii) shall set the <number-of-reported-bearers> element to the number of included <suspended-TMGI> elements; and

iii) shall include a <suspended-TMGI> element set to the corresponding TMGI value for each of the MTCHs of the MBMS bearers that are no longer about to be suspended; and

h) shall include an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdata-request-uri> set to the MCData ID; and

2) shall send the SIP MESSAGE request according to 3GPP TS 24.229 [5].

NOTE 4: The MCData client reports in separate messages the MBMS bearers that are about to be suspended and the MBMS bearers that are no longer about to be suspended.

19.3.4 Receiving a MuSiK download message

When the MCData client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcdata"; and

2) with one of the following:

   a) an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body containing an <mbms-explicitMuSiK-download> element with at least one <group> subelement; or

   b) an application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body containing an <mbms-defaultMuSiK-download> element with zero or more <group> subelements;

the MCData client shall:

1) if the received message contains an <mbms-explicitMuSiK-download> element, set the impacted groups to be those groups identified by the <group> subelements;

2) if the received message contains an <mbms-defaultMuSiK-download> element without <group> subelements, set the impacted groups to be all groups not associated with currently valid explicit MuSiK downloads; and

3) if the received message contains an <mbms-defaultMuSiK-download> element with <group> subelements, first dissociate those groups identified by the <group> subelements from currently valid associations with explicit MuSiK downloads and then set the impacted groups to be all groups not associated with currently valid explicit MuSiK downloads.

If the key identifier within the CSB-ID of the MIKEY payload is a MuSiK-ID (4 most-significant bits have the value '6'), the MCData client:

1) shall process the MIKEY payload according to 3GPP TS 33.180 [26], as follows:

   a) if the initiator field (IDRi) has type 'URI' (identity hiding is not used), the client:

      i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]. If the initiator URI deviates from the public service identity of the participating MCData function serving the MCData client, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.9 and shall not continue with the rest of the steps; and

      ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.180 [26];

   b) otherwise, if the initiator field (IDRi) has type 'UID' (identity hiding in use), the client:

      i) shall convert the public service identity of participating MCData function serving the MCData user to a UID as described in 3GPP TS 33.180 [26]; and

      ii) shall compare the generated UID with the UID in the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [26]. If the two initiator UIDs deviate from each other, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

   c) otherwise, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

   d) shall use the UID to validate the signature of the I_MESSAGE as described in 3GPP TS 33.180 [26];

   e) if authentication verification of the I_MESSAGE fails or the I_MESSAGE does not contain a Status attribute, shall reject the SIP MESSAGE request by sending SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [45], and including warning text set to "136 authentication of the MIKEY-

SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

f) shall examine the Status attribute and shall either mark the associated security functions as "not in use" or shall extract and store the encapsulated MuSiK and the corresponding MuSiK-ID from the payload as specified in 3GPP TS 33.180 [26]; and

2) for each of the impacted groups, shall either associate the status 'security not in use' or shall add/replace in the storage associated with the group the MuSiK-ID and the MuSiK, for use (decrypted) as security key.

NOTE: It is expected that the MCData client is capable of storing a different MuSiK for each MCData group of interest.

The MCData client shall respond with SIP 200 OK only if it finds the message syntactically correct and recognizes it as a valid and error-free MuSiK download (default or explicit) message.

20 IP Connectivity

20.1 General

This subclause describes the IP Connectivity procedures between two MCData clients for on-network. Included are the procedures for MCData client procedures, participating MCData function procedures and controlling MCData function procedures.

20.1.1 MC Data client SDP offer/answer generation

When a MCData client decides to establish an IP Connectivity session, or is answering an IP Connectivity request the MCData client shall include an SDP offer/answer according to subclause 6.1.2 of 3GPP TS 24.229 [5] with the following clarifications:

1) shall set the IP address of the MC Data client to the IP address to be used in the IP Connectivity session; and

NOTE: The MC service operator policy determines if the MC Data client should use an already assigned IP address or should request a new IP address following the procedures defined in 3GPP TS 24.301 [43].

2) depending on the service operator policy, the client shall add a zero port number value to the media descriptions of the SDP offer, in order to inform network entities that media resources are not requested for the session , or add a specific port number value to reserve the necessary media resources to be used in the data exchange.

20.1.2 MC Data participating server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data participating function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the participating MC Data function, if required; and

NOTE: Requirements can exist for the MC Data server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) depending on the service operator policy, shall ensure the port number is zero or replace the port number with a locally assigned port number

20.1.3 MC Data controlling server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data controlling function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the controlling MC Data function, if required; and

NOTE: Requirements can exist for the MC Data controlling server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) depending on the service operator policy, shall ensure the port number is zero or replace the port number with a locally assigned port number.

20.2 MCData Client Procedures

20.2.1 MCData client originating procedures

When a MCData client receives the request by a user or user application to establish a IP Connectivity session with another MCData client the MCData client shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5] with the clarifications given below. The MCData ID of the target MCData client may be explicitly included in the request from the user or user application. If the target MCData ID is not included in the request, the MCData client may implicitly determine the target MCData ID by using the target IP Information included in the request to find a match in the One-to-One communication list of the MCData user profile document as specified in 3GPP TS 24.484 [12]. If the MCData ID of the target MCData client is determined implicitly by the target IP Information included in the request, the client searches in leaves below /<x>/<x>/Common/OnetoOne/UserList/<x>/Entry/IPInformation/<x>Entry/ for a match in the IP Information. The MCData ID is given by matching the user entry.

The MCData client:

1) shall include the g.3gpp.mcdata.ipconn media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn " in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

2) shall include an Accept-Contact header field containing the g.3gpp.mcdata.ipconn media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

3) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

4) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP INVITE request;

5) should include the "timer" option tag in the Supported header field;

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall insert in the SIP INVITE request a MIME resource-lists body with the MCData ID of the invited MCData user, according to rules and procedures of IETF RFC 5366 [18];

8) shall contain an application/vnd.3gpp.mcdata-info+xml MIME body with the <mcdatainfo> element containing the <mcdata-Params> element with:

   a) the <request-type> element set to a value of "one-to-one-ipconn"; and

   b) if the MCData client is aware of active functional aliases and if an active functional alias is to be included in the SIP INVITE request, the <functional-alias-URI> element set to the URI of the used functional alias;

9) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCData function serving the MCData user;

NOTE 1: The MCData client is configured with public service identity identifying the participating MCData function serving the MCData user.

10) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [5];

11) shall include an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.1; and

12) shall send the SIP INVITE request towards the MCData server according to 3GPP TS 24.229 [5].

On receipt of a SIP 2xx response to the SIP INVITE request, the MCData client:

1) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5];

2) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38]; and

3) shall interact with MC Data user or user application.

On receipt of a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request, the MCData client:

1) shall indicate to the MCData user or user application that the IP Connectivity session could not be established; and

2) shall send a SIP ACK request as specified in 3GPP TS 24.229 [5].

On receipt of an indication from the media plane indicating that the IP Connectivity session could not be established, the MCData client:

1) shall generate a SIP BYE request according to 3GPP TS 24.229 [5] with:

   a) Reason code set to "FAILURE_CAUSE";

   b) cause set to "1"; and

   c) text set to "Media bearer or QoS lost";

2) shall set the Request-URI to the MCData session identity to release; and

3) shall send a SIP BYE request towards MCData server according to 3GPP TS 24.229 [5].

20.2.2 MCData client terminating procedures

Upon receipt of an "initial SIP INVITE request for IP Connectivity session for terminating MCData client"request, the MCData client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [5] with the clarifications below.

The MCData client:

1) may reject the SIP INVITE request if either of the following conditions are met:

   a) MCData client does not have enough resources to handle the IP Connectivity session; or

   b) any other reason outside the scope of this specification;

   and skip the rest of the steps after step 2;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCData function either with appropriate reject code as specified in 3GPP TS 24.229 [5] and warning texts as specified in subclause 4.9 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

3) shall interact with the MCData user or user application providing the MCData ID of the inviting MCData user;

3A) may display to the MCData user the functional alias of the inviting MCData user, if provided;

4) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

5) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

6) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [38]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

7) shall include the g.3gpp.mcdata.ipconn media feature tag in the Contact header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in the Contact header field of the SIP 200 (OK) response;

9) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.1; and

10) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of an SIP ACK message to the sent SIP 200 (OK) message, the MCData client shall:

1) shall interact with MC Data user or user application.

20.3 Participating MCData function procedures

20.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP INVITE request for IP Connectivity session for originating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is:

   a) set to a value of "one-to-one-ipconn", shall determine the public service identity of the controlling MCData function hosting the one-to-one IP Connectivity service for the calling user.

5) if unable to identify the controlling MCData function for IP Connectivity session, shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to initiate MCData communications, shall reject the "SIP INVITE request for IP Connectivity session for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

8) shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5];

9) shall include the option tag "timer" in the Supported header field;

10) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

11) shall set the Request-URI of the outgoing SIP INVITE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

12) shall include the MCData ID of the originating user in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

13) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

14) shall set the P-Asserted-Identity in the outgoing SIP INVITE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP INVITE request;

15) shall include an SDP offer according to 3GPP TS 24.229 [5] based on the clause 20.1.2; and

16) shall send the SIP INVITE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP INVITE request in step 16):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.ipconn media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn”; and

   c) the isfocus media feature tag;

5) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

6) shall include an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP 200 (OK) response;

7) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

8) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response; and

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

10) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5]; and

11) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP INVITE request in step 15) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

20.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP INVITE request for IP Connectivity session for terminating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCData function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

4) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

5) shall generate a SIP INVITE request accordance with 3GPP TS 24.229 [5];

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall include the option tag "timer" in the Supported header field;

8) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.ipconn media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn”;

   c) the isfocus media feature tag;

   d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

   e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

9) shall include in the SIP INVITE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [8] that were received (if any) in the incoming SIP INVITE request;

10) shall set the Request-URI of the outgoing SIP INVITE request to the public user identity associated to the MCData ID of the terminating MCData user;

11) shall populate the outgoing SIP INVITE request with the MIME bodies that were present in the incoming SIP INVITE request;

12) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.2; and

14) shall send the SIP INVITE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

4) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.ipconn media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn”; and

   c) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCData function;

5) if the incoming SIP response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response.

6) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

7) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

8) shall interact with the media plane as specified in 3GPP TS 24.582 [15]; and

9) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

20.4 Controlling MCData function procedures

20.4.1 Originating procedures

This subclause describes the procedures for inviting an MCData client to an MCData session. The procedure is initiated by the controlling MCData function as the result of an action in subclause 20.4.2.

The controlling MCData function:

1) shall generate a SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the Supported header field set to "timer";

3) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38]. The refresher parameter shall be omitted;

4) shall include an Accept-Contact header field containing the g.3gpp.mcdata.ipconn media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

5) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" along with parameters "require" and "explicit" according to IETF RFC 3841 [8];

6) shall include a Referred-By header field with the public user identity of the inviting MCData client;

7) shall include in the Contact header field an MCData session identity for the MCData session with the g.3gpp.mcdata.ipconn media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" according to IETF RFC 3840 [16];

8) shall include in the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

9) shall set the Request-URI to the public service identity of the terminating participating MCData function associated to the MCData user to be invited;

NOTE 1: How the controlling MCData function finds the address of the terminating participating MCData function is out of the scope of the current release.

10) shall set the P-Asserted-Identity header field to the public service identity of the controlling MCData function;

11) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] in the SIP INVITE request;

12) shall include in the SIP INVITE request an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.2; and

13) shall send the SIP INVITE request towards the terminating client in accordance with 3GPP TS 24.229 [5].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCData function:

1) shall interact with the media plane as specified in 3GPP TS 24.582 [15].

NOTE 2: The procedures executed by the controlling MCData function prior to sending a response to the inviting MCData client are specified in subclause 20.4.2.

20.4.2 Terminating procedures

In the procedures in this subclause:

1) MCData ID in an incoming SIP INVITE request refers to the MCData ID of the originating user from the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request;

2) MCData ID in an outgoing SIP INVITE request refers to the MCData ID of the called user in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

Upon receipt of a "SIP INVITE request for controlling MCData function for IP Connectivity session", the controlling MCData function:

1) if unable to process the request may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcdata.ipconn media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn";

3) shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported;

4) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

5) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-ipconn" and the SIP INVITE request:

a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "227 unable to determine targeted user for one-to-one IP Connectivity" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below; and

b) contains an application/resource-lists MIME body with exactly one <entry> element, shall invite the MCData user identified by the <entry> element of the MIME body, as specified in subclause 20.4.1; and

c) can interact with the media plane, in case routing or transmission control is necessary.

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 20.4.1 and if the MCData ID in the SIP 200 (OK) response matches to the MCData ID in the corresponding SIP INVITE request. the controlling MCData function:

1) shall generate SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCData function;

5) shall include a SIP URI for the MCData session identity in the Contact header field identifying the MCData session at the controlling MCData function;

6) shall include the following in the Contact header field:

   a) the g.3gpp.mcdata.ipconn media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of “urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn”; and

   c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 20.1.2;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15]; and

10) shall send a SIP 200 (OK) response to the inviting MCData client according to 3GPP TS 24.229 [5].

21 MCData Message Store

21.1 General

This clause defines procedures for communication between MCData message store client and MCData message store function as well as MCData server and MCData message store function as specified in subclause 7.13.3 of 3GPP TS 23.282[2]. The communication between the MCData message store client and MCData message store function shall use HTTP over TLS as specified in annex A of 3GPP TS 24.482 [24].

The MCData message store function shall act as an HTTP server as defined in annex A of 3GPP TS 24.482 [24].

The MCData message store client in the role of an HTTP client shall include the MCData access token (with the “Bearer” authentication scheme) in the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

Editor's note: [eMCData2, CR 0168, C1-204022] The security mechanism for communication from the MCData server acting as an HTTP client and the Message store function acting as an HTTP server is FFS.

The HTTP server (i.e. MCData message store) shall validate the MCData access token as specified in 3GPP TS 24.482 [24].

NOTE 1: In procedures for communication between MCData message store client and MCData message store function, the MCData ID which is the identity of the MCData user is part of MCData access token as specified in 3GPP TS 24.482 [24].

NOTE 1A: In procedures for communication between MCData server and MCData message store function, the MCData ID which is the identity of the MCData user is used as the value of the resource URL variable, " boxId' as specified in subclause 5.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

The interface between MCData message store client and MCData message store function (i.e. MCData-7) as well as the interface between MCData server and MCData message store function (i.e. MCData-8) shall be based on the RESTful API as specified in OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

NOTE 2: Procedures defined for communication between the MCData message store client and MCData message store function as well as MCData server and MCData message store function in the following sections reference subclause 6 “Detailed specification of the resources” of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]. Additional information related to RESTful resources, data types and sequence diagrams are found in subclause 5 and JSON examples in appendix D of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2 MCData message store functions and client procedures

21.2.1 Object retrieval procedure

21.2.1.1 Message store client procedures

To retrieve the object from message store function, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP GET request as specified in subclause 6.2.3 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send the HTTP GET request towards the message store function.

Upon receipt of a HTTP response, the message store client shall follow the procedure as described in subclause 6.2.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.1.2 Message store function procedures

Upon receipt of the HTTP GET request from the client, as per subclause 21.2.1.1, with the Request-URI identifying a resource in the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP GET request by following the procedures described in subclause 6.2.3 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send a HTTP response towards the message store client indicating the result of the operation (e.g. if the object identified by the Request URI was successfully found, it is returned in the HTTP response).

21.2.2 Object search procedure

21.2.2.1 Message store client procedures

To search for information about a selected set of objects in the message store, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.8 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.8.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send the HTTP POST request, which may include a SelectionCriteria, towards the message store function.

Upon receipt of a HTTP response, the message store client shall follow the procedure as describe in subclause 6.8.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.2.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per subclause 21.2.2.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.8.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send an HTTP response, containing the objects matching the SelectionCriteria, towards the message store client.

21.2.3 Update object(s) procedure

21.2.3.1 Message store client procedures

To update object(s) in the message store, the message store client, acting as an HTTP client, shall either follow the procedure described in subclause 6.3 or 6.4, for individual object update, or 6.11 for bulk update of objects, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall either generate an HTTP PUT request as specified in subclause 6.3.4, 6.4.4, for individual object update, or an HTTP POST request, as specified in subclause 6.11.5, for bulk update of objects, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66], with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send HTTP PUT request, for individual object update, or HTTP POST request, for bulk update of objects, towards the message store function.

Upon receipt of a HTTP response, the message store client shall either follow the procedure as described in subclause 6.3.2, 6.4.2 for individual object update response, or subclause 6.11.2 for bulk update of objects response, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.3.2 Message store function procedures

Upon receipt of the HTTP PUT or HTTP POST request from the client, as per subclause 21.2.3.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) if the received request is an HTTP PUT, shall process the HTTP PUT request for individual object update by following the procedure described in subclauses 6.3.2 or 6.4.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66];

3) if the received request is an HTTP POST, shall process the HTTP POST request by following the procedure described in subclause 6.11.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] for bulk update of objects; and

4) shall generate and send an HTTP response towards the message store client indicating the result of the update operation.

21.2.4 Delete stored object(s) procedure

21.2.4.1 Message store client procedures

To delete object(s) in the message store, the message store client, acting as an HTTP client, shall either follow the procedure described in subclause 6.2, for individual object delete, or subclause 6.12 for bulk delete of objects, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall either generate an HTTP DELETE request as specified in subclause 6.2.6, for individual object delete, or an HTTP POST request as specified in subclause 6.12.6, for bulk delete of objects, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66], with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send HTTP DELETE request, for individual object delete, or HTTP POST request, for bulk delete of objects, towards the message store function.

