ETSI TS 129 582 V16.5.0 (2023-07)

LTE;
5G;
Mission Critical Data (MCData)
interworking with Land Mobile Radio (LMR) systems;
Stage 3
(3GPP TS 29.582 version 16.5.0 Release 16)

Reference
RTS/TSGC-0129582vg50

Keywords
5G,LTE

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 7
Introduction 8
1 Scope 9
2 References 9
3 Definitions of terms, symbols and abbreviations 10
3.1 Terms 10
3.2 Abbreviations 11
4 General 11
4.1 MCData overview 11
4.2 Identity, URI and address assignments 12
4.2.1 Public Service identities 12
4.2.2 MCData session identity 12
4.2.3 MCData client ID 12
4.3 Emergency alerts 12
4.4 MCData protocol 12
4.5 Protection of sensitive XML application data 12
4.6 Protection of TLV signalling and media content 13
4.7 Warning Header Field 14
4.7.1 General 14
4.7.2 Warning texts 14
5 Roles 14
5.1 Introduction 14
5.2 IWF 14
5.2.1 General 14
5.2.1A SIP failure case 15
6 Common procedures 15
6.1 Introduction 15
6.2 IWF performing the participating role procedures 15
6.2.1 Void 15
6.2.2 MCData conversation items 15
6.2.2.1 IWF generating an SDS Message 15
6.2.3 Disposition Notifications 17
6.2.3.1 Generating an SDS Notification 17
6.2.4 Sending SIP requests and receiving SIP responses 18
6.2.4.1 Generating a SIP MESSAGE request towards the controlling MCData function 18
6.3 Server role procedures 18
6.3.0 Introduction 18
6.3.1 Distinction of requests at the IWF 18
6.3.1.1 SIP MESSAGE request 18
6.3.1.2 SIP INVITE request 19
6.3.2 Sending SIP requests and receiving SIP responses 19
6.3.2.1 Generating a SIP MESSAGE request towards the terminating MCData client 19
6.3.3 Groups homed in the IWF 19
6.3.4 Void 20
6.3.5 Affiliation check 20
6.4 Handling of MIME bodies in a SIP message 20
6.5 Confidentiality and Integrity Protection of sensitive XML content 20
6.5.1 General 20
6.5.1.1 Applicability and exclusions 20

6.5.1.2 Performing XML content encryption 20
6.5.1.3 Performing integrity protection on an XML body 20
6.5.2 Confidentiality Protection 20
6.5.2.2 Keys used in confidentiality protection procedures 20
6.5.2.3 Procedures for sending confidentiality protected content 21
6.5.2.3.2 IWF performing the role of an MCData server 21
6.5.2.5 IWF copying received XML content 21
6.5.3 Integrity Protection of XML documents 22
6.5.3.2 Keys used in integrity protection procedures 22
6.5.3.3 Sending integrity protected content 22
6.5.3.3.2 Integrity protection at the IWF 22
6.6 Confidentiality and integrity protection of TLV messages 22
6.6.1 General 22
6.6.2 Derivation of master keys for media and media control 23
6.6.3 Protection of MCData signalling and MCData messages 23
6.6.3.1 General 23

7 Registration and service authorisation 23
7.1 Server procedures 23

8 Affiliation 23
8.1 General 23
8.2 IWF performing the participating role procedures 24
8.3 Server procedures 24
8.3.1 General 24
8.3.2 Procedures of the IWF performing the participating role 24
8.3.2.1 General 24
8.3.2.2 Stored information 24
8.3.2.3 Receiving affiliation status change from a user homed in the IWF procedure 25
8.3.2.4 Receiving subscription to affiliation status procedure 25
8.3.2.5 Sending notification of change of affiliation status procedure 25
8.3.2.6 Sending affiliation status change towards MCData server owning MCData group procedure 25
8.3.2.7 Affiliation status retrieval from IWF performing the role of the MCData server owning MCData group procedure 26
8.3.2.8 Procedure for authorising affiliation status change request in negotiated mode sent to a user homed in the IWF 29
8.3.2.9 Forwarding affiliation status change towards an MCData user procedure 29
8.3.2.10 Forwarding subscription to affiliation status towards an MCData user procedure 29
8.3.2.11 Affiliation status determination 29
8.3.2.12 Affiliation status change by implicit affiliation 30
8.3.2.13 Implicit affiliation status change completion 31
8.3.2.14 Implicit affiliation status change cancellation 31
8.3.2.15 Automatic affiliation to configured groups procedure 31
8.3.3 Procedures of the IWF performing the controlling role 31
8.3.3.1 General 31
8.3.3.2 Stored information 32
8.3.3.3 Receiving group affiliation status change procedure 32
8.3.3.4 Receiving subscription to affiliation status procedure 33
8.3.3.5 Sending notification of change of affiliation status procedure 34
8.3.3.6 Implicit affiliation eligibility check procedure 35
8.3.3.7 Affiliation status change by implicit affiliation procedure 35
8.4 Coding 36

9 IWF Short Data Service (SDS) 36
9.1 General 36
9.2 On-network SDS 36
9.2.1 General 36
9.2.2 Standalone SDS using signalling control plane 36
9.2.2.1 General 36
9.2.2.2 Procedures used by the IWF for users homed in the IWF 37
9.2.2.2.1 Originating procedures 37
9.2.2.2.2 Terminating procedures 37
9.2.2.3 IWF performing the participating MCData function procedures 38

9.2.2.3.1 Originating participating MCData function procedures 38
9.2.2.3.2 IWF performing the terminating participating MCData role procedures 38
9.2.2.4 Controlling IWF MCData procedures 39
9.2.2.4.1 Originating controlling IWF procedures 39
9.2.2.4.2 Terminating controlling MCData function procedures 40
9.2.3 Standalone SDS using media plane 42
9.2.4 SDS session 42
9.3 Off-network SDS 42

10 File Distribution (FD) 42

11 Transmission and reception control 42
11.1 General 42
11.2 Auto-receive for File Distribution 42
11.3 Accessing list of deferred data group communications 43

12 Dispositions and Notifications 43
12.1 General 43
12.2 Disposition notifications 43
12.2.1 IWF performing the MCData participating role 43
12.2.1.1 Participating IWF procedures 43
12.2.1.2 Sending a disposition notification message 43
12.2.1.3 Participating IWF receives disposition notification from a controlling MCData function 44
12.2.2 IWF performing the MCData controlling role 44
12.3 On-network disposition notifications 46

13 Communication Release 46

14 Enhanced Status (ES) 46
14.1 General 46
14.2 On-network ES 46
14.2.1 Void 46
14.2.2 IWF performing the participating MCData role procedures 46
14.2.2.1 Originating participating MCData function procedures 46
14.2.2.2 Terminating participating MCData function procedures 47
14.2.3 IWF performing the controlling MCData role procedures 47
14.2.3.1 Originating controlling MCData function procedures 47
14.2.3.2 Terminating controlling MCData function procedures 47