Upon receipt of a HTTP response, the message store client shall either follow the procedure as described in subclause 6.2.2, for individual object delete response, or subclause 6.12.2, for bulk delete of objects response, of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.4.2 Message store function procedures

Upon receipt of the HTTP DELETE or HTTP POST request from the client, as per subclause 21.2.4.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) if the received request is an HTTP DELETE, shall process the HTTP DELETE request for individual object delete by following the procedure described in subclause 6.2.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66];

3) if the received request is an HTTP POST, shall process the HTTP POST request by following the procedure specified in subclause 6.12.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] for bulk delete of objects; and

4) shall generate and send an HTTP response towards the message store client indicating the result of the delete procedure.

21.2.5 Void

21.2.5A Deposit an object

21.2.5A.1 MCData server procedures

To deposit an object of an MCData user in the message store, the MCData server acting as an HTTP client shall follow the procedure described in clause 6.1 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarification:

1) shall generate an HTTP POST request as specified in clause 6.1.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall set the boxId of the resource URL as specified in clause 6.1.1 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] to MCData ID which is the identity of the MCData user;

   c) shall include a valid MCData access token in the HTTP Authorization header; and

2) shall send the HTTP POST request towards the message store function.

Upon receipt of an HTTP response, the MCData server shall follow the procedure described in subclause 6.1.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.5A.2 Message store function procedures

Upon receipt of an HTTP POST request from MCData server, as per subclause 21.2.5A.1, with a Request-URI identifying a resource on the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24]; and

2) if validation is successful then

   a) shall process the HTTP POST request by following the procedures described in clause 6.1.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send the HTTP response towards the MCData server indicating the result of the deposit an object operation as per subclause 6.1.2 of the OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.6 Object and folder copy procedure

21.2.6.1 Message store client procedures

To copy object(s) and/or folder(s) to a destination folder in message store, the message store client, acting as an HTTP client, shall follow the procedure described in subclause 6.18 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.18.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send HTTP POST request identifying the target folder and the source objects(s) and/or folder(s) for copying operation towards the message store function.

Upon receipt of an HTTP response, the message store client should follow the procedure as described in subclause 6.18.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.6.2 Message store function procedures

Upon receipt of the HTTP POST from the client, as per subclause 21.2.6.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.18.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and copy to the target folder the requested source object(s) and/or folders(s); and

3) shall generate and send a HTTP response towards the message store client indicating the result of the operation.

21.2.7 Deleting a folder procedure

21.2.7.1 Message store client procedures

To delete a folder in message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.14 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP DELETE request as specified in subclause 6.14.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send the HTTP DELETE request identifying the folder to be deleted towards the message store function.

Upon receipt of a HTTP response, the message store client should follow the procedure as described in subclause 6.14.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.7.2 Message store function procedures

Upon receipt of the HTTP DELETE request from the client, as per subclause 21.2.7.1, with the Request-URI identifying the folder in the message store to be deleted, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP DELETE request by following the procedures described in subclause 6.14.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall shall generate and send a HTTP response towards the message store client indicating the result of the operation.

21.2.8 Create a folder procedure

21.2.8.1 Message store client procedures

To create a folder in message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.13 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.13.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

b) shall include a valid MCData access token in the HTTP Authorization header; and

c) shall send towards the message store function the HTTP POST request identifying the target folder where the new folder is to be created.

Upon receipt of a HTTP response, the message store client should follow the procedure as described in subclause 6.13.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.8.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per subclause 21.2.8.1, identifying the new folder to be created, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.13.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and create the requested folder; and

3) shall generate and send a HTTP response towards the message store client indicating the result of the operation.

21.2.9 void

21.2.10 Moving object(s) and folder(s) procedure

21.2.10.1 Message store client procedures

To move object(s) and/or folder(s) to a destination folder in the message store, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.19 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.19.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send the HTTP POST request, identifying source objects and/or folder(s) to be moved to the designated destination folder, towards the message store function.

Upon receipt of a HTTP response, the message store client shall follow the procedure as described in subclause 6.19.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.10.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per subclause 21.2.10.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.19.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and perform the move operation; and

3) shall generate and send a HTTP response towards the message store client indicating the result of the operation.

21.2.11 Folder search procedure

21.2.11.1 Message store client procedures

To search for information about a selected set of folder(s) in the message store, the message store client, acting as an HTTP client shall follow the procedure described in subclause 6.16 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.16.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

   c) shall send the HTTP POST request, which may include a SelectionCriteria, towards the message store function.

Upon receipt of a HTTP response, the message store client should follow the procedure as described in subclause 6.16.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.11.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per subclause 21.2.11.1, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.16.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send a HTTP response, containing the folders matching the SelectionCriteria, towards the message store client.

21.2.12 Void

21.2.12ACreate a subscription to notifications

21.2.12A.1 Message store client procedures

In order for the message store client to keep its local store in sync with the MCData message store, it needs to receive notifications about changes in the message store. For this purpose, the message store client would need to subscribe to notification from the message store, Synchronization using subscriptions and notifications is described in clause 5.1.5.1 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

To create a subscription to notifications about changes in the message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in clause 6.20 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.20.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function; and

   b) shall include a valid MCData access token in the HTTP Authorization header; and

2) shall send the HTTP POST request towards the message store function.

Upon receipt of an HTTP response, the message store client should follow the procedure as described in clause 6.20.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.12A.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per subclause 21.2.12.1, with a Request-URI identifying a resource on the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24]; and

2) if validation is successful then

   a) shall process the HTTP POST request by following the procedures described in clause 6.20.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and create the requested subscription; and

3) shall generate and send an HTTP response towards the message store client indicating the result of the operation as per subclause 6.20.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.13 Void

21.2.13ADelete a subscription to notifications

21.2.13A.1 Message store client procedures

To delete / cancel a subscription and stop corresponding notifications about changes in the message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in clause 6.21 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarification:

1) shall generate an HTTP DELETE request as specified in subclause 6.21.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

2) shall send the HTTP DELETE request identifying the subscription to be deleted towards the message store function.

Upon receipt of an HTTP response, the message store client should follow the procedure as described in clause 6.21.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.13A.2 Message store function procedures

Upon receipt of the HTTP DELETE request from the client, as per clause 21.2.13.1, with a Request-URI identifying the subscription resource on the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in TS 24.482 [24]; and

2) if validation is successful then

   a) shall process the HTTP DELETE request by following the procedures described in clause 6.21.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and delete the requested subscription; and

3) shall generate and send an HTTP response towards the message store client indicating the result of the operation as per clause 6.21.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.14 Void

21.2.14AUpdate a subscription to notifications

21.2.14A.1 Message store client procedures

A client may update its subscription to notification in order to:

1) extend the life of the subscription;

2) restart the notification stream from where it left off.

Synchronization using subscriptions and notifications is described in clause 5.1.5.1 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]

To update a subscription to notifications about changes in the message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in clause 6.21 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] the with following clarification:

1) shall generate an HTTP POST request as specified in clause 6.21.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header; and

2) shall send the HTTP POST request towards the message store function.

Upon receipt of an HTTP response, the message store client should follow the procedure described in clause 6.21.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.14A.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per bclause 21.2.14A.1, with a Request-URI identifying a subscription resource on the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in TS 24.482 [24]; and

2) if validation is successful then

   a) shall process the HTTP POST request by following the procedures described in clause 6.21.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] and update the requested subscription; and

3) shall generate and send an HTTP response towards the message store client indicating the result of the operation as per clause 6.21.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.16 Synchronization notifications

21.2.16.1 Message store function procedures

To send notifications about changes in the message store using the message store function, the MCData message store, acting as an HTTP client shall follow the procedure described in clause 6.22 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarification:

1) shall generate an HTTP POST request as specified in clause 6.22.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to the callback URL which was previously provided by the client in its corresponding subscription creation request as specified in clause 21.2.12; and

   b) shall send the HTTP POST request towards the callback URL provided by the client.

Upon receipt of an HTTP response, the message store function should follow the procedure as described in clause 6.22.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.16.2 Message store client procedures

Upon receipt of the HTTP POST request from the MCData message store, as per clause 21.2.16.1, the message store client acting as an HTTP server:

1) shall process the HTTP POST request by following the procedures described in clause 6.22.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

   a) either use the notification content and the reported "restartToken" and "index" as specified in clause 5.1.5.1 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] to have the client's local message store updated accordingly; or

   b) use the notification as a trigger to subsequently search the MCData message store for the list of changes as specified in clause 21.2.11.1; and

2) shall generate and send an HTTP response towards the message store function indicating the result of the operation as per clause 6.22.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

NOTE: The notifications about changes in the MCData message store can be used by the message store client to synchronize its local message store with the MCData message store in two distinguished ways which are listed in sub-bullets "a" and "b" above.

21.2.17 Search-based synchronization

21.2.17.1 Message store client procedures

To search for changes (e.g. newly created objects, recently deleted objects, etc) in the MCData message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in clause 21.2.2.1 with following clarification:

1) shall use the search criterion of "CreatedObjects", "VanishedObjects" or "Flag" in the HTTP POST request as specified in clause 5.1.5.2 and 5.4.2.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] in order to retrieve from the message store the list of the newly created object, recently deleted object and/or changes to flags respectively.

21.2.17.2 Message store function procedures

Upon receipt of the HTTP POST request from the client, as per clause 21.2.17.1, the message store function acting as an HTTP server shall follow the procedure described in clause 21.2.2.2 with the following clarification:

1) if search criterion in the HTTP POST request is set to "CreatedObjects", then the HTTP POST, the response shall include a "creationCursor" as specified in clause 5.3.2.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.18 List subfolders of a given folder

21.2.18.1 Message store client procedures

To list subfolders of a given folder identified by its folder ID in the message store using the message store function, the message store client, acting as an HTTP client shall follow the procedure described in clause 6.14 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarification:

1) shall generate an HTTP GET request as specified in clause 6.14.3 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with the following clarifications:

   a) shall set the Host header field to a hostname identifying the message store function;

   b) shall include a valid MCData access token in the HTTP Authorization header;

c) shall set the query string "listFilter" to:

i) "Subfolders" if only a list of subfolders is to be returned;

ii) "Objects" if only a list of objects is to be returned; or

iii) "All" if a list all contents of the specified folder is to be returned; and

2) shall send the HTTP GET request towards the message store function.

NOTE: in order for the message store client to list the subfolders of the root folder, it first needs to discover its folder ID as described in clause 5.1.6 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] using Folder search procedure specified in clause 21.2.11 of the present document.

Upon receipt of an HTTP response, the message store client should follow the procedure as described in clause 6.14.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.18.2 Message store function procedures

Upon receipt of the HTTP GET request from the client, as per clause 21.2.18.1, with a Request-URI containing the query string listFilter = Subfolders, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24]; and

2) if validation is successful then

a) shall process the HTTP GET request by following the procedures described in clause 6.14.3 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send a HTTP response containing the subfolders towards the message store client indicating the result of the operation as per clause 6.14.2 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

22 Functional alias

22.1 General

Clause 22.2 contains the procedures for management of functional alias at the MCData client, the MCData server serving the MCData user and the MCData server owning the functional alias.

Clause 22.3 describes the coding used for management of functional aliases.

21.2.15 Object(s) upload procedure

21.2.15.1 Message store client procedures

To upload the object(s) to the message store, the message store client acting as an HTTP client, shall follow the procedure described in subclause 6.1 for single upload and subclause 6.10 for bulk upload as specified in the OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarification:

1) shall generate an HTTP POST request as specified in subclause 6.1.5 and 6.10.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66] with following clarifications:

a) shall set the Host header field to a hostname identifying the message store function;

b) shall include a valid MCData access token in the HTTP Authorization header; and

c) shall send the HTTP POST request towards the message store function.

Upon receipt of an HTTP response, the message store client shall follow the procedure as described in subclause 6.1.2 for single upload and 6.10.2 for bulk upload as specified in the OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66].

21.2.15.2 Message store function procedures

Upon receipt of an HTTP POST request from the client, as per subclause 21.2.15.1, with a Request-URI identifying a resource on the message store, the message store function acting as an HTTP server:

1) shall validate the MCData access token (with "Bearer" authentication scheme) received in the Authorization header of the request as specified in 3GPP TS 24.482 [24] and if validation is successful then

2) shall process the HTTP POST request by following the procedures described in subclause 6.1.5 and 6.10.5 of OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C [66]; and

3) shall generate and send the HTTP response towards the message store client indicating the result of the upload operation.

22.2 Procedures

22.2.1 MCData client procedures

22.2.1.1 General

The MCData client procedures consist of:

- a functional alias status change procedure;

- a functional alias status determination procedure; and

- a location based functional alias status change procedure.

In order to obtain information about success or rejection of changes triggered by the functional alias status change procedure for an MCData user, the MCData client needs to initiate the functional alias status determination procedure for the MCData user before starting the functional alias status change procedure for the MCData user.

22.2.1.2 Functional alias status change procedure

In order:

- to indicate that an MCData user requests to activate one or more functional aliases;

- to indicate that the MCData user requests to deactivate one or more functional aliases;

- to refresh indication of an MCData user interest in one or more functional aliases due to near expiration of the expiration time of a functional alias with the status set to the "activated" state received in a SIP NOTIFY request in subclause 22.2.1.3;

- to indicate that the MCData client entering into or exiting from a location area triggers one or more functional aliases to be activated;

- to indicate that the MCData client entering into or exiting from a location area triggers one or more functional aliases to be deactivated; or

- any combination of the above;

the MCData client shall generate a SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34], and IETF RFC 3856 [39].

When the MCData user requests to deactivate a functional alias, the MCData client shall first check the <manual-deactivation-not-allowed-if-location-criteria-met> element within the <anyExt> element of the <entry> element corresponding to the functional alias within the <FunctionalAliasList> list element of the <anyExt> element of the

<OnNetwork> element of the MCData user profile document (see the MCData user profile document in TS 24.484 [12]). If the functional alias has been activated due to a location area trigger and the <manual-deactivation-not-allowed-if-location-criteria-met> element is set to a value of "true", the MCData client shall suppress the MCData user's request.

NOTE 1: If the request is suppressed, a notification message can be displayed to the user.

In the SIP PUBLISH request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

4) if the MCData client requests to activate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [34], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the MCData client requests to deactivate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [34], to zero; and

NOTE 3: Activation and deactivation of functional alias cannot be performed with the same PUBLISH request.

6) shall include an application/pidf+xml MIME body indicating per-user functional alias information according to subclause 22.3.1. In the MIME body, the MCData client:

   a) shall include all functional aliases where the MCData user requests activation for the MCData ID;

   b) shall include the MCData client ID of the targeted MCData client;

   c) shall not include the "status" attribute and the "expires" attribute in the <functionalalias> element;

   d) if the MCData client has received an indication that take over of a functional alias is possible and intends to take over a functional alias, shall include a <take-over> child element set to "true"; and

   e) shall set the <p-id-fa> child element of the <presence> root element to a globally unique value.

The MCData client shall send the SIP PUBLISH request according to TS 24.229 [5].

22.2.1.3 Functional alias status determination procedure

NOTE 1: The MCData UE also uses this procedure to determine which functional alias have been successfully activated for the MCData ID.

In order to discover functional aliases:

1) which which are activated for the MCData user; or

2) which another MCData user has activated;

the MCData client shall generate an initial SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36].

In the SIP SUBSCRIBE request, the MCData client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCData function serving the MCData user;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData client shall include the <mcdata-request-uri> element set to the MCData ID of the targeted MCData user;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7];

4) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the MCData client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [36], to zero;

6) shall include an Events header field set to "presence"; and

7) shall include an Accept header field containing the application/pidf+xml MIME type.

In order to re-subscribe or de-subscribe, the MCData client shall generate an in-dialog SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36]. In the SIP SUBSCRIBE request, the MCData client:

1) if the MCData client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

2) if the MCData client wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [36], to zero;

3) shall include an Events header field set to "presence"; and

4) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-user functional alias information constructed according to subclause 22.3.1, then the MCData client shall determine the status of the MCData user for each functional alias in the MIME body. If the <p-id-fa> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request is included, the <p-id-fa> element value indicates the SIP PUBLISH request which triggered sending of the SIP NOTIFY request.

If the MCData client detected a functional alias activation or deactivation, it shall perform the procedure specified in subclause 8.2.6.

22.2.1.4 Location based functional alias status change procedure

If a location criterion for functional alias activation or de-activation is met, the MCData client shall initiate the functional alias status change procedure as specified in subclause 22.2.1.2.

22.2.2 MCData server procedures

22.2.2.1 General

The MCData server procedures consist of:

- procedures of MCData server serving the MCData user; and
- procedures of MCData server owning the functional alias.

22.2.2.2 Procedures of MCData server serving the MCData user

22.2.2.2.1 General

The procedures of MCData server serving the MCData user consist of:

- a receiving functional alias status change from MCData client procedure;
- a receiving subscription to functional alias status procedure;
- a sending notification of change of functional alias status procedure;
- a sending functional alias status change towards MCData server owning the functional procedure; and
- a functional alias status determination from MCData server owning the functional alias procedure.

22.2.2.2.2 Stored information

The MCData server shall maintain a list of MCData user information entries. The list of the MCData user information entries contains one MCData user information entry for each served MCData ID.

In each MCData user information entry, the MCData server shall maintain:

1) an MCData ID. This field uniquely identifies the MCData user information entry in the list of the MCData user information entries; and
2) a list of functional alias information entries.

In each functional alias information, the MCData server shall maintain:

1) a functional alias ID. This field uniquely identifies the functional alias information entry in the list of the functional alias information entries;
2) a functional alias status;
3) an expiration time;
4) a functional alias p-id-fa; and
5) a next publishing time.