15 Message Formats 47
15.1 IWF message functional definitions and contents 47
15.1.1 General 47
15.1.2 SDS SIGNALLING PAYLOAD message 48
15.1.2.1 Message definition 48
15.1.3 FD SIGNALLING PAYLOAD message 48
15.1.4 DATA PAYLOAD message 48
15.1.4.1 Message definition 48
15.1.5 SDS NOTIFICATION message 49
15.1.5.1 Message definition 49
15.1.6 FD NOTIFICATION message 49
15.1.7 SDS OFF-NETWORK MESSAGE 49
15.1.8 SDS OFF-NETWORK NOTIFICATION message 50
15.1.9 FD NETWORK NOTIFICATION message 50
15.1.10 COMMUNICATION RELEASE message 50
15.1.10.1 Message definition 50
15.1.11 DEFERRED DATA REQUEST message 50
15.1.12 DEFERRED DATA RESPONSE message 50
15.1.13 FD HTTP TERMINATION 50
15.2 General message format and information elements coding 50
15.2.1 General 50
15.2.2 Message type 51
15.2.3 Void 51
15.2.4 Void 51
15.2.5 Void 51

15.2.6 Void 51
15.2.7 Void 51
15.2.8 Void 51
15.2.9 Conversation ID 51
15.2.10 Message ID 52
15.2.11 Void 53
15.2.12 Void 53
15.2.13 Payload 53

16 Media plane 54

17 Handling of Interworking Security Data messages 54
17.1 IWF 54
17.1.1 IWF originates Interworking Security Data message 54
17.1.2 IWF receives Interworking Security Data message 55
17.2 Interworking Security Data message payload 55
17.2.1 Message definition 55
17.2.2 External network type 55

Annex A (informative): Signalling flows 56

Annex B (normative): Timers 57

Annex C (normative): Counters 58

Annex D (normative): XML schemas 59

D.1 XML schema for transporting MCData identities and general services information 59
D.1.1 General 59
D.1.2 XML schema 59

Annex E (informative): Change history 60

History 61

Foreword

This Technical Specification|Report 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.

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

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

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

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

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

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

can indicates that something is possible

cannot indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

Introduction

The present document has been produced as an aspect of work to realise the stage 3 protocols to implement the stage 2 functionality for Interworking between Mission Critical systems and Land Mobile Radio systems as described in 3GPP TS 23.283 [80]. Early stage 3 study work is documented in 3GPP TR 24.883 [90] which covers both MCPTT and MCData interworking.

The document structure describes functionality modelled on 3GPP TS 24.282 [49] because the behaviour of an Interworking Function (IWF) for LMR MCData interworking is modelled on that of an MCData server, and the clause numbering is also based on that used in on 3GPP TS 24.282 [49] in order to aid comparison between the two specifications and identification of any behavioural changes.

The reference numbering is based on that used in 3GPP TR 24.883 [90] and so may not be sequential.

1 Scope

The present document specifies the protocols needed to support a Mission Critical Data (MCData) system interworking with a Land Mobile Radio (LMR) system based on the IWF-2 interface between an MCData server and an Interworking Function (IWF) as described in 3GPP TS 23.283 [80].

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".

[4] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[5] 3GPP TS 23.379: "Functional architecture and information flows to support mission critical communication services; Stage 2".

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

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

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

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

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

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

[31] 3GPP TS 24.481: "Mission Critical Services (MCS) group management Protocol specification".

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

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

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

[49] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management Protocol specification.

[50] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management Protocol specification".

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

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

[78] 3GPP TS 33.180: "Security of the mission critical service".

[80] 3GPP TS 23.283: "Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2".

[81] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; protocol specification;".

[82] 3GPP TS 24.282: " Mission Critical Data (MCData) signalling control; Protocol specification;"

[85] 3GPP TS 24.582: "Mission Critical Data (MCData) media plane control; Protocol specification".

[86] IETF RFC 1738 (December 1994): "Uniform Resource Locators (URL)".

[87] 3GPP TS 29.379: "Mission Critical Push To Talk (MCPTT) call control interworking with LMR systems; Protocol specification".

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

[90] 3GPP TR 24.883: "Mission Critical Systems Connection to LMR".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.379 [5] apply:

Group call
MCPTT call
Mission critical push to talk
Private call
SIP core

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.283 [28] apply:

Interworking Function (IWF)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 29.379 [26] apply:

IWF performing the controlling role
IWF performing the non-controlling
IWF performing the participating role

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.180 [18] apply:

Group Master Key (GMK)
Group Master Key Identifier (GMK-ID)
Private Call Key (PCK)
Private Call Key Identifier (PCK-ID)
Signalling Protection Key (SPK)
Signalling Protection Key Identifier (SPK-ID)

For the purposes of the present document, the following terms and definitions given in IETF RFC 3711 [16] apply:

SRTP master key (SRTP-MK)
SRTP master key identifier (SRTP-MKI)
SRTP master salt (SRTP-MS)

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].

GMK	Group Management Key
GMK-ID	Group Master Key Identifier
GMS	Group Management Server
GUK-ID	Group User Key Identifier
IP	Internet Protocol
MCData	Mission Critical Data
PCK	Private Call Key
PCK-ID	Private Call Key Identifier
RFC	Request For Comment
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SPK	Signalling Protection Key
SPK-ID	Signalling Protection Key Identifier
SRTCP	Secure RTCP
SRTP	Secure RTP
SRTP-MK	SRTP master key
SRTP-MKI	SRTP master key identifier
SRTP-MS	SRTP master salt
SSRC	Synchronization SouRCe
UE	User Equipment

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).

The present document provides the signalling control protocol enhancements to support the MCData architectural procedures for MCData SDS interworking between on-network Mission Critical users and users homed in the IWF, as specified in 3GPP TS 23.283[80].

The present document makes use of the existing IMS procedures specified in 3GPP TS 24.229 [4].

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

- send a standalone SDS using signalling control plane to a user homed in the IWF or to a group including at least one user homed in the IWF; and
- send a standalone SDS using media plane to a user homed in the IWF or to a group including at least one user homed in the IWF.

The procedures in this document allow a user homed in the IWF to:

- send a standalone SDS using signalling control plane to an on-network MCData user or to a group of on-network MCData users; and
- send a standalone SDS using media plane to an on-network MCData user or to a group of on-network MCData users.

The present document does not support the interworking of SDS sessions with users homed in the IWF.

The MCData procedures provided by the present document refer to:

- the media plane procedures defined in 3GPP TS 24.582 [85];

- the group management procedures defined in 3GPP TS 24.481 [31];
- the identity management procedures defined in 3GPP TS 24.482 [49]; and
- the security procedures defined in 3GPP TS 33.180 [78].

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 SDS are specified in clause 9;
- 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; and
- procedures for enhanced status are specified in clause 14.

The IWF acts on behalf of all users homed in the IWF. There are no client procedures specified in the present document and specific client handling within the LMR system is out of scope.

4.2 Identity, URI and address assignments

4.2.1 Public Service identities

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

1) the IWF performing the participating role is configured to be reachable using a public service identity.
2) the IWF performing the controlling role is configured to be reachable using a public service identity.

4.2.2 MCData session identity

There is no MSRP session used at the IWF to support the short data service (SDS).

4.2.3 MCData client ID

The MCData client ID is described in 3GPP TS 24.282 [82] clause 4.8.

4.3 Emergency alerts

4.4 MCData protocol

Clause 15 describes the TLV based message formats used in MCData communications.

Annex I of 3GPP TS 24.379 [81] describes the standard format of the messages and the encoding rules for each type of information element.

4.5 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 exposed to the SIP layer. The following data are classified as sensitive application data:

- MCData ID;
- MCData group ID;
- alert indicator;
- access token (containing the MCData ID); and
- MCData client ID.

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

NOTE: SIP layer protection terminates at the IWF.

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 [51];
- an MCData ID or an MCData Group ID in XML document notified in a SIP NOTIFY request for affiliation according to IETF RFC 3856 [51]; and
- an MCData ID in application/resource-lists+xml document included in a SIP MESSAGE or SIP INVITE request for one-to-one SDS, according to IETF RFC 5366 [20];

3GPP TS 33.180 [78] 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 3GPP TS 24.282 [82] clause 6.6.2.3. 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 MCData servers and an IWF, the XPK is a signalling protection key (SPK).

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

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

3GPP TS 24.282 [82] clause 4.6 provides examples of confidentiality and integrity protection applied to application data.

4.6 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 [78].

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 server and the IWF.
- **MCData Data payload**: the actual user payload for MCData user or application consumption. This payload is confidentiality and integrity protected between the MCData client and the IWF.

An SDS message can be sent over the signalling plane or the media plane. When an SDS message is sent using the signalling plane, the body included in the SIP MESSAGE request, which carries the MCData Data signalling payload, is protected separately between each pair of entities if protection is applied. On the other hand, the body included in the SIP MESSAGE request which carries the MCData data payload is protected between the MCData client and the IWF. The procedures for the protection of the SDS messages over the signalling plane are specified in clause 6.6. Protection of SDS messages over the media control plane is specified in 3GPP TS 24.582 [85].

NOTE: The method by which SDS messages are protected between the IWF and the user homed in the IWF is outside the scope of the present document.

4.7 Warning Header Field

4.7.1 General

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

EXAMPLE: Warning: 399 example.domain.com "200 user not authorised to transmit data"

4.7.2 Warning texts

Warning texts specified in table 4.7.2-1 for interworking are used, in conjunction with existing warning texts as specified in 3GPP TS 24.282 [82].

Table 4.7.2-1: Warning texts for interworking defined for the Warning header field

Code	Explanatory text	Description
300	LMR system does not support requested application	An application has been requested that is not supported in the LMR system.
301	LMR system does not support disposition notification for requested application	A disposition notification has been requested for an application for which the LMR system does not support disposition notifications.

5 Roles

5.1 Introduction

This clause describes the functional roles for an IWF to support the MCData service.

5.2 IWF

5.2.1 General

When referring to the procedures in the present document for the IWF acting as a participating MCData server for the user homed in the IWF, the term, "IWF performing the participating role" is used.

When referring to the procedures in the present document for the IWF acting as a controlling MCData server for the user homed in the IWF, the term "IWF performing the controlling role" is used.

An IWF can perform the controlling role for short data service as defined in the present document.

An IWF can perform the participating role for short data service as defined in the present document.

An IWF in the participating role can serve an originating user homed in the IWF.

An IWF in the participating role can serve a terminating user homed in the IWF.

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

- support the MCData server procedures defined in 3GPP TS 23.283 [80];

- implement the role of an AS performing 3rd party call control acting as a routing B2BUA as defined in 3GPP TS 24.229 [4];
- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [4] and 3GPP TS 24.282 [82] clause 9.2.3 and 3GPP TS 24.282 [82] clause 9.2.4 for short data service;
- for registration and service authorisation, implement the procedures specified in 3GPP TS 24.282 [82] clause 7.3;
- for affiliation, implement the procedures specified in clause 9.2.2;
- for short data service (SDS) functionality implement the MCData server procedures specified in:
  a) clause 9.2; and
  b) clause 6 of 3GPP TS 24.582 [85];
- 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; and
- for communication release functionality implement the MCData server procedures specified in clause 13.2.

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

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

5.2.1A SIP failure case

When initiating a SIP failure response to any received SIP request, depending on operator policy, the IWF may insert a SIP Response-Source header field in accordance with the procedures in clause 5.7.1.0 of 3GPP TS 24.229 [4], 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.

6 Common procedures

6.1 Introduction

This clause describes the IWF procedures for MCData.

6.2 IWF performing the participating role procedures

6.2.1 Void

6.2.2 MCData conversation items

6.2.2.1 IWF generating an SDS Message

In order to generate an SDS message, the IWF performing the participating role:

1) shall generate an SDS SIGNALLING PAYLOAD message as specified in clause 15.1.2;
2) shall generate a DATA PAYLOAD message as specified in clause 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 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause E.2.

When generating an SDS SIGNALLING PAYLOAD message as specified in clause 15.1.2, the IWF performing the participating role:

1) shall set the Date and time IE to the current time as specified in 3GPP TS 24.282 [82] clause 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 clause 15.2.9;

3) if the SDS message continues an existing unfinished conversation, shall, if available, set the Conversation ID IE to the Conversation ID value of the existing conversation as specified in clause 15.2.9, or shall set the Conversation ID IE to the Conversation ID value "UNKNOWN CONVERSATION" as specified in clause 15.2.9;

4) shall set the Message ID IE to a newly generated Message ID value as specified in clause 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:

   i) set to the Message ID value in the previously received SDS message;

   ii) set to the Message ID value "LMR MESSAGE ID"as specified in clause 15.2.10, with the value of octet 16 of the LMR MESSAGE ID set to the value of octet 16 of the Message ID in the previously received SDS message; and

   iii) set to the Message ID value "UNKNOWN ORIGINATING MESSAGE ID" as specified in clause 15.2.10;

6) if the SDS message is for user consumption, shall not include an Application ID IE as specified in 3GPP TS 24.282 [82] clause 15.2.7 and shall not include an Extended application ID IE as specified in 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause 15.2.7; or

   b) an Extended application ID IE with an Extended application ID value representing the intended application as specified in 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause 15.2.3; and

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 3GPP TS 24.282 [82] clause 15.2.3.

When generating a DATA PAYLOAD message for SDS as specified in clause 15.1.4, the IWF performing the participating role:

1) shall set the Number of payloads IE to the number of Payload IEs that need to be encoded, as specified in clause 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 [78]. Otherwise, if end-to-end security is not required for a one-to-one communication, shall include the Payload IE as specified in clause 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 clause 15.2.13;

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

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

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

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

f) if payload is a native LMR message, shall set the Payload content type as "LMR MESSAGE" as specified in clause 15.2.13; and

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

6.2.3 Disposition Notifications

6.2.3.1 Generating an SDS Notification

In order to generate an SDS notification, the IWF performing the participating role:

1) shall generate an SDS NOTIFICATION message as specified in clause 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 3GPP TS 24.282 [82] clause E.1.

When generating an SDS NOTIFICATION message as specified in clause 15.1.5, the IWF performing the participating role:

1) if sending a delivered notification, shall set the SDS disposition notification type IE as "DELIVERED" as specified in 3GPP TS 24.282 [82] clause 15.2.5;

2) if sending a read notification, shall set the SDS disposition notification type IE as "READ" as specified in clause 3GPP TS 24.282 [82] 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 3GPP TS 24.282 [82] clause 15.2.5;

4) if the SDS message could not be delivered, shall set the SDS disposition notification type IE as "UNDELIVERED" as specified in 3GPP TS 24.282 [82] clause 15.2.5;

5) if SDS disposition notification was prevented by the LMR system, shall set the SDS disposition notification type IE as "DISPOSITION PREVENTED BY SYSTEM" as specified in 3GPP TS 24.282 [82] clause 15.2.5;

6) shall set the Date and time IE to the current time to as specified in 3GPP TS 24.282 [82] clause 15.2.8;

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

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

9) if the SDS message was destined for the user, shall not include an Application ID IE (as specified in 3GPP TS 24.282 [82] clause 15.2.7) and shall not include an Extended application ID IE (as specified in 3GPP TS 24.282 [82] clause 15.2.24); and

10) 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 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause 15.2.24.