22.2.2.2.3 Receiving functional alias status change from MCData client procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains either the public service identity identifying the originating participating MCData function serving the MCData user, or the public service identity identifying the terminating participating MCData function serving the MCData user;
2) the SIP PUBLISH request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element which identifies an MCData ID served by the MCData server;
3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];
4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and
5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-user functional alias information according to subclause 22.3.1;

then the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

2) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the originating participating MCData function serving the MCData user, shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP PUBLISH request;

3) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the terminating participating MCData function serving the MCData user, shall identify the originating MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;

4) if the originating MCData ID is different than the served MCData ID or the originating MCData ID is not authorized to modify functional alias status of the served MCData ID, shall send a SIP 403 (Forbidden) response and shall not continue with the rest of the steps;

5) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

6) if the Expires header field of the SIP PUBLISH request has nonzero value, shall determine the candidate expiration interval to according to IETF RFC 3903 [34];

7) if the Expires header field of the SIP PUBLISH request has zero value, shall set the candidate expiration interval to zero;

8) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34]. In the SIP 200 (OK) response, the MCData server:

   a) shall set the Expires header field according to IETF RFC 3903 [34], to the candidate expiration time;

9) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served MCData ID, shall not continue with the rest of the steps;

10) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 22.2.2.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

11) shall consider a copy of the list of the MCData functional alias entries of the served MCData user information entry as the served list of the MCData functional alias information entries;

12) if the candidate expiration interval is nonzero, shall construct the candidate list of the MCData functional alias entries as follows:

   a) for each functional alias ID which has a functional alias information entry in the served list of the functional alias information entries, such that the expiration time of the functional alias information entry has not expired yet, and which is indicated in a "functionalAliasID" attribute of a <functionalAlias> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

      i) shall copy the functional alias information entry into a new functional alias information entry of the candidate list of the functional alias information entries;

      ii) if the functional alias status of the functional alias information entry is "deactivating" or "deactivated", shall set the functional alias status of the new functional alias information entry to the "activated" state and shall reset the activating p-id-fa of the new functional alias information entry; and

      iii) shall set the expiration time of the new functional alias information entry to the current time increased with the candidate expiration interval;

   b) for each functional alias ID which has a functional alias information entry in the served list of the functional alias information entries, such that the expiration time of the functional alias information entry has not expired yet, and which is not indicated in any "functionalAliasID" attribute of the

<functionalAlias> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

i) shall copy the functional alias information entry into a new functional alias information entry of the candidate list of the functional alias information entries; and

ii) if the functional alias status of the functional alias information entry is "activated" or "activating":

- shall set the functional alias status of the new functional alias entry to the "deactivating" state; and

- shall set the expiration time of the new functional alias information entry to the current time increased with twice the value of timer F; and

c) for each functional alias ID:

i) which does not have a functional alias information entry in the served list of the functional alias entries; or

ii) which has a functional alias information entry in the served list of the functional alias information entries, such that the expiration time of the functional alias information entry has already expired;

and which is indicated in a "functionalAliasID" element of the <functionalAlias> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

i) shall add a new functional alias information entry in the candidate list of the functional alias information list for the functional alias ID;

ii) shall set the functional alias status of the new functional alias information entry to the "activating" state;

iii) shall set the expiration time of the new functional alias information entry to the current time increased with the candidate expiration interval; and

iv) shall reset the activating p-id-fa of the new functional alias information entry;

13) if the candidate expiration interval is zero, constructs the candidate list of the functional alias information entries as follows:

a) for each functional alias ID which has an entry in the served list of the functional alias information entries:

i) shall copy the functional alias entry of the served list of the functional alias information into a new functional alias information entry of the candidate list of the functional alias information entries;

ii) shall set the functional alias status of the new functional alias information entry to the "de-activating" state; and

iii) shall set the expiration time of the new functional alias information entry to the current time increased with twice the value of timer F;

14) shall replace the list of the functional alias information entries stored in the served MCData user information entry with the candidate list of the functional alias information entries;

15) shall perform the procedures specified in subclause 22.2.2.2.6 for the served MCData ID and each functional alias:

a) which does not have a functional alias information entry in the served list of the functional alias information entries and which has a functional alias information entry in the candidate list of the functional alias information entries with the functional alias status set to the "activating" state;

b) which has a functional alias information entry in the served list of the functional alias information entries with the expiration time already expired, and which has a functional alias information entry in the candidate list of the functional alias information entries with the functional alias status set to the "activating" state;

c) which has a functional alias information entry in the served list of the functional alias information entries with the functional alias status set to the "deactivating" state or the "deactivated" state and with the expiration

time not expired yet, and which has an functional alias information entry in the candidate list of the functional alias information entries with the functional alias status set to the "activating" state; or

d) which has a functional alias information entry in the served list of the functional alias information entries with the functional alias status set to the "activated" state and with the expiration time not expired yet, and which has an functional alias information entry in the candidate list of the functional alias information entries with the functional alias status set to the "deactivating" state;

16) shall identify the handled p-id-fa in the <p-id-fa> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

17) shall perform the procedures specified in subclause 22.2.2.2.5 for the served MCData ID.

22.2.2.2.4 Receiving subscription to functional alias status procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains either the public service identity identifying the originating participating MCData function serving the MCData user, or the public service identity identifying the terminating participating MCData function serving the MCData user;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element which identifies an MCData ID served by the MCData server;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7]; and

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

the MCData server:

1) shall identify the served MCData ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

2) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the originating participating MCData function serving the MCData user, shall identify the originating MCData ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the terminating participating MCData function serving the MCData user, shall identify the originating MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

4) if the originating MCData ID is different than the served MCData ID and the originating MCData ID is not authorized to modify functional alias status of the served MCData ID, shall send a SIP 403 (Forbidden) response and shall not continue with the rest of the steps; and

5) shall generate a SIP 200 (OK) response to the SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 6665 [36].

For the duration of the subscription, the MCData server shall notify the subscriber about changes of the information of the served MCData ID, as described in subclause 22.2.2.2.5.

22.2.2.2.5 Sending notification of change of functional alias status procedure

In order to notify the subscriber about changes of functional aliases of the served MCData ID, the MCData server:

1) shall consider an MCData user information entry such that:

   a) the MCData user information entry is in the list of MCData user information entries described in subclause 22.2.2.2.2; and

   b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

   as the served MCData user information entry;

2) shall generate an application/pidf+xml MIME body indicating per-user functional alias information according to clause 22.3.1 and the served list of the MCData user information entries with the following clarifications:

   a) the MCData server shall not include information from functional alias information entry with the expiration time already expired;

   b) the MCData server shall not include information from a functional alias information entry with the functional alias status set to the "deactivated" state;

   c) if this procedures is invoked by procedure in clause 22.2.2.2.3 where the handled p-id-fa value was identified, the MCData server shall set the <p-id-fa> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id-fa value; and

3) send a SIP NOTIFY request according to 3GPP TS 24.229 [5], and IETF RFC 6665 [36] for the subscription created in clause 22.2.2.2.4. In the SIP NOTIFY request, the MCData server shall include the generated application/pidf+xml MIME body indicating per-user functional alias information.

22.2.2.2.6 Sending functional alias status change towards MCData server owning the functional alias procedure

NOTE 1: Usage of one SIP PUBLISH request to carry information about change of functional alias state of several MCData users served by the same MCData server is not supported in this version of the specification.

In order:

- to send an activation request of a served MCData ID for a handled functional alias ID;
- to send an deactivation request of a served MCData ID for a handled functional alias ID;
- to send a take over request of a served MCData ID for a handled functional alias ID due to take over; or
- to send an activation request of a served MCData ID for a handled functional alias ID due to near expiration of the previously published information;

the MCData server shall generate a SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39]. In the SIP PUBLISH request, the MCData server:

1) shall set the Request-URI to the public service identity of the controlling MCData function associated with the handled functional alias ID;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

   a) shall include the <mcdata-request-uri> element set to the handled functional alias ID; and

   b) shall include the <mcdata-calling-user-id> element set to the served MCData ID;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) if sending an activation request, shall set the Expires header field according to IETF RFC 3903 [34], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if sending an deactivation request, shall set the Expires header field according to IETF RFC 3903 [34], to zero;

6) shall include an P-Asserted-Identity header field set to the public service identity of the MCData server according to 3GPP TS 24.229 [5];

7) shall set the current p-id-fa to a globally unique value;

8) shall consider an MCData user information entry such that:

a) the MCData user information entry is in the list of MCData user information entries described in clause 22.2.2.2.2; and

b) the MCData ID of the MCData user information entry is equal to the served MCData ID;

as the served MCData user information entry;

9) for each functional alias information entry such that:

a) the functional alias information entry has the "activating" functional alias status, the functional alias ID set to the handled functional alias ID, the expiration time has not expired yet and the activating p-id-fa is not set; and

b) the functional alias information entry is in the list of the functional alias information entries of the served MCData user information entry;

shall set the activating p-id-fa of the functional alias information entry to the current p-id-fa; and

10) shall include an application/pidf+xml MIME body indicating per-functional alias status information constructed according to clause 22.3.1.2. The MCData server shall indicate all served MCData user IDs, such that:

a) the functional alias status is set to "activating" with or without "take-over" element or "activated", and the expiration time has not expired yet in a functional alias information entry with the functional alias ID set to the handled functional alias;

b) the functional alias information entry is in the list of the functional alias information entries of an MCData user information entry; and

c) the MCData user information entry is a served MCData user information entry.

The MCData server shall set the <p-id-fa> child element of the <presence> root element to the current p-id-fa.

The MCData server shall not include the "expires" attribute in the <functionalAlias> element.

The MCData server shall send the SIP PUBLISH request according to 3GPP TS 24.229 [5].

If timer F expires for the SIP PUBLISH request sent for a (de)activation request of served MCData ID for the functional alias ID or upon receiving a SIP 3xx, 4xx, 5xx or 6xx response to the SIP PUBLISH request, the MCData server:

1) shall remove each functional alias ID entry such that:

a) the functional alias information entry has the functional alias ID set to the handled functional alias ID; and

b) the functional alias information entry is in the list of the functional alias information entries of the served MCData user information entry.

22.2.2.2.7 Functional alias status determination from MCData server owning functional alias procedure

NOTE 1: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of functional alias state of several MCData users served by the same MCData server is not supported in this version of the specification.

In order to discover whether a served MCData user successfully activated a handled functional alias in the MCData server owning the functional alias, the MCData server shall generate an initial SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36].

In the SIP SUBSCRIBE request, the MCData server:

1) shall set the Request-URI to the public service identity of the controlling MCData function associated with the handled functional alias;

2) shall include an application/vnd.3gpp.mcdata-info+xml MIME body. In the application/vnd.3gpp.mcdata-info+xml MIME body, the MCData server:

a) shall include the <mcdata-request-uri> element set to the handled functional alias ID; and

b) shall include the <mcdata-calling-user-id> element set to the served MCData ID;

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) if the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

5) if the MCData server wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [36], to zero;

6) shall include an Accept header field containing the application/pidf+xml MIME type;

7) shall include an Events header field set to "presence"; and

8) shall include an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to subclause 22.3.2, indicating the served MCData ID.

In order to re-subscribe or de-subscribe, the MCData server shall generate an in-dialog SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36]. In the SIP SUBSCRIBE request, the MCData server:

1) if the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [36], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [4].

2) if the MCData server wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [36], to zero;

3) shall include an Events header field set to "presence"; and

4) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to TS 24.229 [5], IETF RFC 3856 [39], and IETF RFC 6665 [36], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-functional alias information constructed according to subclause 22.3.1, then the MCData server:

1) for each served MCData ID such that the application/pidf+xml MIME body of SIP NOTIFY request contains:

   a) a <tuple> element of the root <presence> element;

   b) the "id" attribute of the <tuple> element indicating the served MCData ID;

   c) an <functionalAlias> child element of the <status> element of the <tuple> element; and

   d) the "expires" attribute of the <functionalAlias> element indicating expiration of activation of functional alias;

   perform the following:

   a) if a functional alias information entry exists such that:

      i) the functional alias information entry has the "activating" functional alias status, the functional alias ID set to the handled functional alias ID, and the expiration time has not expired yet;

      ii) the functional alias information entry is in the list of the functional alias information entries of an MCData user information entry with the MCData ID set to the served MCData ID; and

      iii) the MCData user information entry is in the list of MCData user information entries described in clause 22.2.2.2.2;

      shall set the functional alias status of the functional alias information entry to "activated"; and

shall set the next publishing time of the functional alias information entry to the current time and half of the time between the current time and the expiration of the functional alias; and

2) for each functional alias information entry such that:

   a) the functional alias information entry has the "activated" functional alias status or the "deactivating" functional alias status, the functional alias ID set to the handled functional alias ID, and the expiration time has not expired yet;

   b) the functional alias information entry is in the list of the functional alias information entries of an MCData user information entry with the MCData ID set to a served MCData ID; and

   c) the MCData user information entry is in the list of MCData user information entries described in clause 22.2.2.2.2; and

   for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

   a) a <tuple> element of the root <presence> element;

   b) the "id" attribute of the <tuple> element indicating the served MCData ID; and

   c) an <functionalAlias> child element of the <status> child element of the <tuple> element.

   perform the following:

   a) shall set the functional alias status of the functional alias information entry to "deactivated"; and

   b) shall set the expiration time of the functional alias information entry to the current time; and

3) if a <p-id-fa> element is included in the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request, then for each functional alias information entry such that:

   a) the functional alias information entry has the "activating" functional alias status, the functional alias ID set to the handled functional alias ID, the expiration time has not expired yet and with the activating p-id-fa set to the value of the <p-id-fa> element;

   b) the functional alias information entry is in the list of the functional alias information entries of an MCData user information entry with the MCData ID set to a served MCData ID; and

   d) the MCData user information entry is in the list of MCData user information entries described in clause 22.2.2.2.2; and

   for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

   a) a <tuple> element of the root <presence> element;

   b) the "id" attribute of the <tuple> element indicating the served MCData ID; and

   c) an <functionalAlias> child element of the <status> child element of the <tuple> element;

   perform the following:

   a) shall set the functional alias status of the functional alias information entry to "deactivated"; and

   b) shall set the expiration time of the functional alias information entry to the current time.

22.2.2.3 Procedures of MCData server owning the functional alias

22.2.2.3.1 General

The procedures of MCData server owning the functional alias consist of:

- receiving functional alias status change procedure;
- receiving subscription to functional alias status procedure;

- sending notification of change of functional alias status procedure; and
- modification of functional alias eligibility check procedure.

22.2.2.3.2 Stored information

The MCData server shall maintain a list of functional alias information entries.

In each functional alias information entry, the MCData server shall maintain:

1) a functional alias ID. This field uniquely identifies the functional alias information entry in the list of the functional alias information entries; and
2) a list of MCData user information entries.

In each MCData user information entry, the MCData server shall maintain:

1) an MCData ID. This field uniquely identifies the MCData user information entry in the list of the MCData user information entries;
2) a take-over possible indication; and
3) an expiration time.

22.2.2.3.3 Receiving functional alias status change procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains the public service identity of the controlling MCData function associated with the served functional alias;
2) the SIP PUBLISH request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the <mcdata-request-uri> element and the <mcdata-calling-user-id> element;
3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];
4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and
5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-functional alias information constructed according to clause 22.2.3.2;

then the MCData server:

1) shall identify the served functional alias in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;
2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP PUBLISH request;
3) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;
4) if the functional alias does not exist in the MCData server, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

4a) if SIP PUBLISH request is for activation of a functional alias then:

   a) if handled MCPTT ID does not match with any of the entries in the <mcptt-user-list> which contains the MCPTT IDs of MCPTT users which are allowed to activate the functional alias; or
   b) if no local policy exists that authorizes the request by the handled MCPTT ID;

shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response according to 3GPP TS 24.229 [11], IETF RFC 3903 [12] and IETF RFC 3856 [13] and skip the rest of the steps;

5) if SIP PUBLISH request is for activation of a functional alias and the number of activations for the handled functional alias is equal <max-simultaneous-activations>, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

6) if SIP PUBLISH request is for take over of a functional alias, the MCData server shall use the <allow-takeover> element to determine if take over is possible. If take over is not possible, the MCData server shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

7) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34]. In the SIP 200 (OK) response, the MCData server:

   a) shall set the Expires header field according to IETF RFC 3903 [34], to the selected expiration time;

8) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served functional alias ID, shall not continue with the rest of the steps;

9) if the handled MCData ID is different from the MCData ID in the "id" attribute of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request, shall not continue with the rest of the steps;

10) shall consider a functional alias information entry such that:

   a) the functional alias information entry is in the list of functional alias information entries described in clause 22.2.2.3.2; and

   b) the functional alias ID of the functional alias information entry is equal to the served functional alias ID;

   as the served functional alias information entry;

11) if the selected expiration time is zero:

   a) shall remove the MCData user information entry such that:

      i) the MCData user information entry is in the list of the MCData user information entries of the served functional alias information entry; and

      ii) the MCData user information entry has the MCData ID set to the served MCData ID;

12) if the selected expiration time is not zero:

   a) shall consider an MCData user information entry such that:

      i) the MCData user information entry is in the list of the MCData user information entries of the served functional alias information entry; and

      ii) the MCData ID of the MCData user information entry is equal to the handled MCData ID;

      as the served MCData user information entry;

   b) if the MCData user information entry does not exist:

      i) shall insert an MCData user information entry with the MCData ID set to the handled MCData ID into the list of the MCData user information entries of the served functional alias information entry; and

      ii) shall consider the inserted MCData user information entry as the served MCData user information entry; and

      iii) shall set the expiration time according to the selected expiration time;

13) shall identify the handled p-id-fa in the <p-id-fa> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

14) shall perform the procedures specified in clause 22.2.2.3.5 for the served functional alias ID.

22.2.2.3.4 Receiving subscription to functional alias status procedure

NOTE: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of functional alias state of several MCData users served by the same MCData server is not supported in this version of the specification.

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity of the controlling MCData function associated with the served functional alias;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcdata-info+xml MIME body containing the<mcdata-request-uri> element and the <mcdata-calling-user-id> element;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in TS 24.229 [5]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type; and

5) the SIP SUBSCRIBE request contains an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to clause 22.3.2 indicating the same MCData ID as in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

then the MCData server:

1) shall identify the served functional alias ID in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

2) shall identify the handled MCData ID in the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

3) if the Expires header field of the SIP SUBSCRIBE request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP SUBSCRIBE request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

4) if a functional alias does not exist in the MCData server, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps;

5) if the handled MCData ID based on local policy is not authorized for notifications of the functional alias identified by the served functional alias ID, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 3903 [34] and IETF RFC 3856 [39] and skip the rest of the steps; and

6) shall generate a SIP 200 (OK) response to the SIP SUBSCRIBE request according to TS 24.229 [5], IETF RFC 6665 [36].

For the duration of the subscription, the MCData server shall notify subscriber about changes of the information of the served MCData ID, as described in clause 22.2.2.3.5.

22.2.2.3.5 Sending notification of change of functional alias status procedure

In order to notify the subscriber identified by the handled MCData ID about changes of the functional alias status of the served functional alias ID, the MCData server:

1) shall consider a functional alias information entry such that:

   a) the functional alias information entry is in the list of functional alias information entries described in clause 22.2.2.3.2; and

   b) the functional alias ID of the functional alias information entry is equal to the served functional alias ID;

2) shall consider an MCData user information entry such:

   a) the MCData user information entry is in the list of the MCData user information entries of the served functional alias information entry; and

   b) the MCData ID of the MCData user information entry is equal to the handled MCData ID;

   as the served MCData user information entry;

3) shall generate an application/pidf+xml MIME body indicating per-functional alias information according to clause 22.3.1 and the served list of the served MCData user information entry of the functional alias information entry with following clarifications:

   a) the MCData server shall include the "expires" attribute in the <functionalAlias> element; and

   b) if this procedures is invoked by procedure in subclause 22.2.2.3.3 where the handled p-id-fa was identified, the MCData server shall set the <p-id-fa> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id-fa value; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [5], and IETF RFC 6665 [36] for the subscription created in clause 22.2.2.3.4. In the SIP NOTIFY request, the MCData server shall include the generated application/pidf+xml MIME body indicating per-functional alias information.

22.2.2.3.6 Functional alias status automatic deactivation procedure

In order to deactivate a functional alias associated with a target MCData ID:

1) externally triggered by an MCData administrator by a mechanism outside of the scope of the standard; or

2) directly by the MCData function owning the functional alias as a result of an internal trigger like the expiration of the functional alias association;

the MCData server

1) shall consider a functional alias information entry such that:

   a) the functional alias information entry is in the list of functional alias information entries described in clause 22.2.2.3.2; and

   b) the functional alias ID of the functional alias information entry is equal to the served functional alias ID;

   as the served functional alias information entry;

2) shall remove the MCData user information entry such that:

   a) the MCData user information entry is in the list of the MCData user information entries of the served functional alias information entry; and

   b) the MCData user information entry has the MCData ID set to the target MCData ID; and

3) shall perform the procedures specified in subclause 22.2.2.3.5 for the served functional alias ID.

22.3 Coding

22.3.1 Extension of application/pidf+xml MIME type

22.3.1.1 Introduction

The clauses of the parent clause describe an extension of the application/pidf+xml MIME body specified in IETF RFC 3863 [40]. The extension is used to indicate:

- per-user functional alias information; and
- per-functional alias status information.

22.3.1.2 Syntax

The application/pidf+xml MIME body indicating per-user functional alias information is constructed according to IETF RFC 3863 [40] and:

1) contains a <presence> root element according to IETF RFC 3863 [40];
2) contains an "entity" attribute of the <presence> element set to the MCData ID of the MCData user;
3) contains one <tuple> child element according to IETF RFC 3863 [40] per <presence> element;
4) can contain a <p-id-fa> child element defined in the XML schema defined in table 22.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;
5) contains an "id" attribute of the <tuple> element set to the MCData client ID;
6) contains one <status> child element of each <tuple> element;
7) contains one <functionalAlias> child element defined in the XML schema defined in table 22.3.1.2-1, of the <status> element, for each functional alias in which the MCData user is interested;
8) contains a "functionalAliasID" attribute of each <fucntionalAlias> element set to the functional alias ID of the functional alias in which the MCData user is interested;;
9) can contain a "status" attribute of each <functionalAliasID> element indicating the activation status of functional alias for the MCData user; and
10) can contain an "expires" attribute of each <functionalAlias> element indicating expiration of activation of the functional alias for the MCData user.

The application/pidf+xml MIME body indicating per-functional alias status information is constructed according to IETF RFC 3856 [39] and:

1) contains the <presence> root element according to IETF RFC 3863 [40];
2) contains an "entity" attribute of the <presence> element set to the functional alias ID of the functional alias;
3) contains one <tuple> child element according to IETF RFC 3863 [40] of the <presence> element;
4) can contain a <p-id-fa> child element defined in the XML schema defined in table 22.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;
5) contains an "id" attribute of the <tuple> element set to the MCData ID;
6) contains one <status> child element of each <tuple> element;
7) contains one <functionalAlias> child element defined in the XML schema defined in table 22.3.1.2-1, of the <status> element, for each MCData ID for which functional alias information is provided;
8) contains one "user" attribute defined in the XML schema defined in table 22.3.1.2-2, of the <functionalAlias> element set to the MCData client ID; and
9) can contain an "expires" attribute defined in the XML schema defined in table 22.3.1.2-2, of the <functionalAlias> element indicating expiration of activation of the functional alias for the MCData user.

Table 22.3.1.2-1: XML schema with elements and attributes extending the application/pidf+xml MIME body

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:mcdataPresInfoFA:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:mcdataPIFA10="urn:3gpp:ns:mcdataPresInfoFA:1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- MCData functional alias specific child elements of tuple element -->
  <xs:element name="functionalAlias" type="mcdataPIFA10:functionalAliasType"/>
  <xs:complexType name="functionalAliasType">
```

```
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="functionalAliasID" type="xs:anyURI" use="optional"/>
    <xs:attribute name="user" type="xs:anyURI" use="optional"/>
    <xs:attribute name="status" type="mcdataPIFA10:statusType" use="optional"/>
    <xs:attribute name="expires" type="xs:dateTime" use="optional"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="statusType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="activating"/>
      <xs:enumeration value="activated"/>
      <xs:enumeration value="deactivating"/>
      <xs:enumeration value="take-over-possible"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="p-id-fa" type="xs:string"/>

  <xs:element name="take-over" type="xs:boolean"/>

  </xs:schema>
```

The application/pidf+xml MIME body refers to namespaces using prefixes specified in table 22.3.1.2-2.

Table 22.3.1.2-2: Assignment of prefixes to namespace names in the application/pidf+xml MIME body

Prefix	Namespace
mcdataPIFA10	urn:3gpp:ns:mcdataPresInfoFA:1.0
NOTE: The "urn:ietf:params:xml:ns:pidf" namespace is the default namespace so no prefix is used for it in the application/pidf+xml MIME body.	

22.3.2 Extension of application/simple-filter+xml MIME type

22.3.2.1 Introduction

The subclauses of the parent clause describe an extension of the application/simple-filter+xml MIME body specified in IETF RFC 4661 [41].

The extension is used to indicate per-user restrictions of presence event package notification information for functional alias information.

22.3.2.2 Syntax

The application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information is constructed according to IETF RFC 4661 [41] and:

1) contains a <filter-set> root element according to IETF RFC 4661 [41];

2) contains an <ns-bindings> child element according to IETF RFC 4661 [41], of the <filter-set> element;

3) contains an <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [41] set to "pidf"; and

   B) contains a "urn" attribute set to the "urn:ietf:params:xml:ns:pidf" value;

4) contains a <ns-binding> child element according to IETF RFC 4661 [41], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [41], set to "mcdataPIFA10"; and

   B) contains an "urn" attribute according to IETF RFC 4661 [41], set to the "urn:3gpp:ns:mcdataPresInfoFA:1.0" value;

5) contains a <filter> child element according to IETF RFC 4661 [41], of the <filter-set> element where the <filter> element;

   A) contains an "id" attribute set to a value constructed according to IETF RFC 4661 [41];

   B) does not contain a "uri" attribute of the <filter> child element according to IETF RFC 4661 [41]; and

   C) does not contain a "domain" attribute according to IETF RFC 4661 [41];

6) contains a <what> child element according to IETF RFC 4661 [41], of the <filter> element; and

7) contains an <include> child element according to IETF RFC 4661 [41], of the <what> element where the <include> element;

   A) does not contain a "type" attribute according to IETF RFC 4661 [41]; and

   B) contains the value, according to IETF RFC 4661 [41], set to concatenation of the '//pidf:presence/pidf:tuple[@id="' string, the MCData ID, and the '"]' string.

Annex A (informative): Signalling flows

Annex B (normative): Media feature tags within the current document

B.1 General

This subclause describes the media feature tag definitions that are applicable for the 3GPP IM CN Subsystem for the realisation of the Mission Critical Data (MCData) service.

B.2 Definition of media feature tag for Mission Critical Data (MCData) communications Short Data Service (SDS)

Media feature tag name: g.3gpp.mcdata.sds

ASN.1 Identifier: 1.3.6.1.8.2.29

Summary of the media feature indicated by this media feature tag: This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Data (MCData) communications Short Data Service (SDS).

Values appropriate for use with this media feature tag: Boolean

The media feature tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This media feature tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Indicating that a mobile phone supports the Mission Critical Data (MCData) communications Short Data Service (SDS).

Related standards or documents: 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control Protocol specification"

Security Considerations: Security considerations for this media feature tag are discussed in subclause 11.1 of IETF RFC 3840 [16].

B.3 Definition of media feature tag for Mission Critical Data (MCData) communications File Distribution (FD)

Media feature tag name: g.3gpp.mcdata.fd

ASN.1 Identifier: 1.3.6.1.8.2.30

Summary of the media feature indicated by this media feature tag: This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Data (MCData) communications File Distribution (FD).

Values appropriate for use with this media feature tag: Boolean

The media feature tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This media feature tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Indicating that a mobile phone supports the Mission Critical Data (MCData) communications File Distribution (FD).

Related standards or documents: 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control Protocol specification"

Security Considerations: Security considerations for this media feature tag are discussed in subclause 11.1 of IETF RFC 3840 [16].

Annex C (normative): ICSI values defined within the current document

C.1 General

This subclause describes the IMS Communications Service Identifier (ICSI) definitions that are applicable for the 3GPP IM CN Subsystem for the realisation of the Mission Critical Data (MCData) service.

NOTE: The template has been created using the headers of the table in http://www.3gpp.org/specifications-groups/34-uniform-resource-name-urn-list

C.2 Definition of ICSI value for the Mission Critical Data (MCData) service

C.2.1 URN

urn:urn-7:3gpp-service.ims.icsi.mcdata

C.2.2 Description

This URN indicates that the device has the capabilities to support the Mission Critical Data (MCData) service. This URN is also used by the device to associate a SIP request with the Mission Critical Data (MCData) service.

C.2.3 Reference

3GPP TS 24.282: "Mission Critical Data (MCData) signalling control Protocol specification".

C.2.4 Contact

Name: Ricky Kaura

Email: ricky.kaura@samsung.com

C.2.5 Registration of subtype

Yes

C.2.6 Remarks

This URN is included in the "g.3gpp.icsi-ref" media feature tag in the Contact header field of SIP requests (not SIP MESSAGE) and responses, and the Accept-Contact header fields of non-register SIP requests.

This URN can be included by the device in the P-Preferred-Service header field of SIP requests, and is asserted by the network into the P-Asserted-Service header field of SIP Requests.

C.3 Definition of ICSI value for the Mission Critical Data (MCData) communications Short Data Service (SDS)

C.3.1 URN

urn:urn-7:3gpp-service.ims.icsi.mcdata.sds

C.3.2 Description

This URN indicates that the device has the capabilities to support the Mission Critical Data (MCData) Short Data Service (SDS) IMS communication service. This URN is also used by the device to associate a SIP request with the Mission Critical Data (MCData) Short Data Service (SDS) IMS communication service.

C.3.3 Reference

3GPP TS 24.282: "Mission Critical Data (MCData) signalling control Protocol specification".

C.3.4 Contact

Name: Ricky Kaura

Email: ricky.kaura@samsung.com

C.3.5 Registration of subtype

Yes

C.3.6 Remarks

This URN is included in the "g.3gpp.icsi-ref" media feature tag in the Contact header field of SIP requests (not SIP MESSAGE) and responses, and the Accept-Contact header fields of non-register SIP requests.

This URN can be included by the device in the P-Preferred-Service header field of SIP requests, and is asserted by the network into the P-Asserted-Service header field of SIP Requests.

C.4 Definition of ICSI value for Mission Critical Data (MCData) communications File Distribution (FD)

C.4.1 URN

urn:urn-7:3gpp-service.ims.icsi.mcdata.fd

C.4.2 Description

This URN indicates that the device has the capabilities to support the Mission Critical Data (MCData) File Distribution (FD) IMS communication service. This URN is also used by the device to associate a SIP request with the Mission Critical Data (MCData) File Distribution (FD) IMS communication service.

C.4.3 Reference

3GPP TS 24.282: "Mission Critical Data (MCData) signalling control Protocol specification".

C.4.4 Contact

Name: Ricky Kaura

Email: ricky.kaura@samsung.com

C.4.5 Registration of subtype

Yes

C.4.6 Remarks

This URN is included in the "g.3gpp.icsi-ref" media feature tag in the Contact header field of SIP requests (not SIP MESSAGE) and responses, and the Accept-Contact header fields of non-register SIP requests.

This URN can be included by the device in the P-Preferred-Service header field of SIP requests, and is asserted by the network into the P-Asserted-Service header field of SIP Requests.

Annex D (normative): XML schemas

D.1 XML schema for transporting MCData identities and general services information

D.1.1 General

This subclause defines XML schema and MIME type for transporting MCData identities and general services information.

D.1.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:ns:mcdataInfo:1.0"
  xmlns:mcdatainfo="urn:3gpp:ns:mcdataInfo:1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

  <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/
schemaLocation="http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd">

  <!-- root XML element -->
  <xs:element name="mcdatainfo" type="mcdatainfo:mcdatainfo-Type" id="info"/>

  <xs:complexType name="mcdatainfo-Type">
    <xs:sequence>
      <xs:element name="mcdata-Params" type="mcdatainfo:mcdata-ParamsType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="mcdata-ParamsType">
    <xs:sequence>
      <xs:element name="mcdata-access-token" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="request-type" type="xs:string" minOccurs="0"/>
      <xs:element name="mcdata-request-uri" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="mcdata-calling-user-id" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="mcdata-called-party-id" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="mcdata-calling-group-id" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="alert-ind" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="originated-by" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="mcdata-client-id" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:element name="mcdata-controller-psi" type="mcdatainfo:contentType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="protectionType">
    <xs:restriction base="xs:string">
       <xs:enumeration value="Normal"/>
       <xs:enumeration value="Encrypted"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="contentType">
    <xs:choice>
      <xs:element name="mcdataURI" type="xs:anyURI"/>
      <xs:element name="mcdataString" type="xs:string"/>
      <xs:element name="mcdataBoolean" type="xs:boolean"/>
```

```
      <xs:any namespace="##other" processContents="lax"/>
      <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>
    </xs:choice>
    <xs:attribute name="type" type="mcdatainfo:protectionType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

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

</xs:schema>
```

D.1.3 Semantic

Editor's note: In the current release, support for emergency groups and emergency group communications (in particular the use of the <emergency-ind> element) may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

The <mcdatainfo> element is the root element of the XML document. The <mcdatainfo> element can contain subelements.

NOTE 1: The subelements of the <mcdata-info> are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <mcdata-info> element

If the <mcdatainfo> contains the <mcdata-Params> element then:

1) the <mcdata-access-token>, <mcdata-request-uri>, <mcdata-controller-psi>, <mcdata-calling-user-id>, <mcdata-called-party-id>, <mcdata-calling-group-id>, <alert-ind>, <originated-by> and <mcdata-client-id> can be included with encrypted content;

2) for each element in 1) that is included with content that is not encrypted:

   a) the element has the "type" attribute set to "Normal";

   b) if the element is the <mcdata-request-uri>, <mcdata-calling-user-id>, <mcdata-called-party-id> or <mcdata-calling-group-id> or <originated-by> then the <mcdataURI> element is included;

   c) if the element is the <mcdata-access-token> or <mcdata-client-id>, then the <mcdataString> element is included; and

   d) if the element is <alert-ind> then the <mcdataBoolean> element is included;

3) for each element in 1) that is included with content that is encrypted:

   a) the element has the "type" attribute set to "Encrypted";

   b) the <xenc:EncryptedData> element from the "http://www.w3.org/2001/04/xmlenc#" namespace is included and:

      i) can have a "Type" attribute can be included with a value of "http://www.w3.org/2001/04/xmlenc#Content";

      ii) can include an <EncryptionMethod> element with the "Algorithm" attribute set to value of "http://www.w3.org/2009/xmlenc11#aes128-gcm";

      iii) can include a <KeyInfo> element with a <KeyName> element containing the base 64 encoded XPK-ID; and

      iv) includes a <CipherData> element with a <CipherValue> element containing the encrypted data.

NOTE 2: When the optional attributes and elements are not included within the <xenc:EncryptedData> element, the information they contain is known to sender and the receiver by other means.

If the <mcdatainfo> contains the <mcdata-Params> element then:

1) the <mcdata-access-token> can be included with the access token received during authentication procedure as described in 3GPP TS 24.382 [49];

2) the <request-type> can be included with:

   a) a value of "one-to-one-sds" to indicate that the MCData client wants to initiate a one-to-one SDS request;

   b) a value of "group-sds" to indicate the MCData client wants to initiate a group SDS request;

   c) a value of "one-to-one-fd" to indicate that the MCData client wants to initiate a one-to-one FD request;

   d) a value of "group-fd" to indicate that the MCData client wants to initiate a group FD request;

   e) a value of "msf-disc-req" to indicate that the MCData client wishes to discover the absoluteURI of the media storage function for HTTP requests;

   f) a value of "msf-disc-res" when the participating MCData function sends the absolute URI to the MCData client;

   g) a value of "notify" when the controlling MCData function needs to send a notification to the MCData client;

   h) a value of "one-to-one-sds-session" to indicate that the MCData client wants to initiate a one-to-one SDS session; and

   i) a value of "group-sds-session" to indicate the MCData client wants to initiate a group SDS session.