6.2.4 Sending SIP requests and receiving SIP responses

6.2.4.1 Generating a SIP MESSAGE request towards the controlling MCData function

This clause is referenced from other procedures.

In a SIP MESSAGE request, the IWF performing the participating role:

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 [6];

   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 [6]; and

   c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [4]), in a P-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

2) 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 [4]; and

3) shall set the Request-URI to the public service identity of the controlling MCData function.

6.3 Server role procedures

6.3.0 Introduction

The IWF performs the MCData server role when exchanging SDS messages with MCData servers within the MC system. The IWF does not communicate directly with MCData clients. The IWF does not support the FD service. Clause 6.3 describes the IWF operating as a controlling and participating MCData server.

6.3.1 Distinction of requests at the IWF

6.3.1.1 SIP MESSAGE request

The IWF shall perform the role of an MCData server in distinguishing between the following SIP MESSAGE requests for originations and terminations from 3GPP TS 24.282 [82] clause 6.3.1.1 as described below:

- SIP MESSAGE request routed to the IWF performing the terminating participating MCData role 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 IWF performing the MCData server role 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 the IWF performing the controlling MCData role 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"; and

- SIP MESSAGE requests routed to the IWF performing the terminating participating role as a result of initial filter criteria with the Request-URI set to the public service identity of the IWF performing the participating role and containing a Content-Type header field set to "application/vnd.3gpp.mcdata-info+xml" and includes an XML body containing a <mcdatainfo> root element with a <mcdata-Params> element containing an <anyExt> element with the <request-type> element set to a value of "Interworking Security Data message". Such requests are known as "SIP MESSAGE request for Interworking Security Data message for participating function".

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

6.3.1.2 SIP INVITE request

The IWF shall perform the role of an MCData server in distinguishing between the following SIP INVITE requests for originations and terminations from 3GPP TS 24.282 [82] clause 6.3.1.2 as described below:

- SIP INVITE request routed to the IWF performing the terminating participating MCData role 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 IWF performing the controlling MCData role 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 IWF performing the terminating participating MCData role 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"; and

- SIP INVITE request routed to the IWF performing the controlling MCData role 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".

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 clause is referenced from other procedures. Refer to 3GPP TS 24.282 [82] clause 6.3.2.1.

6.3.3 Groups homed in the IWF

How information about groups homed in the IWF is stored and retrieved by the IWF is out of scope of the present document. The procedures to perform these actions are supported by the IWF but are not defined.

6.3.4 Void

6.3.5 Affiliation check

The IWF shall determine that the MCData user, with MCData 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 clause 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.

NOTE: How the IWF determines which users homed in the IWF are affiliated to the MCData group is out of scope of the present document.

6.4 Handling of MIME bodies in a SIP message

The IWF shall support MIME bodies in SIP requests and SIP responses according to 3GPP TS 24.282 [82] clause 6.4.

6.5 Confidentiality and Integrity Protection of sensitive XML content

6.5.1 General

6.5.1.1 Applicability and exclusions

The procedures in clause 6.5 apply in general to all procedures described in clause 9, 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 IWF includes XML elements or attributes pertaining to the data specified in clause 4.6 in SIP requests or SIP responses, the IWF shall perform the procedures in clause 6.5.2.3.2, with the exception that when the IWF 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 IWF shall perform the procedures specified in clause 6.5.2.5.

6.5.1.3 Performing integrity protection on an XML body

The IWF shall perform the procedures in clause 6.5.3.3.2 just prior to sending a SIP request or SIP response.

6.5.2 Confidentiality Protection

6.5.2.2 Keys used in confidentiality protection procedures

Confidentiality protection uses an XPK to encrypt the data which is an SPK as specified in clause 4.5. In the case of an IWF as a server sending or receiving to another server this key will be an SPK. An SPK-ID is used to key the SPK. It is assumed that before the procedures in this clause are called, the SPK/SPK-ID are available on the sender and recipient of the encrypted content as described in 3GPP TS 24.282 [82] clause 4.6.

The procedures in clause 6.5.2.3 and 3GPP TS 24.282 [82] clause 6.5.2.4 are used with an XPK equal to the SPK and a XPK-ID equal to the SPK-ID when the IWF sends confidentiality protected content to an MCData server.

6.5.2.3 Procedures for sending confidentiality protected content

6.5.2.3.2 IWF performing the role of an MCData server

If the IWF performing the role of an MCData server determines locally that it needs to confidentially protect content to an MCData server, then sending confidentially protected content between MCData servers is enabled.

When sending confidentiality protected content, the IWF:

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

2) shall perform the procedures in 3GPP TS 24.282 [82] clause 6.5.2.3.3 to confidentiality protect XML elements containing the content described in clause 4.5; and

3) shall perform the procedures in 3GPP TS 24.282 [82] clause 6.5.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in clause 4.5.

If the IWF determines locally that it does not need to confidentiality protect content sent to an MCData server, then sending confidentiality protected content between MCData servers is disabled, and the content is included in XML elements and attributes without encryption.

6.5.2.5 IWF copying received XML content

The following procedure is executed when an IWF 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 IWF:

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 3GPP TS 24.282 [82] clause 6.5.2.4.1:

   a) shall use the keying information described in clause 6.5.2.2 to decrypt the content within the XML element by following the procedures specified in 3GPP TS 24.282 [82] clause 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 clause 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 clause 6.5.2.2 and by following the procedures specified in 3GPP TS 24.282 [82] clause 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 clause 6.5.2.3.2, shall include the decrypted content in the same XML MIME body of the outgoing SIP request; and

3) for each encrypted XML URI attribute in the XML MIME body of the incoming SIP request as determined by 3GPP TS 24.282 [82] clause 6.5.2.4.1:

   a) shall use the keying information described in clause 6.5.2.2 to decrypt the URI value of the XML attribute by following the procedures specified in 3GPP TS 24.282 [82] clause 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 clause 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 clause 6.5.2.2 and by following the procedures specified in 3GPP TS 24.282 [82] clause 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 clause 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

6.5.3.2 Keys used in integrity protection procedures

Integrity protection uses an XPK to sign the data which is an SPK as specified in clause 4.5. In the case of an IWF as a server sending or receiving to another server this key will be an SPK. An SPK-ID is used to key the SPK. It is assumed that before the procedures in clause 6.5.3.3 and 3GPP TS 24.282 [82] clauses 6.5.3.3.1, 6.5.3.3.3 and 6.5.3.4 are called, the SPK/SPK-ID are available on the sender and recipient of the integrity protected content, as described in clause 4.5.

The procedure in clause 6.5.3.3 and 3GPP TS 24.282 [82] clause 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 IWF sends integrity protected content to an MCData server

6.5.3.3 Sending integrity protected content

6.5.3.3.2 Integrity protection at the IWF

The IWF determines locally whether sending integrity protected content from the IWF to an MCData server is enabled.

When sending integrity protected content, the IWF shall use the appropriate keying information specified in clause 6.5.3.2 and shall perform the procedures in 3GPP TS 24.282 [82] clause 6.5.3.3.3 to integrity protect XML MIME bodies.