3) the <mcdata-request-uri> can be included with an MCData group ID;

4) the <mcdata-calling-user-id> can be included, set to MCData ID of the originating user;

5) the <mcdata-called-party-id> can be included, set to the MCData ID of the terminating user;

6) the <mcdata-calling-group-id> can be included to indicate the MCData group identity to the terminating user;

7) the <alert-ind> can be:

   a) set to "true" to indicate that an alert to be sent; or

   b) set to "false" to indicate that an alert to is be cancelled;

8) the <originated-by> can be included, set to the MCData ID of the originating user of an MCData emergency alert when being cancelled by another authorised MCDATA user;

9) the <mcdata-client-id>: can be included, set to the MCData client ID of the MCData client that originated a SIP INVITE request, SIP REFER request or SIP MESSAGE request; and

10) the <mcdata-controller-psi> can be included, set to the PSI of the controlling MCData function that handled the one-to-one or group MCData data request; and

11) the <anyExt> can be included with the following elements not declared in the XML schema:

   a) a <pre-established-session-ind> of type "xs:Boolean":

      i) set to a value of "true" by MCData client in pre-established session setup request to indicate MCData participating function about initiation of pre-established session.

   b) a <mcdata-communication-state> of type "xs:string" can be included to indicate state of MCData communication within pre-established session. The <mcdata-communication-state> can be set to:

      i) a value of "establish-request" by MCData participating function to indicate to the MCData client about MCData communication establishement request within pre-established session;

      ii) a value of "establish-success" by MCData participating function or MCData client to indicate that the MCData communication is established successfully;

      iii) a value of "establish-fail" by MCData participating function or MCData client to indicate that the MCData communication establishement is failed or rejected;

iv) a value of "terminate-request" by MCData participating function to indicate to the MCData client about MCData communication termination request within pre-established session; and

v) a value of "terminated" by MCData participating function or MCData client to indicate MCData communication is terminated.

c) an <emergency-ind> of type "xs:Boolean" can be included and set to:

i) "true" to indicate that the communication that the MCData client is initiating is an emergency MCData communication; or

ii) "false" to indicate that the MCData client is cancelling an emergency MCData communication (i.e. converting it back to a non-emergency communication);

d) an <alert-ind-rcvd> of type "xs:Boolean":

i) may be set to “true” and included in a SIP MESSAGE to indicate that the emergency alert or cancellation was received successfully;

e) an <mc-org> of type “xs:string” may be:

i) set to the MCData user's Mission Critical Organization and included in an emergency alert sent by the MCData server to terminating MCData clients;

The recipient of the XML ignores any unknown element and any unknown attribute.

D.1.4 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcdata-info+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. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

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

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

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 24.282 "Mission Critical Data (MCData) signalling control;Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications Usage:

Applications supporting the mission critical data communications procedures 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>

D.2 Void

D.3 XML schema for MCData (de)-affiliation requests

D.3.1 General

This subclause defines XML schema and MIME type for MCData (de)-affiliation requests.

D.3.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:3gpp:ns:affiliationCommand:1.0"
xmlns:mcdataaff="urn:3gpp:ns:affiliationCommand:1.0"
attributeFormDefault="unqualified" elementFormDefault="qualified">
  <xs:complexType name="affiliate-command" id="affil">
    <xs:sequence>
      <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcdataaff:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>
  <xs:complexType name="de-affiliate-command">
    <xs:sequence>
      <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcdataaff:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>
  <xs:element name="command-list">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="affiliate" type="mcdataaff:affiliate-command" minOccurs="0"
maxOccurs="1"/>
        <xs:element name="de-affiliate" type="mcdataaff:de-affiliate-command" minOccurs="0"
maxOccurs="1"/>
        <xs:element name="anyExt" type="mcdataaff:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

D.3.3 Semantic

The <command-list> element is the root element of the XML document. The <command-list> element may contain <affiliate-command>, or <de-affiliate-command> subelements or both.

If the <command-list> contains the <affiliate-command> element then:

1) the <affiliate-command> element contains a list of <group> subelements having at least one subelement. The recipient shall perform an affiliation for all the MCData groups contained in the list for the clients for which the <command-list> applies.

If the <command-list> contains the <de-affiliate-command> element then:

1) the <de-affiliate-command> element contains a list of <group> subelements having at least one subelement. The recipient shall perform a de-affiliation for all the MCData groups contained in the list for the clients for which the <command-list> applies.

The recipient of the XML ignores any unknown element and any unknown attribute.

D.3.4 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcdata-affiliation-command+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. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

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

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

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 24.282 "Mission Critical Data (MCData) signalling control" version 14.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical data functions 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>

D.4 XML schema for MCData location information

D.4.1 General

This subclause defines the XML schema and the MIME type for location information.

D.4.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:mcdataloc="urn:3gpp:ns:mcdataLocationInfo:1.0"
targetNamespace="urn:3gpp:ns:mcdataLocationInfo:1.0" elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

    <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/>

    <xs:element name="location-info" id="loc">
        <xs:annotation>
            <xs:documentation>Root element, contains all information related to location
configuration, location request and location reporting for the MCData service</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:choice>
                <xs:element name="Configuration" type="mcdataloc:tConfigurationType"/>
                <xs:element name="Request" type="mcdataloc:tRequestType"/>
```

```
                <xs:element name="Report" type="mcdataloc:tReportType"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
            </xs:choice>
            <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tConfigurationType">
        <xs:sequence>
            <xs:element name="NonEmergencyLocationInformation"
type="mcdataloc:tRequestedLocationType" minOccurs="0"/>
            <xs:element name="EmergencyLocationInformation" type="mcdataloc:tRequestedLocationType"
minOccurs="0"/>
            <xs:element name="TriggeringCriteria" type="mcdataloc:TriggeringCriteriaType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="ConfigScope">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Full"/>
                    <xs:enumeration value="Update"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestType">
        <xs:complexContent>
            <xs:extension base="mcdataloc:tEmptyType">
                <xs:attribute name="RequestId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="tReportType">
        <xs:sequence>
            <xs:element name="TriggerId" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="CurrentLocation" type="mcdataloc:tCurrentLocationType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="ReportID" type="xs:string" use="optional"/>
        <xs:attribute name="ReportType" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Emergency"/>
                    <xs:enumeration value="NonEmergency"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="TriggeringCriteriaType">
        <xs:sequence>
            <xs:element name="CellChange" type="mcdataloc:tCellChange" minOccurs="0"/>
            <xs:element name="TrackingAreaChange" type="mcdataloc:tTrackingAreaChangeType"
minOccurs="0"/>
            <xs:element name="PlmnChange" type="mcdataloc:tPlmnChangeType" minOccurs="0"/>
            <xs:element name="MbmsSaChange" type="mcdataloc:tMbmsSaChangeType" minOccurs="0"/>
            <xs:element name="MbsfnAreaChange" type="mcdataloc:tMbsfnAreaChangeType" minOccurs="0"/>
            <xs:element name="PeriodicReport" type="mcdataloc:tIntegerAttributeType" minOccurs="0"/>
            <xs:element name="TravelledDistance" type="mcdataloc:tIntegerAttributeType"
minOccurs="0"/>
            <xs:element name="McdataSignallingEvent" type="mcdataloc:tSignallingEventType"
minOccurs="0"/>
            <xs:element name="GeographicalAreaChange" type="mcdataloc:tGeographicalAreaChange"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tCellChange">
        <xs:sequence>
            <xs:element name="AnyCellChange" type="mcdataloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificCell" type="mcdataloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
```

```
            <xs:element name="ExitSpecificCell" type="mcdataloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmptyType"/>
    <xs:simpleType name="tEcgi">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}[0-1]{28}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tSpecificCellType">
        <xs:simpleContent>
            <xs:extension base="mcdataloc:tEcgi">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tEmptyTypeAttribute">
        <xs:complexContent>
            <xs:extension base="mcdataloc:tEmptyType">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="tTrackingAreaChangeType">
        <xs:sequence>
            <xs:element name="AnyTrackingAreaChange" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="EnterSpecificTrackingArea" type="mcdataloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificTrackingArea" type="mcdataloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tTrackingAreaIdentityFormat">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}[0-1]{16}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tTrackingAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcdataloc:tTrackingAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tPlmnChangeType">
        <xs:sequence>
            <xs:element name="AnyPlmnChange" type="mcdataloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificPlmn" type="mcdataloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificPlmn" type="mcdataloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tPlmnIdentityFormat">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tPlmnIdentity">
        <xs:simpleContent>
            <xs:extension base="mcdataloc:tPlmnIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbmsSaChangeType">
        <xs:sequence>
```

```
            <xs:element name="AnyMbmsSaChange" type="mcdataloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificMbmsSa" type="mcdataloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="ExitSpecificMbmsSa" type="mcdataloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbmsSaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="65535"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbmsSaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcdataloc:tMbmsSaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbsfnAreaChangeType">
        <xs:sequence>
            <xs:element name="EnterSpecificMbsfnArea" type="mcdataloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:element name="ExitSpecificMbsfnArea" type="mcdataloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbsfnAreaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="255"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbsfnAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcdataloc:tMbsfnAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tIntegerAttributeType">
        <xs:simpleContent>
            <xs:extension base="xs:integer">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tTravelledDistanceType">
        <xs:sequence>
            <xs:element name="TravelledDistance" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSignallingEventType">
        <xs:sequence>
            <xs:element name="InitialLogOn" type="mcdataloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="GroupCallNonEmergency" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallNonEmergency" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="LocationConfigurationReceived" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmergencyEventType">
        <xs:sequence>
            <xs:element name="GroupCallEmergency" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
```