NOTE: Each XML MIME body is integrity protected separately.

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 [78].

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

The MCData signalling messages sent and received by an IWF are on-network communications and do not include FD.

The MCData data signalling messages may be:

1. SDS SIGNALLING PAYLOAD;
2. SDS NOTIFICATION; or
3. COMMUNICATION RELEASE.

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 the IWF acting on behalf of users homed in the IWF.

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 the IWF acting on behalf of MCData clients

homed in the IWF. The IWF acts as termination point for protection of one-to-one MCData data messages that are sent and received by the IWF acting on behalf of MCData clients homed in the IWF.

The protection of MCData communications between the user homed in the IWF and the IWF acting on behalf of the user homed in the IWF is outside the scope of the present document.

If protection of MCData data signalling messages between the IWF and another MCData function acting in a participating or controlling role is configured, the SPK and the SPK-ID protect the MCData data signalling messages sent and received between the IWF and that MCData function.

The GMK and the GMK-ID are distributed to the IWF acting on behalf of users homed in the IWF using the group document subscription and notification procedure specified in 3GPP TS 24.481 [31].

The PCK and the PCK-ID are generated by the IWF initiating the standalone SDS using signalling control plane.

The SPK and the SPK-ID are configured in the IWF if it is acting as the participating MCData function or if it is acting as the controlling MCData function.

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 [78].

6.6.2 Derivation of master keys for media and media control

On-network MCData services employing the media plane are not supported by the IWF.

6.6.3 Protection of MCData signalling and MCData messages

6.6.3.1 General

The MCData messages may be encrypted and integrity protected between the IWF and the MCData system. When encryption is applied the media shall be encrypted as specified in 3GPP TS 33.180 [78].

Both unprotected MCData messages and MCData messages that are encypted and/or integrity protected can also be end-to-end encrypted for interworking between an MCData client and the IWF.

NOTE: LMR end to end encryption is independent of 3GPP encryption and is out of scope of the present document.

7 Registration and service authorisation

7.1 Server procedures

How users homed in the IWF are registered and service authorized is out of scope of the present document.

8 Affiliation

8.1 General

Clause 8.2 describes the procedures for explicit affiliation by a user homed in the IWF.

Clause 8.3 contains the IWF procedures for handling explicit affiliation by:

- an MCData client to a group homed in the IWF; and
- an IWF on behalf of a user homed in the IWF towards an MCData server owning an MCData group.

Clause 8.3 contains the IWF procedures for handling implicit affiliation by:

- an MCData client to a group homed in the IWF; and
- an IWF on behalf of a user homed in the IWF towards an MCData server owning an MCData group.

The procedures for implicit affiliation in this clause are triggered at the IWF performing the participating role in the following circumstances:

- when generating a SIP MESSAGE request on behalf of a user homed in the IWF to initiate an MCData emergency alert targeted to an MCData group and the user homed in the IWF is not already affiliated to that MCData group.

The procedures for implicit affiliation in this clause are triggered at the IWF performing the controlling role in the following circumstances:

- on receipt of a SIP MESSAGE request from the participating MCData function 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.

Clause 8.4 describes the coding used for explicit affiliation.

8.2 IWF performing the participating role procedures

The IWF acts on behalf of all users homed in the IWF. There are no client procedures specified in the present document and specific client handling within the LMR system is out of scope.

8.3 Server procedures

8.3.1 General

The procedures performed by the IWF in the role of the MCData server consist of:

- procedures of the IWF performing the participating role; and
- procedures of the IWF performing the controlling role.

8.3.2 Procedures of the IWF performing the participating role

8.3.2.1 General

The procedures of the IWF serving users homed in the IWF provide:

- sending affiliation status change towards the MCData server owning an MCData group in clause 8.3.2.6;
- affiliation status retrieval from the MCData server owning an MCData group in clause 8.3.2.7;
- authorizing affiliation status change request in negotiated mode sent to a user homed in the IWF in clause 8.3.2.8;
- affiliation status determination in clause 8.3.2.11;
- affiliation status change by implicit affiliation in clause 8.3.2.12;
- implicit affiliation status change completion in clause 8.3.2.13;
- implicit affiliation status change cancellation in clause 8.3.2.14; and
- automatic affiliation to configured groups in clause 8.3.2.15.

8.3.2.2 Stored information

The IWF maintains information equivalent to that defined in 3GPP TS 24.282 [82] clause 8.3.2.2.

NOTE: The virtual data structure referenced in this clause is for information only. Implementors may choose other means to track affiliation status for users homed in the IWF. References to the elements of this virtual data structure are made in other clauses with the understanding that implementors choosing not to use this virtual data structure will take other appropriate actions.

8.3.2.3 Receiving affiliation status change from a user homed in the IWF procedure

Any notification of the IWF by users homed in the IWF of changes in their affiliation status is out of scope of 3GPP.

8.3.2.4 Receiving subscription to affiliation status procedure

Any notification of users homed in the IWF of their affiliation status is out of scope of 3GPP.

8.3.2.5 Sending notification of change of affiliation status procedure

Any notification of users homed in the IWF of their affiliation status is out of scope of 3GPP.

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 users homed in the IWF served by the same IWF 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 IWF performing the participating role shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51]. In the SIP PUBLISH request, the IWF performing the participating role:

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 [4]), in a P-Asserted-Service header field according to IETF RFC 6050 [9];
4) if sending an affiliation request, shall set the Expires header field according to IETF RFC 3903 [37], 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 [24].

5) if sending a de-affiliation request, shall set the Expires header field according to IETF RFC 3903 [37] to zero;
6) shall include a P-Asserted-Identity header field set to the public service identity of the IWF performing the role of the MCData server according to 3GPP TS 24.229 [4];
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 clause 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 TS 24.282 [82] clause 8.4.1. The IWF performing the role of 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 IWF performing the participating role shall set the <p-id> child element of the <presence> root element to the current p-id.

The IWF performing the participating role shall not include the "expires" attribute in the <affiliation> element.

The IWF performing the participating role shall send the SIP PUBLISH request according to 3GPP TS 24.229 [4].

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 IWF performing the participating role:

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 retrieval from IWF performing the role of the 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 IWF performing the role of the MCData server is not supported in this version of the specification.

In order to discover whether a served user homed in the IWF was successfully affiliated to a handled MCData group in the MCData server owning the handled MCData group, the IWF performing the role of the MCData server shall

generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26].

In the SIP SUBSCRIBE request, the IWF performing the role of 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 IWF performing the role of 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 [4]), in a P-Asserted-Service header field according to IETF RFC 6050 [9];

4) if the IWF performing the role of the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], 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 [24].

5) if the IWF performing the role of the MCData server wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [26], 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 3GPP TS 24.282 [82] clause 8.4.2, indicating the served MCData ID.

In order to re-subscribe or de-subscribe, the IWF performing the role of MCData server shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26]. In the SIP SUBSCRIBE request, the IWF performing the role of the MCData server:

1) if the IWF performing the role of the MCData server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], 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 [24].

2) if the IWF performing the role of the MCData server wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [26], 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 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to 3GPP TS24.282 [82], clause 8.4.1, then the IWF performing the role of 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 clause 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 clause 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 clause 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 authorising affiliation status change request in negotiated mode sent to a user homed in the IWF

Authorising affiliation status change request in negotiated mode sent to a user homed in the IWF is not supported in the present document.

8.3.2.9 Forwarding affiliation status change towards an MCData user procedure

The procedure for forwarding affiliation status change towards an MCData user is not supported in the present specification.

8.3.2.10 Forwarding subscription to affiliation status towards an MCData user procedure

The procedure for forwarding a subscription to affiliation status towards an MCData user is not supported in the present specification.

8.3.2.11 Affiliation status determination

This clause is referenced from other procedures.

If the IWF performing the participating role needs to determine the affiliation status of an user homed in the IWF to an MCData group, the IWF performing the participating role:

1) shall find the user information entry in the list of MCData user information entries described in clause 8.3.2.2 such that the MCData ID of the MCData user information entry is equal to the MCData ID associated with the user homed in the IWF;

   a) if the applicable MCData user information entry cannot be found, then the IWF performing the participating role shall determine that the user homed in the IWF is not affiliated to the MCData group and 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 MCData client ID associated with the user homed in the IWF;

   a) if the applicable MCData client information entry cannot be found, then the IWF performing the participating role shall determine that the user homed in the IWF is not affiliated to the MCData group and skip the rest of the steps; and

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 user homed in the IWF is 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 user homed in the IWF is not 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 user homed in the IWF is not affiliated to the targeted MCData group.

8.3.2.12 Affiliation status change by implicit affiliation

This clause is referenced from other procedures.

Upon determining that implicit affiliation of a user homed in the IWF is required to an MCData group, the IWF performing the participating role:

1) shall determine the MCData client ID of the user homed in the IWF;

2) shall determine the MCData group ID to which the user homed in the IWF is to be affiliated;

3) shall determine the MCData ID associated with the user homed in the IWF;

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 clause 8.3.2.2;

   b) the MCData ID of the MCData user information entry is equal to the MCData ID determined in step 3;

   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 a maximum limit associated by the IWF to the user homed in the IWF, shall, based on MCData service provider policy, reduce the candidate MCData group IDs to that maximum value;

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 maximum limit associated with the user homed in the IWF, 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 clause is referenced from other procedures.

If the IWF performing the participating role has received a SIP 2xx response from the controlling MCData function to a SIP request that had triggered performing the procedures of clause 8.3.2.12, the IWF performing the participating role:

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 clause 8.3.2.12 to "affiliated".

8.3.2.14 Implicit affiliation status change cancellation

This clause is referenced from other procedures.

If the IWF performing the participating role receives a SIP 4xx, 5xx or 6xx response from the controlling MCData function for an implicit affiliation status change operation, the IWF performing the participating role:

1) shall remove the MCData group ID entry added by the procedures of clause 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 associated with the received SIP 4xx, 5xx, or 6xx response;

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 determined in the execution of the procedure in clause 8.3.2.12; 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 associated with the user homed in the IWF.

8.3.2.15 Automatic affiliation to configured groups procedure

This clause is referenced from other procedures.

When the IWF performing the participating role determines that automatic affiliation of a user homed in the IWF to configured groups is needed, the IWF shall perform the procedures specified in clause 8.3.2.6 for the served MCData ID and each configured MCData group ID.

8.3.3 Procedures of the IWF performing the controlling role

8.3.3.1 General

The procedures of the IWF performing the controlling role consist of:

- receiving group affiliation status change procedure;
- receiving subscription to affiliation status procedure;
- sending notification of change of affiliation status procedure;
- implicit affiliation eligibility check procedure; and
- affiliation status change by implicit affiliation procedure.

8.3.3.2 Stored information

The IWF maintains information equivalent to that defined in 3GPP TS 24.282 [82], clause 8.3.3.2.

NOTE: The virtual data structure referenced in this clause is for information only. Implementors can choose other means to track affiliation status for users homed in the IWF. References to the elements of this virtual data structure are made in other clauses with the understanding that implementors choosing not to use this virtual data structure will take other appropriate actions.

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 IWF performing the controlling role 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-identity> element;
3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [4]), in a P-Asserted-Service header field according to IETF RFC 6050 [9];
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 clause 8.4.1;

then the IWF performing the controlling role:

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-identity> 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 is not available to the IWF performing the controlling role, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] 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 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] 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 [4], IETF RFC 3903 [37]. In the SIP 200 (OK) response, the IWF performing the controlling role:
    a) shall set the Expires header field according to IETF RFC 3903 [37], 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 clause 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 clause 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 IWF performing the controlling role 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-identity> element;

3) the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [4]), in a P-Asserted-Service header field according to IETF RFC 6050 [9];

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 8.4.2 indicating the same MCData ID as in the <mcdata-calling-user-identity> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP SUBSCRIBE request;

then the IWF performing the controlling role:

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-identity> 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 is not available to the IWF performing the controlling role, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] 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 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] 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 [4], IETF RFC 6665 [26].

For the duration of the subscription, the IWF shall notify subscriber about changes of the information of the served MCData ID, as described in clause 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 IWF:

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 clause 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 clause 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 IWF shall include the "expires" attribute in the <affiliation> element; and

b) if this procedure is invoked by procedure in clause 8.3.3.3 where the handled p-id was identified, the IWF 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 [4], and IETF RFC 6665 [26] for the subscription created in clause 8.3.3.4. In the SIP NOTIFY request, the IWF shall include the generated application/pidf+xml MIME body indicating per-group affiliation information.

8.3.3.6 Implicit affiliation eligibility check procedure

This clause 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 IWF performing the controlling role to check on the eligibility of the MCData user to be implicitly affiliated to the MCData group, the IWF performing the controlling role:

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-identity> 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 is not available to the IWF performing the controlling role, 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 clause 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 clause 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 IWF performing the controlling role to perform an implicit affiliation to, the IWF performing the controlling role:

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-identity> 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 clause 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; and

5) shall perform the procedures specified in clause 8.3.3.5 for the served MCData group ID.

8.4 Coding

The IWF shall support the coding specified in 3GPP TS 24.282 [82] clause 8.4.

9 IWF 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 as defined in 3GPP TS 24.481 [31], to "false".

If the <mcdata-allow-short-data-service> element under the <list-service> element, in the group document, is set to "false" for an MCData group:

- an IWF shall not send an SDS to the said MCData group; and
- an IWF performing the terminating MCData controlling role shall reject a request to send SDS to the said MCData group.

9.2 On-network SDS

9.2.1 General

On-network SDS employing the media plane is not supported by the IWF in the present document.

9.2.2 Standalone SDS using signalling control plane

9.2.2.1 General

The procedures in the subsequent clauses of clause 9.2.2 are used by the IWF 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 Procedures used by the IWF for users homed in the IWF

9.2.2.2.1 Originating procedures

The IWF shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

The IWF:

1) 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 [89];

   b) an application/vnd.3gpp.mcdata-info+xml MIME body with a <request-type> element set to a value of "one-to-one-sds"; 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 [78]. The IWF:

      i) if necessary, shall determine keying material from the key management server;

NOTE: How the IWF obtains the keying material is out of scope of the present document.

      ii) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

      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 [78];

      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 [78];

      v) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

      vi) shall add the MCData ID associated with the originating user homed in the IWF to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

      vii) shall sign the MIKEY-SAKKE I_MESSAGE using the originating signing key determined by the IWF performing the role of an MCData server 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 [78];

2) if a group standalone SDS message is to be sent:

   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-sds";

      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 associated with the originating user homed in the IWF; and

3) shall generate a standalone SDS message as specified in clause 6.2.2.1.