```
            <xs:element name="GroupCallImminentPeril" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallEmergency" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="InitiateEmergencyAlert" type="mcdataloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestedLocationType">
        <xs:sequence>
            <xs:element name="ServingEcgi" type="mcdataloc:tEmptyType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcdataloc:tEmptyType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcdataloc:tEmptyType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcdataloc:tEmptyType" minOccurs="0"/>
            <xs:element name="GeographicalCoordinate" type="mcdataloc:tEmptyType" minOccurs="0"/>
            <xs:element name="minimumIntervalLength" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCurrentLocationType">
        <xs:sequence>
            <xs:element name="CurrentServingEcgi" type="mcdataloc:tLocationType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcdataloc:tLocationType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcdataloc:tLocationType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcdataloc:tLocationType" minOccurs="0"/>
            <xs:element name="CurrentCoordinate" type="mcdataloc:tPointCoordinate" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="protectionType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Normal"/>
            <xs:enumeration value="Encrypted"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="tLocationType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="Ecgi" type="mcdataloc:tEcgi" minOccurs="0"/>
            <xs:element name="SaId" type="mcdataloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="MbsfnAreaId" type="mcdataloc:tMbsfnAreaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="mcdataloc:protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tGeographicalAreaChange">
        <xs:sequence>
            <xs:element name="AnyAreaChange" type="mcdataloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificAreaType" type="mcdataloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:element name="ExitSpecificAreaType" type="mcdataloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSpecificAreaType">
        <xs:sequence>
            <xs:element name="GeographicalArea" type="mcdataloc:tGeographicalAreaDef"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="TriggerId" type="xs:string" use="required"/>
```

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

    <xs:complexType name="tPointCoordinate">
        <xs:sequence>
            <xs:element name="longitude" type="mcdataloc:tCoordinateType"/>
            <xs:element name="latitude" type="mcdataloc:tCoordinateType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCoordinateType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="threebytes" type="mcdataloc:tThreeByteType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="mcdataloc:protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="tThreeByteType">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="16777215"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tGeographicalAreaDef">
        <xs:sequence>
            <xs:element name="PolygonArea" type="mcdataloc:tPolygonAreaType" minOccurs="0"/>
            <xs:element name="EllipsoidArcArea" type="mcdataloc:tEllipsoidArcType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tPolygonAreaType">
        <xs:sequence>
            <xs:element name="Corner" type="mcdataloc:tPointCoordinate" minOccurs="3"
maxOccurs="15"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEllipsoidArcType">
        <xs:sequence>
            <xs:element name="Center" type="mcdataloc:tPointCoordinate"/>
            <xs:element name="Radius" type="xs:nonNegativeInteger"/>
            <xs:element name="OffsetAngle" type="xs:unsignedByte"/>
            <xs:element name="IncludedAngle" type="xs:unsignedByte"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdataloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="anyExtType">
        <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

D.4.3 Semantic

The <location-info> element is the root element of the XML document. The <location-info> element contains the <Configuration>, <Request> and <Report> subelements, of which only one can be present.

<Configuration> element has a <ConfigScope> attribute that can assume the values "Full" and "Update". The value "Full" means that the Configuration> element contains the full location configuration which replaces any previous location configuration. The value "Update" means that the location configuration is in addition to any previous location configuration. To remove configuration elements a "Full" configuration is needed. The <Configuration> element contains the following child elements:

1) <NonEmergencyLocationInformation>, an optional element that specifies the location information requested in non-emergency situations. The <NonEmergencyLocationInformation> has the subelements:

   a) <ServingEcgi>, an optional element specifying that the serving E-UTRAN Cell Global Identity (ECGI) needs to be reported;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported;

   c) <MbmsSaId>, an optional element specifying that the serving MBMS Service Area Id needs to be reported;

   d) <MbsfnArea>, an optional element specifying that the MBSFN area Id needs to be reported;

   e) <GeographicalCoordinate>, an optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [47] needs to be reported; and

   f) <minimumIntervalLength>, a mandatory element specifying the minimum time the MCData client needs to wait between sending location reports. The value is given in seconds;

2) <EmergencyLocationInformation>, an optional element that specifies the location information requested in emergency situations. The <EmergencyLocationInformation> has the subelements:

   a) <ServingEcgi>, an optional element specifying that the serving ECGI needs to be reported;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported;

   c) <MbmsSaId>, an optional element specifying that the serving MBMS Service Area Id needs to be reported;

   d) <MbsfnArea>, an optional element specifying that the MBSFN area Id needs to be reported;

   e) <GeographicalCoordinate>, an optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [47] needs to be reported; and

   f) <minimumIntervalLength>, a mandatory element specifying the minimum time the MCData client needs to wait between sending location reports. The value is given in seconds; and

3) <TriggeringCriteria>, a mandatory element specifying the triggers for the MCData client to perform reporting in non emergency status. The <TriggeringCriteria> element contains the following sub-elements:

   a) <CellChange>, an optional element specifying what cell changes trigger location reporting. Consists of the following sub-elements:

      I) <AnyCellChange>, an optional element. The presence of this element specifies that any cell change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

      II) <EnterSpecificCell>, an optional element specifying an ECGI which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

      III) <ExitSpecificCell>, an optional element specifying an ECGI which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   b) <TrackingAreaChange>, an optional element specifying what tracking area changes trigger location reporting. Consists of the following sub-elements:

      I) <AnyTrackingAreaChange>, an optional element. The presence of this element specifies that any tracking area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

      II) <EnterSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

      III) <ExitSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

c) <PlmnChange>, an optional element specifying what PLMN changes trigger location reporting. Consists of the following sub-elements:

   I) <AnyPlmnChange>, an optional element. The presence of this element specifies that any PLMN change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   II) <EnterSpecificPlmn>, an optional element specifying a PLMN Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

   III) <ExitSpecificPlmn>, an optional element specifying a PLMN Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

d) <MbmsSaChange>, an optional element specifying what MBMS changes trigger location reporting. Consists of the following sub-elements:

   I) <AnyMbmsSaChange>, an optional element. The presence of this element specifies that any MBMS SA change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   II) <EnterSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

   III) <ExitSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

e) <MbsfnAreaChange>, an optional element specifying what MBSFN changes trigger location reporting. Consists of the following sub-elements:

   I) <AnyMbsfnAreaChange>, an optional element. The presence of this element specifies that any MBSFN area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   II) <EnterSpecificMbsfnArea>, an optional element specifying an MBSFN area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

   III) <ExitSpecificMbsfnArea>, an optional element specifying an MBSFN area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

f) <PeriodicReport>, an optional element specifying that periodic location reports shall be sent. The value in seconds specifies the reporting interval. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

g) <TravelledDistance>, an optional element specifying that the travelled distance shall trigger a report. The value in metres specified the travelled distance. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

h) <McdataSignallingEvent>, an optional element specifying what signalling events triggers a location report. The <McdataSignallingEvent> element has the following sub-elements:

   I) <InitialLogOn>, an optional element specifying that an initial log on triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   II) <GroupCallNonEmergency>, an optional element specifying that a non-emergency group call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

   III) <PrivateCallNonEmergency>, an optional element specifying that a non-emergency private call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

   IV) <LocationConfigurationReceived>, an optional element specifying that a received location configuration triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

i) <GeographicalAreaChange>, an optional element specifying what geographical are changes trigger location reporting. Consists of the following sub-elements:

   I) <AnyAreaChange>, an optional element. The presence of this element specifies that any geographical area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificArea>, an optional element specifying a geographical area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string. The <EnterSpecificArea> element has the following sub-elements:

A) <GeographicalArea>, an optional element containing a <TriggerId> attribute and the following two subelements:

x1) <PolygonArea>, an optional element specifying the area as a polygon specified in subclause 5.2 in 3GPP TS 23.032 [47]; and

x2) <EllipsoidArcArea>, an optional element specifying the area as an Ellipsoid Arc specified in subclause 5.7 in 3GPP TS 23.032 [47]; and

III) <ExitSpecificAreaType>, an optional element specifying a geographical area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string.

4) the <anyExt> shall be included with the following element not declared in the XML schema:

a) <EmergencyTriggeringCriteria>, a mandatory element specifying the triggers for the MCData client to perform reporting in emergency status. The <TriggeringCriteria> element contains the following sub-elements:

I) <CellChange>, an optional element specifying what cell changes trigger location reporting. Consists of the following sub-elements:

A) <AnyCellChange>, an optional element. The presence of this element specifies that any cell change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificCell>, an optional element specifying an ECGI which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

C) <ExitSpecificCell>, an optional element specifying an ECGI which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <TrackingAreaChange>, an optional element specifying what tracking area changes trigger location reporting. Consists of the following sub-elements:

A) <AnyTrackingAreaChange>, an optional element. The presence of this element specifies that any tracking area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

C) <ExitSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

III) <PlmnChange>, an optional element specifying what PLMN changes trigger location reporting. Consists of the following sub-elements:

A) <AnyPlmnChange>, an optional element. The presence of this element specifies that any PLMN change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificPlmn>, an optional element specifying a PLMN Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

C) <ExitSpecificPlmn>, an optional element specifying a PLMN Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

IV) <MbmsSaChange>, an optional element specifying what MBMS changes trigger location reporting. Consists of the following sub-elements:

A) <AnyMbmsSaChange>, an optional element. The presence of this element specifies that any MBMS SA change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

C <ExitSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

V) <MbsfnAreaChange>, an optional element specifying what MBSFN changes trigger location reporting. Consists of the following sub-elements:

A) <AnyMbsfnAreaChange>, an optional element. The presence of this element specifies that any MBSFN area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificMbsfnArea>, an optional element specifying an MBSFN area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

C) <ExitSpecificMbsfnArea>, an optional element specifying an MBSFN area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

VI)<PeriodicReport>, an optional element specifying that periodic location reports shall be sent. The value in seconds specifies the reporting interval. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

VII) <TravelledDistance>, an optional element specifying that the travelled distance shall trigger a report. The value in metres specified the travelled distance. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

VIII) <McdataSignallingEvent>, an optional element specifying what signalling events triggers a location report. The <McdataSignallingEvent> element has the following sub-elements:

A) <InitialLogOn>, an optional element specifying that an initial log on triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <GroupCallNonEmergency>, an optional element specifying that a non-emergency group call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

C) <PrivateCallNonEmergency>, an optional element specifying that a non-emergency private call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

D) <LocationConfigurationReceived>, an optional element specifying that a received location configuration triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

IX)<GeographicalAreaChange>, an optional element specifying what geographical are changes trigger location reporting. Consists of the following sub-elements:

A) <AnyAreaChange>, an optional element. The presence of this element specifies that any geographical area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

B) <EnterSpecificArea>, an optional element specifying a geographical area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string. The <EnterSpecificArea> element has the following sub-elements:

x1)<GeographicalArea>, an optional element containing a <TriggerId> attribute and the following two subelements:

i1) <PolygonArea>, an optional element specifying the area as a polygon specified in subclause 5.2 in 3GPP TS 23.032 [47]; and

i2) <EllipsoidArcArea>, an optional element specifying the area as an Ellipsoid Arc specified in subclause 5.7 in 3GPP TS 23.032 [47]; and

C) <ExitSpecificAreaType>, an optional element specifying a geographical area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string.

<Request> is an element with a <RequestId> attribute. The <Request> element is used to request a location report. The value of the <RequestId> attribute is returned in the corresponding <ReportId> attribute in order to correlate the request and the report.

<Report> is an element used to include the location report. It contains a <ReportId> attribute and a <ReportType> attribute. The <ReportId> attribute is used to return the value in the <RequestId> attribute in the <Request> element. The <ReportType> attribute has two values "Emergency" and "NonEmergency" used to inform whether the client is sending the report in an emergency situation or not. The <Report> element contains the following sub-elements:

1) <TriggerId>, an optional element which can occur multiple times that contain the value of the <TriggerId> attribute associated with a trigger that has fired; and

2) <CurrentLocation>, a mandatory element that contains the location information. The <CurrentLocation> element contains the following sub-elements:

   a) <CurrentServingEcgi>, an optional element containing the ECGI of the serving cell;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times. It contains the ECGI of any neighbouring cell the MCData client can detect;

   c) <MbmsSaId>, an optional element containing the MBMS Service Area Id the MCData client is using;

   d) <MbsfnArea>, an optional element containing the MBSFN area the MCData is located in; and

   e) <CurrentCoordinate>, an optional element containing the longitude and latitude coded as in subclause 6.1 in 3GPP TS 23.032 [47].

The contents of the subelements in the <CurrentLocation> subelement of the <Report> element can be encrypted. The following rules are applied when any of these elements are included:

1) if confidentiality protection is not required, then:

   a) the "type" attributes associated with the <CurrentServingEcgi>, <NeighbouringEcgi>, <MbmsSaId>, and <MbsfnArea> elements of the <Report> element have the value "Normal" and

      ii) the <Ecgi> subelement of the <CurrentServingEcgi> element contains the unencrypted value of the ECGI of the serving cell;

      iii) the <Ecgi> subelement of the <NeighbouringEcgi> element contains the unencrypted value of the ECGI of any neighbouring cell;

      iv) the <SaId> subelement of the <MbmsSaId> element contains the unencrypted value of the MBMS Service Area Id the MCData client is using; and

      v) the <MbsfnAreaId> subelement of the <MbsfnArea>, element contains the unencrypted value of the MBSFN area the MCData is located in;

   b) the "type" attributes associated with the <longitude> and <latitude> subelements of the <CurrentCoordinate> element have the value "Normal" and the <three-bytes> subelements of <longitude> and <latitude> subelements contain the unencrypted value of longitude and latitude.

2) if confidentiality protection is required, then:

   a) the "type" attributes associated with the <CurrentServingEcgi>, <NeighbouringEcgi>, <MbmsSaId>, and <MbsfnArea> elements have the value "Encrypted";

   b) the "type" attributes associated with the <longitude> and <latitude> subelements of the <CurrentCoordinate> element have the value "Encrypted";

c) for each of the elements described in 2a) and subelements described in 2b) above, the <xenc:EncryptedData> element from the "http://www.w3.org/2001/04/xmlenc#" namespace is included and:

i) can have a "Type" attribute can be included with a value of "http://www.w3.org/2001/04/xmlenc#Content";

ii) can include an <EncryptionMethod> element with the "Algorithm" attribute set to value of "http://www.w3.org/2009/xmlenc11#aes128-gcm";

iii) can include a <KeyInfo> element with a <KeyName> element containing the base 64 encoded XPK-ID; and

iv) includes a <CipherData> element with a <CipherValue> element containing the encrypted data.

NOTE: When the optional attributes and elements are not included within the <xenc:EncryptedData> element, the information they contain is known to sender and the receiver by other means.

The recipient of the XML ignores any unknown element and any unknown attribute.

D.4.4 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp. mcdata-location-info+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. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

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

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

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 24.282 "Mission Critical Data (MCData) signalling control; Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical data 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>

D.5 XML schema for MBMS usage information

D.5.1 General

This subclause defines XML schema and MIME type for application/vnd.3gpp.mcdata-mbms-usage-info+xml.

D.5.2 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:mcdataMbmsUsage:1.0"
xmlns:mcdatambms="urn:3gpp:ns:mcdataMbmsUsage:1.0">
    <!-- the root element -->
    <xs:element name="mcdata-mbms-usage-info" type="mcdatambms:mcdata-mbms-usage-info-Type"
id="mbms"/>
    <xs:complexType name="mcdata-mbms-usage-info-Type">
    <xs:sequence>
        <xs:element name="mbms-listening-status" type="mcdatambms:mbms-listening-statusType"
        minOccurs="0"/>
        <xs:element name="mbms-suspension-status" type="mcdatambms:mbms-suspension-statusType"
        minOccurs="0"/>
        <xs:element name="announcement" type="mcdatambms:announcementTypeParams" minOccurs="0"/>
        <xs:element name="version" type="xs:integer"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="mbms-listening-statusType">
    <xs:sequence>
        <xs:element name="mbms-listening-status" type="xs:string"/>
        <xs:element name="session-id" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="general-purpose" type="xs:boolean" minOccurs="0"/>
        <xs:element name="TMGI" type="xs:hexBinary" maxOccurs="unbounded"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="mbms-suspension-statusType">
    <xs:sequence>
        <xs:element name="mbms-suspension-status" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="number-of-reported-bearers" type="xs:integer" minOccurs="0"
maxOccurs="1"/>
        <xs:element name="suspended-TMGI" type="xs:hexBinary" minOccurs="0"/>
        <xs:element name="other-TMGI" type="xs:hexBinary" minOccurs="0" maxOccurs="unbounded"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:element name="mbms-defaultMuSiK-download" type="mcdatambms:mbms-default-ctrlkey-
downloadType"/>
<xs:complexType name="mbms-default-ctrlkey-downloadType">
        <xs:sequence>
            <xs:element type="xs:anyURI" name="group" minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:element name="mbms-explicitMuSiK-download" type="mcdatambms:mbms-explicit-ctrlkey-
downloadType"/>
    <xs:complexType name="mbms-explicit-ctrlkey-downloadType">
        <xs:sequence>
            <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="announcementTypeParams">
    <xs:sequence>
        <xs:element name="TMGI" type="xs:hexBinary" minOccurs="1"/>
        <xs:element name="QCI" type="xs:integer" minOccurs="0"/>
        <xs:element name="frequency" type="xs:unsignedLong" minOccurs="0"/>
        <xs:element name="mbms-service-areas" type="mcdatambms:mbms-service-areasType"
minOccurs="0"/>
        <xs:element name="GPMS" type="xs:positiveInteger" minOccurs="0"/>
```

```
        <xs:element name="report-suspension" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="mbms-service-areasType">
        <xs:sequence>
            <xs:element name="mbms-service-area-id" type="xs:hexBinary"
            minOccurs="1" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcdatambms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute/>
    </xs:complexType>

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

D.5.3 Semantic

The <mcdata-mbms-usage-info> element is the root element of the XML document. The <mcdata-mbms-usage-info> element contains the subelements:

1) <mbms-listening-status> containing the following elements:

   a) <mbms-listening-status> element contains a string used to indicate the MCData listening status:

      - The value "listening" indicates that the MCData client now is receiving RTP media packets and/or RTCP control packets over the MBMS subchannel in the session identified by the <session-id> element or if the <general-purpose> element is set to "true", that the MCData client is now listening to the general purpose MBMS subchannel.

      - The value "not-listening" indicates that the MCData client has stopped listening to the MBMS subchannel in the session identified by the <session-id> element or, if the <general-purpose> element is set to "false", that the MCData client no longer listens to the general purpose MBMS subchannel.

   Table D.5.3-1 shows the ABNF of the <mbms-listening-status> element.

Table D.5.3-1: ABNF syntax of values of the <mbms-listening-status> element

```
mbms-listening-status = listening-value / not-listening-value
listening-value = %x6c.69.73.74.65.6e.69.6e.67 ; "listening"
not-listening-value = %x6e.6f.74.2d.6c.69.73.74.65.6e.69.6e.67 ; "not-listening"
```

   b) <session-id> element contains the value of the URI received in the Contact header field received from the controlling MCData function when an on-demand session was established, or from the participating MCData function in the Connect message when the session was established over a pre-established session. This element is mandatory if the <general-purpose> element is not present in the application/vnd.3gpp.mcdata-mbms-usage-info+xml MIME body.

   c) <general-purpose> element is a boolean with the following meaning:

      - True indicates that the MCData client is listening to the general purpose MBMS subchannel associated to the TMGI(s) in the <TMGI> element(s) but have not yet received a Map Group To bearer message for any session that the MCData client is involved in.

      - False indicates that the MCData client is not listening to the general purpose MBMS subchannel any longer.

      Absence of the <general-purpose> element requires that the <session-id> element is present in the application/vnd.3gpp.mcdata-mbms-usage-info+xml; and

d) <TMGI>: element contains the TMGI. The <TMGI> element is coded as described in 3GPP TS 24.008 [62] subclause 10.5.6.13 excluding the Temporary Mobile Group Identity IEI and Length of Temporary Mobile Group Identity contents (octet 1 and octet 2 in 3GPP TS 24.008 [62] subclause 10.5.6.13).

2) <mbms-suspension-status>: contains the following subelements:

a) <mbms-suspension-status>: element is a string used to indicate the MBMS bearers intended suspension status:

- The value "suspending" indicates that the RAN has decided to suspend the referenced MBMS bearer(s) at the beginning of the next MCCH modification period.

- The value "not-suspending" indicates that the RAN has decided to revoke its decision to suspend the referenced MBMS bearer(s) before the beginning of the next MCCH modification period.

Table D.5.3-2 shows the ABNF of the <mbms-suspension-status> element.

Table D.5.3-2: ABNF syntax of values of the <mbms-suspension-status> element