9.2.2.2.2 Terminating procedures

Upon receipt of an SDS intended for a user homed in the IWF, the IWF processes the message according to the procedures in clause 9.2.2.3.2.

9.2.2.3 IWF performing the participating MCData function procedures

9.2.2.3.1 Originating participating MCData function procedures

If the IWF acting in a participating MCData role determines that it needs to send an SDS message:

1) shall determine the MCData ID of the originating user;

2) shall determine the public service identity of the controlling MCData function associated with the requested SDS message:

   a) if the SDS message to be sent is a group SDS message the public service identity is that of the controlling MCData function associated with the MCData group identity of the destination group; or

   b) if the SDS message to be sent is a one-to-one SDS message the public service identity is that of the controlling MCData function hosting the one-to-one standalone SDS service for the calling user;

NOTE 1: How the IWF determines the public service identity of the controlling MCData function is out of scope of the present document.

3) if unable to identify the controlling MCData function for standalone SDS shall complete any further actions to notify the user homed in the IWF, and shall not continue with any of the remaining steps;

4) shall ensure that the payload size of the message is not larger than a configured value compatible with the MCData service;

NOTE 2: 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).

NOTE 3: The configured value for maximum payload size should not be 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 [50]. How the IWF determines the value to configure is out of scope of the present document.

5) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

6) 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 2) in this clause;

7) shall include MIME bodies in to the outgoing SIP MESSAGE request according to clause 9.2.2.2.1;

8) shall include the MCData ID of the originating user in the <mcdata-calling-user-identity> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

9) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [4]), into the P-Asserted-Service header field of the outgoing SIP MESSAGE request;

10) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public service identity of the IWF; and

11) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

Upon receipt of a SIP response in response to the SIP MESSAGE request in step 11) the IWF completes any further actions needed to handle the response – e.g. notify the user homed in the IWF.

9.2.2.3.2 IWF performing the terminating participating MCData role procedures

Upon receipt of a "SIP MESSAGE request for standalone SDS for terminating participating MCData function", the IWF performing the participating role:

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 IWF 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 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 identify the user homed in the IWF;

3) if the user homed in the IWF does not exist, then the participating IWF may reject the SIP MESSAGE request with a SIP 404 (Not Found) response, and shall skip the remaining steps;

4) if the SIP MESSAGE request contains an application/mikey MIME body containing a MIKEY-SAKKE I_MESSAGE and decryption of the content of the MIME body is to occur at the IWF, then the IWF:

   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 [78];

   b) shall convert the MCData ID to a UID as described in 3GPP TS 33.180 [78];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

   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 clause 4.7 and not continue with rest of the steps in this clause; 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 [78]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78]; and

NOTE: Any trans-encryption between the IWF and the user homed in the IWF is out of scope of the present document.

5) takes any further steps necessary to handle the message – e.g. notify the user homed in the IWF.

If the IWF determines that a SIP 200 (OK) response shall be sent on behalf of a user homed in the IWF in response to the SIP message request, the IWF shall send a SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [4].

If the IWF determines that a SIP 4xx, 5xx or 6xx response shall be sent on behalf of a user homed in the IWF in response to the SIP message request, the IWF shall send said SIP 4xx, 5xx or 6xx response to the controlling MCData function according to 3GPP TS 24.229 [4]:

1) shall determine which Warning header field(s) to place in the SIP response; and

2) shall send the SIP response to the controlling MCData function according to 3GPP TS 24.229 [4].

9.2.2.4 Controlling IWF MCData procedures

9.2.2.4.1 Originating controlling IWF procedures

This clause describes the procedures for sending a SIP MESSAGE from the IWF performing the controlling role and is initiated by the IWF performing the role of a controlling MCData function as a result of an action in clause 9.2.2.4.2 or upon the determination by the IWF performing the controlling role that a SIP MESSAGE is to be sent on behalf of a user homed in the IWF.

The controlling MCData function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

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 [6] 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 [6] in the outgoing SIP MESSAGE request;

4) if the SIP MESSAGE is to be sent as the result of receiving a SIP MESSAGE originated by an MCData client, shall copy the following MIME bodies in the received SIP MESSAGE request into the outgoing SIP MESSAGE request by following the guidelines in clause 6.4; otherwise, if the SIP MESSAGE is to be sent on behalf of a user homed in the IWF, shall create the following MIME bodies in the outgoing SIP MESSAGE request by following the guidelines in clause 306.4 and the procedures in clause 9.2.2.2.1:

   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 SIP MESSAGE is to be sent as the result of receiving a SIP MESSAGE originated by an MCData client, then 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", or if the SIP MESSAGE is to be sent on behalf of a user homed in the IWF and the IWF performing the controlling role determines that the outgoing SIP MESSAGE is associated with a group,

      i) 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 insert its own public service identity 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 [4].

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 IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24]. 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 clause 4.7, and shall not continue with the rest of the steps in this clause;

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 IWF performing the controlling role 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 clause 11.1 indicate that the MCData user is not allowed to send SDS communications due to message size as determined by step 3) of clause 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 clause 4.7, and shall not continue with the rest of the steps in this clause; 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 clause 4.7, 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 clause 9.2.2.4.1, or if the MCData user identified in the <entry> element of the MIME body indicates a user homed in the IWF, the processes used by IWF performing the controlling role to handle the incoming SIP MESSAGE request are out of scope;

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 clause 6.3.3, and shall continue with the remaining steps if the procedures in clause 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 clause 4.7 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-identity> 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 clause 4.7 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 clause 4.7 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 clause 4.7 and shall not continue with the rest of the steps;

   f) if the group SDS procedures in clause 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 clause 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 clause 4.7, and shall not continue with the rest of the steps in this clause;

      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 clause 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 clause 4.7, and shall not continue with the rest of the steps in this clause; and

iii) is not allowed to send SDS communications on this group identity due to message size as determined by step 5) of clause 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 clause 4.7, and shall not continue with the rest of the steps in this clause;

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 clause 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 clause 4.7, and skip the rest of the steps below;

h) shall determine targeted group members for MCData communications by following the procedures in clause 6.3.3;

i) if the procedures in clause 6.3.3 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 clause 4.7, and skip the rest of the steps below; and

j) shall send SIP MESSAGE requests to the targeted MCData group members identified in step h) above by following the procedure in clause 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 [4].

9.2.3 Standalone SDS using media plane

The IWF does not support standalone SDS using the media plane in the present document.

9.2.4 SDS session

The IWF does not support an SDS session in the present document.

9.3 Off-network SDS

Off-network SDS is not applicable to interworking.

10 File Distribution (FD)

File distribution is not supported by the IWF in the present document.

11 Transmission and reception control

11.1 General

How the IWF determines authorisation of a user homed in the IWF to initiate MCData communications is out of scope.

11.2 Auto-receive for File Distribution

File distribution is not supported by the IWF in the present document.

11.3 Accessing list of deferred data group communications

Accessing list of deferred data group communication is associated with file distribution which is not supported by the IWF in the present document.

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.

The IWF acting on behalf of a participant homed in the IWF 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.

12.2 Disposition notifications

12.2.1 IWF performing the MCData participating role

12.2.1.1 Participating IWF procedures

If the IWF performing the MCData participating role decides to send a disposition notification

the IWF shall follow the procedures of clause 12.2.1.2.