```
mbms-suspension-status = suspending-value / not-suspending-value
suspending-value = %x73.75.73.70.65.6e.64.69.6e.67 ; "suspending"
not-suspending-value = %x6e.6f.74.2d.73.75.73.70.65.6e.64.69.6e.67 ; "not-suspending"
```

b) <number-of-reported-bearers>: a hex binary number denoting the total number of occurrences of the <suspended-TMGI> and <other-TMGI> elements reported as part of the MBMS bearer suspension status;

c) <suspended-TMGI>: contains a TMGI that is being reported as about to be suspended or as no longer about to be suspended; and

d) <other-TMGI>: contains a TMGI that is not being reported as about to be suspended or as no longer about to be suspended, but which shares the same MCH with MBMS bearers reported in the <suspended-TMGI> elements;

3) <announcement> element containing the following elements:

a) <TMGI>: contains the TMGI. The <TMGI> element is coded as described in 3GPP TS 24.008 [62] subclause 10.5.6.13 excluding the Temporary Mobile Group Identity IEI and Length of Temporary Mobile Group Identity contents (octet 1 and octet 2 in 3GPP TS 24.008 [62] subclause 10.5.6.13);

b) <QCI>: element contains QCI information used by the ProSe UE-Network Relay to determine the ProSe Per-Packet Priority value to be applied for the multicast packets relayed to Remote UE over PC5. QCI values are defined in 3GPP TS 23.203 [63];

c) <frequency>: element containing identification of frequency in case of multi carrier support. The <frequency> element is coded as specified in 3GPP TS 29.468 [57];

NOTE 1: In the current release the frequency in the <frequency> element is the same as the frequency used for unicast.

d) <mbms-service-areas>: element is a list of MBMS service area IDs for the applicable MBMS broadcast area as specified in 3GPP TS 23.003 [31] for Service Area Identifier (SAI), and with the encoding as specified in 3GPP TS 29.061 [64] for the MBMS-Service-Area AVP;

e) <GPMS>: element is a positive integer that gives the number of the media line containing the general purpose MBMS subchannel in the application/sdp MIME body attached to the SIP MESSAGE request containing the MBMS announcements;

f) <report-suspension>: element is a boolean with the following meaning:

- True indicates that the MCData client is instructed to notify the MCData server when it becomes aware of an intended change in the suspension status of a listened MBMS bearer.

- False indicates that the MCData client is instructed not to notify the MCData server if it becomes aware of an intended change in the suspension status of a listened MBMS bearer ; and

g) <anyExt> element can contain the following elements not shown in the XML schema:

i) < mcdata-mbms-rohc> element: presence of the < mcdata-mbms-rohc> element indicates that the flows delivered by the announced MBMS bearer are header compressed with ROHC as specified in RFC 5795 [60] and RFC 3095 [61]; and

ii) <max-cid> element: of type integer restricted to the range 1 to 16383 indicating the maximum CID value that can be used by the header compressor, see subclause 5.1.2 in RFC 5795 [60]). If max-cid > 15 then the header compressor uses the large CID representation. Else, the header compressor uses the small CID representation;

4) <version> is an element of type "xs:integer" indicating the version of the application/vnd.3gpp.mbms-usage-info MIME body. In this version the <version element> indicates "1"; and

5) <anyExt> element can contain the following elements:

a) <mbms-defaultMuSiK-download> that can contain:

i) a <group> element containing the identity, in the form of a URI, of a group for which the MuSiK download is performed; and

b) <mbms-explicitMuSiK-download> that can contain:

i) a <group> element containing the identity, in the form of a URI, of a group for which the MuSiK download is performed.

The recipient of the XML ignores any unknown element and any unknown attribute.

D.5.4 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcdata-mbms-usage-info+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. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

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

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

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 24.379 "Mission Critical Push To Talk (MCData) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk 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 E (normative): IANA registration forms

E.1 MIME type for transporting MCData signalling content

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcdata-signalling

Required parameters:

None

Optional parameters:

None

Encoding considerations:

binary.

Security considerations:

General mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

Security mechanisms specific to this MIME type are dependent upon the business and trust relationship between the mission critical data communications (MCData) operator and the SIP carrier operator. MCData operators may wish to encrypt and integrity protect the content transported by this MIME type indepedently of mechanisms provided by the transport layer. Such mechanisms are being specified in Rel-14 by 3GPP SA3. Security mechanisms applied to MCData signalling content is point-to-point (UE to server, server to server, server to UE).

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

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:

The content transported within this MIME type needs to be interpreted by a server as specific decisions are made based on the signalling content (e.g. store disposition history). The final destination point of the content is the terminating UE. Each UE and server that handles the content transported using this MIME type shall understand the definition of the messages and protocol elements as defined in 3GPP TS 24.282. Any messages and protocol elements not defined by 3GPP TS 24.282 shall be ignored by the recipient UE or server.

Published specification:

3GPP TS 24.282 "Mission Critical Data (MCData) signalling control; Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Application Usage:

Applications supporting the mission critical data communications procedures as described in the published specification. This MIME type shall contain signalling content that is related to the payload that is delivered to a terminating user or an application of the terminating user.

Fragment identifier considerations:

None.

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>

E.2 MIME type for transporting MCData payload content

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcdata-payload

Required parameters:

None

Optional parameters:

None

Encoding considerations:

binary.

Security considerations:

General mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

Security mechanisms specific to this MIME type are dependent upon the business and trust relationship between the mission critical data communications (MCData) operator and the SIP carrier operator. MCData operators may wish to encrypt and integrity protect the content transported by this MIME type indepedently of mechanisms provided by the transport layer. Such mechanisms are being specified in Rel-14 by 3GPP SA3. Security mechanisms applied to MCData payload are end-to-end (UE to UE).

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

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:

The content transported within MIME type does not need to be interpreted by a server. It represents the payload that is delivered to the end-user or an application of the end-user. Each UE and server that handles the content transported using this MIME type shall understand the definition of the messages and protocol elements as defined in 3GPP TS 24.282. Any messages and protocol elements not defined by 3GPP TS 24.282 shall be ignored by the recipient UE or server.

Published specification:

3GPP TS 24.282 "Mission Critical Data (MCData) signalling control; Protocol specification" available via http://www.3gpp.org/specs/numbering.htm.

Application Usage:

Applications supporting the mission critical data communications procedures as described in the published specification. This MIME type shall contain data that is delivered to a terminating user or an application of the terminating user.

Fragment identifier considerations:

None.

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 F (normative): Timers

F.1 General

The following tables give a brief description of the timers used in the present document.

For the on-network timers described in the present document, the following timer families are used:

- TDPx: Timer Data Participating function x; and
- TDCy: Timer Data Controlling function y.

For the off-network timers described in the present document, the following timer families are used:

- TFSz: Timer oFf-network SDS z;

where x, y and z represent numbers.

F.2 On-network timers

F.2.1 Timers in the participating MCData function

Table F.2.1-1: Participating MCData function timers

Timer	Timer value	Cause of start	Normal stop	On expiry
TDP1 (SDS re-delivery timer) (NOTE)	Default value: 60 seconds Configurable.	On reception of a "SIP MESSAGE request for SDS disposition notification for MCData server" containing an SDS disposition notification type set to a value of "UNDELIVERED",	On reception of a "SIP MESSAGE request for SDS disposition notification for MCData server" containing an SDS disposition notification type set to a value of "DELIVERED", "READ" or "DELIVERED AND READ"	Re-deliver the SDS message to the MCData user.
NOTE: More than one instance of this timer can be running in the participating MCData function, each instance associated with a specific SDS message.				

F.2.2 Timers in the controlling MCData function

Table F.2.2-1: Controlling MCData function timers

Timer	Timer value	Cause of start	Normal stop	On expiry
TDC1 (disposition notification timer) (NOTE 1)	Default value: 5 seconds Configurable.	On reception of a "SIP MESSAGE request for SDS disposition notification for MCData server" from a group member and aggregation of dispositions is required.	On reception of a "SIP MESSAGE request for SDS disposition notification for MCData server" from a group member where aggregation of disposition notifications is required and all other disposition notifications have been received from all other group members	Send the aggregated disposition notifications to the MCData user.
TDC2 (file availability timer) (NOTE 2)	(NOTE 3)	On reception of an FD request using HTTP or using media plane.	On reception of a "SIP MESSAGE request for FD disposition notification for MCData server" from all the invited member(s) and the FD disposition notification type IE is set to "FILE DOWNLOAD REQUEST REJECTED"	Recipients are informed that the file is not available to download any longer as specified in subclause 12.4.2.1
TDC3 (request for extension)	Default value: 15 seconds Configurable.	Upon receiving SIP 200 (OK) from MCData client for the SIP INFO / SIP MESSAGE message sent as intent to release communication	Upon receiving request for extension of MCData communication from MCData client.	Release the MCData communication immediately.

NOTE 1: More than one instance of this timer can be running in the controlling MCData function, each instance associated with a specific group SDS message.
NOTE 2: More than one instance of this timer can be running in the controlling MCData function associated with each file. Each timer for the file is associated uniquely to a Conversation ID and Message ID.
NOTE 3: An FD request can contain metadata with "file availability" information. If the FD request contains "file availability", then the controlling MCData function uses this information to derive the timer value. If the FD request does not contain "file availability" information, then the controlling MCData function sets a value for the timer based upon local policy.

F.2.3 Timers in the MCData UE

Table F.2.3-1: MCData UE timers

Timer	Timer value	Cause of start	Normal stop	On expiry
TDU1 (delivery and read) (NOTE)	Default value: 120 milliseconds Configurable.	When the client receives a SDS message with Disposition request type IE set to "DELIVERY AND READ".	When a SDS message display indication is received.	Send a SDS notification with Disposition type IE set to "DELIVERED" and when the MCData client has displayed the message to the MCData user, send a SDS notification with Disposition type IE set to "READ"
TDU2 (FD non-mandatory download timer) (NOTE)	Default value: 60 seconds Configurable.	On reception of an FD request not indicating mandatory download as specified in subclause 10.2.1.2.3	When the MCData user performs the action to accept, reject or defer the FD request as specified in subclause 10.2.1.2.3	No specific action by the MCData UE.
NOTE: Value of timer TDU1 (delivery and read) should be configured such that, when a consolidated "DELIVERED AND READ" notification is not feasible, the MCData client is able to send the "DELIVERED" disposition notification without delay.				

F.3 Off-network timers

F.3.1 Timers in off-network SDS

The table F.3.1-1 lists the timers used in off-network SDS, their start values, their limits, describes the cause of the start, and the action to take on normal stop and on expiry.

Table F.3.1-1: Timers in off-network SDS

Timer	Timer value	Cause of start	Normal stop	On expiry
TFS1 (SDS message retransmission)	Default value: 40 millisecond Configurable.	When the client sends a SDS OFF-NETWORK MESSAGE message.	Associated counter CFS1 (SDS message retransmission) reaches upper limit	Send a SDS OFF-NETWORK MESSAGE message.
TFS2 (SDS notification retransmission)	Default value: 40 millisecond Configurable.	When the client sends a SDS OFF-NETWORK NOTIFICATION message.	Associated counter CFS2 (SDS notification retransmission) reaches upper limit	Send a SDS OFF-NETWORK NOTIFICATION message.
TFS3 (delivery and read)	Default value: 120 millisecond Configurable.	When the client receives a SDS OFF-NETWORK MESSAGE with Disposition request type IE set to "DELIVERY AND READ".	When a SDS message display indication is received.	Send a SDS OFF-NETWORK NOTIFICATION message with Disposition type IE set to "DELIVERED" and when the MCData client has displayed the message to the MCData user, send a SDS OFF-NETWORK NOTIFICATION message with Disposition type IE set to "READ"
NOTE: Value of timer TFS3 (delivery and read) should be configured such that, when a consolidated "DELIVERED AND READ" notification is not feasible, the MCData client is able to send the "DELIVERED" disposition notification without delay.				

F.3.2 Timers in off-network emergency alert

The table F.3.2-1 lists the timers used in off-network emergency alert, their start values, their limits, describes the cause of start, and the action to take on normal stop and on expiry.

Table F.3.2-1: Timers in off-network emergency alert

Timer	Timer value	Cause of start	Normal stop	On expiry
TFE1 (Emergency Alert)	Default value: 30 seconds Maximum value: 60 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFE1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [4].	Receipt of GROUP EMERGENCY ALERT.	Receipt of GROUP EMERGENCY ALERT CANCEL.	Assume end of emergency state, remove associated user from the list.
TFE2 (emergency alert retransmission)	Default value: 5 seconds Maximum value: 10 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFE2" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [4].	Transmission of GROUP EMERGENCY ALERT.	Transmission of GROUP EMERGENCY ALERT CANCEL.	Transmit GROUP EMERGENCY ALERT.

Annex G (normative): Counters and states

G.1 General

The following tables give a brief description of counters and states used in the present document.

G.2 On-network counters

None defined.

G.3 Off-network counters

G.3.1 Counters in off-network SDS

The table G.3.1-1 lists the counters used in off-network SDS, their default upper limits and the action to take upon reaching the upper limit. The counters start at 1.

Table G.3.1-1: Counters in off-network SDS

Counter	Upper Limit	Associated timer	Upon reaching the upper limit
CFS1 (SDS message retransmission)	Default value: 5 Configurable.	TFS1	Stop timer TFS1.
CFS2 (SDS notification retransmission)	Default value: 5 Configurable.	TFS2	Stop timer TFS2.

G.4 On-network emergency related states

G.4.1 MCData emergency alert state

Table G.4.1-1 provides the semantics of the MCData emergency alert (MDEA) state values. This is an internal state of the MCData client and is managed by the MCData client. These state values aid in the managing of the information elements of MCData emergency alerts and their cancellations.

Table G.4.1-1: MCData emergency alert state

MCData emergency alert state values	State-entering events	Comments
MDEA 1: no-alert	initial state emergency alert cancelled emergency alert request denied	emergency alerts can be cancelled via requests with <alert-ind> set to "false" (by initiator or by authorised user)
MDEA 2: emergency-alert-confirm-pending	emergency alert request sent	emergency alerts can be requested using <alert-ind> set to "true"
MDEA 3: emergency-alert - initiated	emergency alert response (success) received	
MDEA 4: emergency-alert-cancel-pending	emergency alert cancellation request sent by alert originator	

Editor's Note: [CR 0066, WI eMCData2] The text above needs to be revisited/revised if Stage 2 changes to include MCData emergency communications group or MCData emergency state.

G.4.2 MCData emergency state

The MCData emergency state is managed by the MCData client and MCData user. High-level characteristics of this state are captured in table G.4.2-1.

Table G.4.2-1: MCData emergency state

MCData emergency state	State-setting events	State-clearing events	Comments
Values: "set": MCData user is in a life-threatening situation "clear": MCData user is not in a life-threatening situation Managed by: MCData client and MCData user	MCData emergency alert initiated MCData emergency communication initiated	MCData emergency alert cancelled (by initiator) MCData emergency alert cancelled (by authorised-user) MCData emergency communication cancelled by initiator (if there is no outstanding MCData emergency alert) MCData user manually clears the state	While the MCData client is in the MCData emergency state, all group communications it makes will be MCData emergency group communications, providing the group is authorised for MCData emergency group communications. While in an emergency group communication while in the MCData emergency state, the MCData user is an emergency participant and will have pre-emptive priority over non-emergency participants in the emergency group communication.

G.4.3 In-progress emergency group state

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

This state conforms with TS 23.282 [2]. It is managed by the controlling MCData function. High-level characteristics of this state are captured in table G.4.3-1.

Table G.4.3-1: in-progress emergency group state

In-progress emergency group state values	State-entering events	Comments
"true"	acceptance by the controlling MCData function of an MCData emergency group communication request.	
"false"	initial state prior to any communication activity acceptance by the controlling MCData function of an MCData emergency group cancel request.	

G.4.4 MCData emergency group state

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

The MCData emergency group state is the MCData client's perspective of the in-progress emergency group state which is managed by the controlling MCData function. The MCData emergency group (MDEG) state is managed by the MCData client to enable the requesting of MCData emergency-level priority as early as possible in the origination of an MCData emergency group communication. High-level characteristics of this state are captured in table G.4.4-1.

Table G.4.4-1: MCData emergency group state

MCData emergency group state values	State-entering events	Comments
MDEG 1: no-emergency	initial state prior to any communication activity Emergency group communication cancel request received on behalf of another user from the MCData server Emergency group communication cancel response (success) in response to initiator's request	
MDEG 2: in-progress	Emergency group communication response received (confirm) to initiator's emergency group communication request Emergency group communication request received (on behalf of another user)	In this state, all participants in communications on this group will receive emergency level priority whether or not they are in the MCData emergency state themselves.
MDEG 3: cancel-pending	Emergency group communication cancel request sent by initiator	The controlling MCData server may not grant the cancel request for various reasons, e.g., other users in an MCData emergency state remain in the communication.
MDEG 4: confirm-pending	Emergency group communication request sent by initiator	The controlling MCData server may not grant the request for various reasons, e.g., the MCData group is not configured as being emergency-capable so it can't be assumed that the group will enter the in-progress state.

G.4.5 MCData emergency group communication state

Editor's note: In the current release, support for emergency groups and emergency group communications may be absent, partial or limited, namely only provided to the extent of facilitating emergency alert functionality.

Table G.4.5-1 provides the semantics of the MCData emergency group communication (MDEGC) state values. This is an internal state of the MCData client and is managed by the MCData client. This state variable aids in the managing of the information elements of MCData emergency group communications and MCData emergency alerts and their cancellations.

Table G.4.5-1: MCData emergency group communication state

MCData emergency group communication state values	Semantics	Comments
MDEGC 1: emergency-gc-capable	MCData emergency-capable client is not currently in an MCData emergency group communication that it has originated, nor is it in the process of initiating one.	MCData emergency state: may or may not be set in this state, depending upon the MCData client's MDEA state
MDEGC 2: emergency-communication-requested	MCData client has initiated an MCData emergency group communication request.	MCData emergency state: is set
MDEGC 3: emergency-communication-granted	MCData client has received an MCData emergency group communication grant.	If the MCData user initiates a communication while the MCData emergency state is still set, that communication will be an MCData emergency group communication, assuming that the group is authorised for the client to initiate emergency group communications on. MCData emergency state: is set

Annex H (informative): INFO packages defined in the present document

H.1 Info package for indication of communication release

H.1.1 Scope

This subclause contains the information required for the IANA registration of info package g.3gpp.mcdata-com-release in accordance with IETF RFC 6086.

H.1.2 g.3gpp.mcdata-com-release info package

H.1.2.1 Overall description

When one of the communication release conditions are met e.g. lack of bearer capacity, limit for the maximum amount of data or time that a participant transmits from a single request to transmit exceeded, the MCData server may decide to release communication. Based on local policy and configuration, MCData server can release the communication without prior notification to MCData user; or it may send a notification to MCData user and allow the user to request for extension if the MCData user wants to. With this notification, MCData server may also request for more information related to ongoing communication like amount of data remainnig to be transmitted. If MCData user requests for extension of the MCData communication, MCData server can accept or reject based on local policy.

H.1.2.2 Applicability

This package is used to:

- send MCData server's intent to release the communication to the MCData client
- send more data from MCData client to MCData server when requested
- request extension of the MCData communication to MCData server.
- send response for extension request from MCData server to MCData client.

H.1.2.3 Appropriateness of INFO Package Usage

A number of solutions were discussed for sending MCData server's intent to release the communication along with request for more data to MCData user. The solutions were:

1) Use of the session related methods (e.g. SIP RE-INVITE 200 (OK) response.
2) Use of the SIP INFO method as described in IETF RFC 6086, by defining a new info package.

The result of the evaluation of the above solutions were:

1) An SIP INVITE request will have three-way handshake, which may not be optimal to transfer the required data.
2) The use of SIP INFO request was found as the most appropriate solution since the SIP INFO request could be sent in the existing SIP session and can carry QUERY response in 200 OK.

H.1.2.4 Info package name

g.3gpp.mcdata-com-release

H.1.2.5 Info package parameters

None defined

H.1.2.6 SIP options tags

None defined

H.1.2.7 INFO message body parts

The MIME type of the message body carrying application/vnd.3gpp.mcdata-signalling and application/vnd.3gpp.mcdata-payload. Both application/vnd.3gpp.mcdata-signalling and application/vnd.3gpp.mcdata-payload MIME type is defined in this specification.

H.1.2.8 Info package usage restrictions

None defined.

H.1.2.9 Rate of INFO Requests

Single INFO request generated after MCData server decides to release communication with prior notification to MCData client and not requesting for more data.

Two INFO requests generated after MCData server decides to release communication with prior notification to MCData client and requesting more data.

Two INFO requests generated after MCData client requests for extension of communication.

H.1.2.10 Info package security considerations

The security is based on the generic security mechanism provided for the underlying SIP signalling. No additional security mechanism is defined.

H.1.2.11 Implementation details and examples

UAC generation of INFO requests: See 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification".

UAS processing of INFO requests: See 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification".

Annex I (informative): Change history

Change history						
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**New**
2017-01					Initial version.	0.0.0
2017-01					Implementing the following P-CRs after CT1#101-bis: C1-170189, C1-170438, C1-170439, C1-170440, C1-170442, C1-170480.	0.1.0
2017-02					Implementing editorials spotted in v0.1.0 and implementing the following P-CRs after CT1#102: C1-171057, C1-171058, C1-171119.	0.2.0
2017-04					Implementing the following P-CRs after CT1#103: C1-171420, C1-171423, C1-171428, C1-171728, C1-171732, C1-171737; C1-171739; C1-171740; C1-171741; C1-171742; C1-171744; C1-171745; C1-171778; C1-171806; C1-171814; C1-171815; C1-171816; C1-171817; C1-171819.	0.3.0
2017-05					Implementing the following P-CRs after CT1#104: C1-172166; C1-172167; C1-172168; C1-172218; C1-172224; C1-172225; C1-172247; C1-172283; C1-172371; C1-172372; C1-172373; C1-172374; C1-172375; C1-172377; C1-172537; C1-172538; C1-172541; C1-172542; C1-172544; C1-172545; C1-172546; C1-172548; C1-172736; C1-172737; C1-172739; C1-172742; C1-172752.	0.4.0
2017-06	CT-76	CP-171110			Version 1.0.0 created for presentation at CT for information	1.0.0
2017-06	CT-76				Version 14.0.0 created after approval at CT	14.0.0
2017-06	CT-76				Addition of missing XSD files	14.0.1
2017-09	CT-77	CP-172102	0001	1	Completing affiliation check for MCData	14.1.0
2017-09	CT-77	CP-172102	0002	1	Fixing auto-send and auto-receive	14.1.0
2017-09	CT-77	CP-172102	0003	1	Adding warnings for MCData	14.1.0
2017-09	CT-77	CP-172102	0004	1	SDS Session Late entry	14.1.0
2017-09	CT-77	CP-172102	0005		mcdata-mcdata-id	14.1.0
2017-09	CT-77	CP-172102	0006	1	Services configuration	14.1.0
2017-09	CT-77	CP-172102	0007		Location information	14.1.0
2017-09	CT-77	CP-172102	0008	1	Security clause 4.7	14.1.0
2017-09	CT-77	CP-172102	0009	2	Confidentiality and Integrity Protection of TLV messages	14.1.0
2017-09	CT-77	CP-172102	0010		Timers and counters	14.1.0
2017-09	CT-77	CP-172102	0012	1	Off-network SDS	14.1.0
2017-09	CT-77	CP-172102	0013		Redundant editor's notes	14.1.0
2017-12	CT-78	CP-173064	0015	1	MCData Overview	14.2.0
2017-12	CT-78	CP-173064	0016	3	Authentication and key distribution	14.2.0
2017-12	CT-78	CP-173064	0017		Corrections to deferred download	14.2.0
2017-12	CT-78	CP-173064	0018		Redundant Editor's Notes	14.2.0
2017-12	CT-78	CP-173064	0019		Enhanced Status	14.2.0
2017-12	CT-78	CP-173064	0020		File availability parameters	14.2.0
2017-12	CT-78	CP-173064	0021		EN on security	14.2.0
2017-12	CT-78	CP-173064	0022	2	Corrections on FD Disposition Notification	14.2.0
2017-12	CT-78	CP-173064	0023	2	Remove mcdata-signed+xml	14.2.0
2017-12	CT-78	CP-173075	0014	3	Response-Source header field handling completion	15.0.0
2018-03	CT-79	CP-180073	0025	1	Correction to mcdatainfo schema	15.1.0
2018-03	CT-79	CP-180082	0026	3	Accessing list of deferred data group communications	15.1.0
2018-03	CT-79	CP-180082	0027	1	Authorized MCData user initiated communication release with prior indication	15.1.0
2018-03	CT-79	CP-180082	0028	1	Authorized MCData user initiated communication release without prior indication	15.1.0
2018-03	CT-79	CP-180082	0029	1	On-network Enhanced Status	15.1.0
2018-06	CT-80	CP-181054	0034	2	MCData Cplane SDS procedure selection criterion	15.2.0
2018-06	CT-80	CP-181064	0035	1	Modification in usage of mcdata-enhanced-status-operational-values element for on-network ES	15.2.0
2018-06	CT-80	CP-181064	0036	2	Off network enhanced status	15.2.0
2018-06	CT-80	CP-181064	0037	1	MCData originating user initiated release of MCData communication over HTTP	15.2.0

2018-06	CT-80	CP-181064	0038	1	MCData server initiated release of MCData communication over HTTP	15.2.0
2018-06	CT-80	CP-181064	0039	1	MCData server initiated release of MCData communication over HTTP with prior indication	15.2.0
2018-06	CT-80	CP-181064	0040	1	Auth user initiated release of MCData communication over HTTP	15.2.0
2018-06	CT-80	CP-181064	0041	1	Auth user initiated release of MCData communication over HTTP with prior indication	15.2.0
2018-06	CT-80	CP-181054	0043	2	Protected payload message types	15.2.0
2018-06	CT-80	CP-181064	0045	1	Extended application Id for MCData SDS messages	15.2.0
2018-06	CT-80	CP-181064	0046	1	Essential corrections in communication release procedures	15.2.0

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2018-09	CT#81	CP-182125	0048	1	A	Completed IANA registrations for MCData	15.3.0
2018-09	CT#81	CP-182125	0050	1	A	Fix issues with encoding of IEs in MONP messages for MCData	15.3.0
2018-09	CT#81	CP-182147	0051		F	Change Extended Application ID from TLV to TLV-E	15.3.0
2018-09	CT#81	CP-182125	0053		A	Addition of Registration without Auth Token	15.3.0
2018-12	CT#82	CP-183045	0056		F	Removal of editor's notes	15.4.0
2018-12	CT#82	CP-183059	0058		A	Correct root element in presence event package	15.4.0
2018-12	CT#82	CP-183059	0060		A	Correction of the "prefix" attribute handling	15.4.0
2018-12	CT#82	CP-183059	0062		A	Rel-14 completed IANA registrations for MCData	15.4.0
2019-03	CT#83	CP-190094	0063	2	F	Clarification of encoding of MCData signalling content and MCData payload content	15.5.0
2019-06	CT#84	CP-191118	0065		A	Removing IP Address from media-level section in SDP body for MCData Standalone SDS using media plan, SDS Session and FD using media plane	15.6.0
2019-06	CT#84	CP-191118	0070	1	A	Corrections in MCData SDS Session	15.6.0
2019-06	CT#84	CP-191140	0066	3	B	Emergency Alerts for MCData – General sections	16.0.0
2019-06	CT#84	CP-191140	0067	3	B	Emergency Alerts for MCData – sending origination request, on-network	16.0.0
2019-06	CT#84	CP-191140	0068	2	B	Emergency Alerts for MCData – cancelation, on-network	16.0.0
2019-09	CT#85	CP-192061	0071	1	C	Extended Application ID for MCData FD Messages	16.1.0
2019-09	CT#85	CP-192061	0072	1	B	Add Location procedures for MCData	16.1.0
2019-09	CT#85	CP-192042	0076	1	A	Fix for plugtest reported issue on mcdata notification	16.1.0
2019-12	CT#86	CP-193108	0077	1	C	Introduction of LMR Message as a value for MCData Payload content type	16.2.0
2019-12	CT#86	CP-193109	0078	1	C	Adding file description in MCData FD communication	16.2.0
2019-12	CT#86	CP-193102	0079	2	B	Pre-established session – References, General details and warning updates	16.2.0
2019-12	CT#86	CP-193102	0080	2	B	Common procedures for initiating SDS communication using pre-established session	16.2.0
2019-12	CT#86	CP-193102	0081	2	B	Pre-established session – General and PF use of resource sharing	16.2.0
2019-12	CT#86	CP-193102	0082	2	B	Client side procedure - Pre-established session establishment	16.2.0
2019-12	CT#86	CP-193102	0083	2	B	Pre-established session release	16.2.0
2019-12	CT#86	CP-193102	0084	2	B	Client side procedures – Initiating one-to-one SDS communication using pre-established session	16.2.0
2019-12	CT#86	CP-193102	0085	2	B	PF side procedures – Initiating MCData communication using pre-established session	16.2.0
2019-12	CT#86	CP-193102	0086	2	B	Initiating group SDS communication using pre-established session	16.2.0
2019-12	CT#86	CP-193102	0087	2	B	Leaving SDS communication using pre-established session	16.2.0
2019-12	CT#86	CP-193102	0088	2	B	PF side procedure - Pre-established session establishment	16.2.0
2019-12	CT#86	CP-193109	0091	1	F	Correct target of error response	16.2.0
2019-12	CT#86	CP-193102	0092	2	B	Add signalling plane capability to support transmission / reception via MBMS in MCData	16.2.0
2019-12	CT#86	CP-193109	0094	1	F	Correction of internal clause reference for implicit affiliation	16.2.0
2019-12	CT#86	CP-193102	0095	3	B	Add off-network emergency alert to MCData	16.2.0
2019-12	CT#86	CP-193109	0096	1	F	Correct MCData location schema	16.2.0
2019-12	CT#86	CP-193102	0097	3	B	Addition of Location information to SDS	16.2.0
2020-03	CT#87e	CP-200121	0099		F	Correcting SIP related terminology	16.3.0
2020-03	CT#87e	CP-200121	0100	1	F	Correct reference in 8.3.2.6	16.3.0
2020-03	CT#87e	CP-200122	0101	1	B	IP Connectivity	16.3.0
2020-03	CT#87e	CP-200115	0102	1	B	MCData key download procedure	16.3.0
2020-03	CT#87e	CP-200115	0103	2	B	Retrieval of stored object	16.3.0
2020-03	CT#87e	CP-200115	0104	2	B	Search for Objects in MCData message store	16.3.0
2020-03	CT#87e	CP-200115	0105	3	B	Update Object(s) in MCData message store	16.3.0
2020-03	CT#87e	CP-200115	0106	1	B	Delete Stored Object(s) in MCData message store.	16.3.0
2020-03	CT#87e	CP-200115	0107	1	B	Add Message Store Client subclause	16.3.0
2020-03	CT#87e	CP-200115	0108	1	B	Copy stored object(s) and-or folder(s)	16.3.0
2020-03	CT#87e	CP-200115	0109	1	B	Creating new folder	16.3.0
2020-03	CT#87e	CP-200115	0110	1	B	Delete folder	16.3.0
2020-03	CT#87e	CP-200115	0111	1	B	Move object(s) and folder(s)	16.3.0
2020-03	CT#87e	CP-200115	0112	1	B	Search for Folders in MCData message store	16.3.0
2020-03	CT#87e	CP-200115	0113	1	B	Move the stored object to destination folder	16.3.0
2020-03	CT#87e	CP-200115	0114	1	B	Upload the objects to the MCData message store	16.3.0
2020-03	CT#87e	CP-200115	0115	1	C	Accessing the absolute URI associated with the media storage function	16.3.0
2020-03	CT#87e	CP-200121	0116	1	F	Corrections to TDC2 and TDC3 timer handling	16.3.0
2020-03	CT#87e	CP-200115	0117	1	B	The pre-establshed session modification for MCData	16.3.0
2020-06	CT#88-e	CP-201112	0118	1	B	Deposit an object	16.4.0

2020-06	CT#88-e	CP-201112	0119	1	B	Create a subscription to notifications	16.4.0
2020-06	CT#88-e	CP-201112	0120	1	B	Delete a subscription to notifications	16.4.0
2020-06	CT#88-e	CP-201112	0121	1	B	Update a subscription to notifications MCC note: In the first sentence of §21.2.14A.1, the word "may" was substituted for "can".	16.4.0
2020-06	CT#88-e	CP-201112	0122	1	B	Synchronization notificatdion MCC note: Resolved reference to clause "21.2.n" in § 21.2.16.2 1) b) as 21.2.11.1.	16.4.0
2020-06	CT#88-e	CP-201112	0123	1	B	Search-based Synchronization	16.4.0
2020-06	CT#88-e	CP-201112	0124	1	B	List folder	16.4.0
2020-06	CT#88-e	CP-201112	0125	3	C	Editor's note for hostname of MCData message store is addressed MCC note: CR not written to correct version of the Spec, but was implementable.	16.4.0
2020-06	CT#88-e	CP-201112	0126	2	B	Support for MCData emergency alert and communications MCC note: This CR introduces the abbreviation IMPU; MCC has added this in the list of abbreviations, choosing the most appropriate of the five variations appearing in other 3GPP Specs. Similarly, MCC has provided the expansions of abbreviations UUID and URN introduced, but not defined by, this CR. The newly introduced term "Group identity" has a circular definition. In §D.1.3,, "can" has been changed to "may" in newly introduced bullet points 11 c), 11 c) i), and 11 e).	16.4.0
2020-06	CT#88-e	CP-201112	0127	2	B	Emergency Alerts for MCData – client procedures	16.4.0
2020-06	CT#88-e	CP-201112	0128	2	B	Handling of MCData Emergency Alerts at the MCData participating servers	16.4.0
2020-06	CT#88-e	CP-201112	0129	2	B	Handling of MCData Emergency Alerts at the MCData controlling server	16.4.0
2020-06	CT#88-e	CP-201112	0130	2	B	Auxiliary procedures in support of Emergency Alerts for MCData	16.4.0
2020-06	CT#88-e	CP-201112	0131	1	F	Issue fixes in MCData pre-established session	16.4.0
2020-06	CT#88-e	CP-201123	0132	1	B	IPConnectivity extension to include IP Information	16.4.0
2020-06	CT#88-e	CP-201123	0133	3	F	Corrections to file upload-download procedure as per stage 2 architecture changes	16.4.0
2020-06	CT#88-e	CP-201123	0134		B	Add functional alias status definitions	16.4.0
2020-06	CT#88-e	CP-201123	0135		B	Add functional alias to clause 4.6	16.4.0
2020-06	CT#88-e	CP-201121	0136		F	Correct <mcdata-calling-user-identity>	16.4.0
2020-06	CT#88-e	CP-201121	0137		D	Editorial correction – 6.3.6.1 MCC note: removal of extraneous underlining	16.4.0
2020-06	CT#88-e	CP-201121	0138		D	Editorial correction – 10.2.5.4.4 MCC note: adds "if" at start of point 9) g)	16.4.0
2020-06	CT#88-e	CP-201121	0139	1	D	Error correction – 13.2.1.1 MCC note: change of "client" to "server" is not editorial!	16.4.0
2020-06	CT#88-e	CP-201123	0140		B	Functional alias – 5.2	16.4.0
2020-06	CT#88-e	CP-201123	0141		B	Functional alias – 5.3	16.4.0
2020-06	CT#88-e	CP-201123	0142		B	Functional alias – 9.2.1.2	16.4.0
2020-06	CT#88-e	CP-201123	0143	1	B	Functional alias – 9.2.2.2.1	16.4.0
2020-06	CT#88-e	CP-201123	0144		B	Functional alias – 9.2.2.3.1	16.4.0
2020-06	CT#88-e	CP-201123	0145	1	B	Functional alias – 9.2.3.2.3	16.4.0
2020-06	CT#88-e	CP-201123	0146	1	B	Functional alias – 9.2.3.3.3	16.4.0
2020-06	CT#88-e	CP-201123	0147	1	B	Functional alias – 9.2.4.2.3	16.4.0
2020-06	CT#88-e	CP-201123	0148		B	Functional alias – 9.2.4.3.3	16.4.0
2020-06	CT#88-e	CP-201123	0149	1	B	Functional alias – 9.2.5.1.1	16.4.0
2020-06	CT#88-e	CP-201123	0150	1	B	Functional alias – 9.2.5.2.1.1	16.4.0
2020-06	CT#88-e	CP-201123	0151	1	B	Functional alias – 9.2.5.3.1.1	16.4.0
2020-06	CT#88-e	CP-201123	0152	1	B	Functional alias – 10.2.4.2.1	16.4.0
2020-06	CT#88-e	CP-201123	0153	1	B	Functional alias – 10.2.4.3.1	16.4.0
2020-06	CT#88-e	CP-201123	0154	1	B	Functional alias – 10.2.5.2.3	16.4.0
2020-06	CT#88-e	CP-201123	0155		B	Functional alias – 10.2.5.2.4	16.4.0
2020-06	CT#88-e	CP-201123	0156	1	B	Functional alias – 10.2.5.3.3	16.4.0
2020-06	CT#88-e	CP-201123	0157	1	B	Functional alias – 16.2.1.1	16.4.0
2020-06	CT#88-e	CP-201123	0158	1	B	Functional alias – 16.2.1.2	16.4.0
2020-06	CT#88-e	CP-201123	0159	1	B	Functional alias – 20.2.1	16.4.0
2020-06	CT#88-e	CP-201123	0160		B	Functional alias – 20.2.2	16.4.0
2020-06	CT#88-e	CP-201124	0161	1	B	Functional alias – affiliation procedures in 8.2	16.4.0
2020-06	CT#88-e	CP-201124	0163	1	B	Functional alias – MCData Client procedures	16.4.0
2020-06	CT#88-e	CP-201124	0164	1	B	Functional Alias – MCData Server procedures	16.4.0
2020-06	CT#88-e	CP-201124	0162	1	B	Functional alias – Coding	16.4.0
2020-06	CT#88-e	CP-201121	0165		F	Remove duplicate RFC 3856 reference	16.4.0
2020-06	CT#88-e	CP-201124	0166		B	Update MCData Overview clause 4.1	16.4.0
2020-06	CT#88-e	CP-201121	0167	1	D	Implement missing reference number	16.4.0

2020-06	CT#88-e	CP-201112	0168	1	B	Resolving EN for identifying user between MCData Server and MCData message store	16.4.0
2020-06	CT#88-e	CP-201124	0169		F	Corrections in IP Connectivity SDP offer/answer generation	16.4.0
2020-06	CT#88-e	CP-201112	0170	1	B	Signalling plane support in MCData for user plane SDS using MBMS	16.4.0
2020-06	CT#88-e	CP-201088	0173		A	Off-network MCData support	16.4.0
2020-06	CT#88-e	CP-201088	0174	1	A	Adding mcdata id in signalling payload for sender of the data in MCData media plane (Session) communication	16.4.0
2020-06	CT#88-e	CP-201124	0177		B	Update service authorization procedures to support limiting the number of authorized clients per MCData user	16.4.0
2020-06	CT#88-e	CP-201124	0178	1	B	Restricting incoming/outgoing MCData communications-control	16.4.0
2020-06	CT#88-e	CP-201112	0179	1	F	Client SIP INVITE request descriptions	16.4.0
2020-07						Editorial corrections	16.4.1
2020-09	CT#89-e	CP-202165	0180		F	Editors Notes in IP Connectivity	16.5.0
2020-09	CT#89-e	CP-202165	0181	1	F	Increment service authorisations	16.5.0
2020-09	CT#89-e	CP-202154	0184	1	F	Miscellaneous fixes	16.5.0
2020-09	CT#89-e	CP-202165	0185		F	Corrections on MCData related MONASTERY2 CRs implementation	16.5.0
2020-12	CT#90-e	CP-203202	0196		F	Fix on authorizations limit client notification	16.6.0
2020-12	CT#90-e	CP-203202	0198	1	F	Reject the unauthorized user request for functional alias activation	16.6.0

History

Document history		
V16.4.1	July 2020	Publication
V16.5.0	October 2020	Publication
V16.6.0	January 2021	Publication