Upon receipt of a SIP 202 (Accepted) response in response to the SIP MESSAGE request, the IWF:

1) can perform internal actions to process the response.

Upon receipt of a SIP 200 (OK) response in response to the SIP MESSAGE request, the IWF:

1) can perform internal actions to process the response.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, the IWF:

1) can perform internal actions to process the response.

12.2.1.2 Sending a disposition notification message

The IWF performing the participating role may follow the procedures in this clause 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; or
- indicate to the participating MCData function serving the MCData user that dispostion notification has been prevented for an SDS message intended for users homed in the LMR system.

Before sending a disposition notification the IWF performing the participating role needs to determine:

- the group identity related to an SDS message request received as part of a group communication. The IWF performing the participating role 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 message request; and

- the MCData user targeted for the disposition notification. The IWF performing the participating role 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 message request.

The IWF performing the participating role generates a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

The IWF performing the participating role:

1) shall build the SIP MESSAGE request as specified in clause 6.2.4.1;

2) shall follow the rules specified in clause 6.4 for the handling of MIME bodies in a SIP message when processing the remaining steps in this clause;

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 [20];

4) 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;

5) if sending an SDS notification, shall generate an SDS NOTIFICATION message and include it in the SIP MESSAGE request as specified in clause 6.2.3.1; and

6) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

12.2.1.3 Participating IWF receives disposition notification from a controlling MCData function

Upon receipt of a:

- "SIP MESSAGE request for SDS disposition notification for terminating MCData client ";

The IWF:

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 IWF 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 identify the user homed in the IWF;

3) if the identity of the user homed in the IWF does not exist, then the participating IWF shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response. Otherwise, continue with the rest of the steps; and

4) can perform internal actions to process the message.

If the IWF determines that a SIP 2xx response shall be sent on behalf of a user homed in the IWF in response to the SIP MESSAGE requests, the IWF shall send a SIP 2xx response to the controlling MCData function.

If the IWF determines that a SIP 4xx, 5xx or 6xx response shall be sent on behalf of a user homed in the IWF in response to the SIP MESSAGE request, the IWF shall send the response to the controlling MCData function.

12.2.2 IWF performing the MCData controlling role

When triggered by:

- receipt of a "SIP MESSAGE request for SDS disposition notification for MCData server"; or

- the IWF determining that it shall send an SDS disposition notification

the IWF performing the MCData controlling role:

1) if the IWF has received the SIP MESSAGE;

a) 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 IWF may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24]. Otherwise, continue with the rest of the steps;

b) 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";

c) 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 clause 4.7, and shall not continue with the rest of the steps;

d) shall attempt to correlate the disposition notification to the original SDS request using the values contained in the Conversation ID and Message ID of the SDS NOTIFICATION message contained in the application/vnd.3gpp.mcdata-signalling MIME body of the SIP MESSAGE; and

e) if unable to correlate the disposition notification as determined by step d), 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 clause 4.7, and shall not continue with the rest of the steps;

2) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

3) 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 [6] in the outgoing SIP MESSAGE request;

4) 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 [6] in the outgoing SIP MESSAGE request;

5) shall set the Request-URI to the public service identity of the terminating participating MCData function associated with the MCData user to be invited ;

NOTE 1: How the IWF finds the public service identity of the terminating MCData participating function is out of the scope of the present document.

6) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds";

7) shall copy the MCData ID of the MCData user listed in the MIME resources body of the incoming SIP MESSAGE request, or the MCData ID of the participant homed in the IWF, into the <mcdata-request-uri> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP MESSAGE request;

8) if an 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;

NOTE 2: How the IWF obtains the group document is out scope of the present document.

b) shall verify that the MCData ID contained in the <mcdata-calling-user-identity> element matches to a group member. If there is no match, the IWF 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 clause 4.7, 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 3GPP TS 24.282 [82] clause 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 3: If the aggregated MCData disposition notifications do not fit into one SIP MESSAGE request, then the IWF 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 9; and

iv) if all MCData disposition notifications have been received from all group members shall continue with step 9; 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 9;

9) if an 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;

10) when notifying other users:

a) shall send the SIP MESSAGE request to those users homed in the MCData system according to rules and procedures of 3GPP TS 24.229 [4]; and

11) when acknowledging the triggering event:

a) shall generate a SIP 202 (Accepted) response in response to any

- "SIP MESSAGE request for SDS disposition notification for MCData server".

12.3 On-network disposition notifications

13 Communication Release

The IWF shall handle communication release with the MCData system by behaving as a peer MCData server towards the MCData system as specified in 3GPP TS 24.282 [82] clauses 13.2.2.2.3, 13.2.2.2.4, 13.2.3 and 13.2.4.

Communication release in the LMR system is out of scope of 3GPP.

14 Enhanced Status (ES)

14.1 General

14.2 On-network ES

14.2.1 Void

14.2.2 IWF performing the participating MCData role procedures

14.2.2.1 Originating participating MCData function procedures

If the IWF performing the participating MCData role determines that an Enhanced Status message needs to be sent on behalf of a participant homed in the IWF then it:

1) shall use the "id" attribute of the selected operation value from <mcdata-enhanced-status-operational-values> element under <list-service> element as defined in 3GPP TS 24.481 [31], to generate a group standalone SDS message using the procedures described in clause 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 IWF performing the participating MCData role should follow the procedure described in clause 9.2.2.3.2.

14.2.3 IWF performing the controlling MCData role procedures

14.2.3.1 Originating controlling MCData function procedures

If the IWF performing the controlling MCData role determines that an Enhanced Status message needs to be sent on behalf of a participant homed in the IWF then it follows the procedure described in clause 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 IWF performing the controlling MCData role should follow the procedure described in clause 9.2.2.4.2.

15 Message Formats

15.1 IWF message functional definitions and contents

15.1.1 General

The following clauses describe the MCData message functional definitions and contents. Each message consists 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 [81].

15.1.2 SDS SIGNALLING PAYLOAD message

15.1.2.1 Message definition

This message is sent by the MCData client towards a participant homed in the IWF via the network and from the IWF towards MCData clients 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: MCData server to IWF and IWF to MCData server

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 3GPP TS 24.282 [82] clause 15.2.8	M	V	5
	Conversation ID	Conversation ID 3GPP TS 24.282 [82] clause 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
21	InReplyTo message ID	InReplyTo message ID 3GPP TS 24.282 [82] clause 15.2.11	O	TV	17
22	Application ID	Application ID 3GPP TS 24.282 [82] clause 15.2.7	O	TV	2
8-	SDS disposition request type	SDS disposition request type 3GPP TS 24.282 [82] clause 15.2.3	O	TV	1
7D	Extended application ID	Extended application ID 3GPP TS 24.282 [82] clause 15.2.24	O	TLV-E	3-x

15.1.3 FD SIGNALLING PAYLOAD message

The IWF does not support the FD SIGNALLING PAYLOAD message.

15.1.4 DATA PAYLOAD message

15.1.4.1 Message definition

This message is sent by the MCData client towards a participant homed in the IWF via the network and from the IWF towards MCData clients when sending an SDS 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: MCData server to IWF and IWF to MCData server

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 3GPP TS 24.282 [82] clause 15.2.12	M	V	1
7A	Security parameters and Payload	MCData Protected Payload message 3GPP TS 33.180 [78]	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 clause 15.2.13.

15.1.5 SDS NOTIFICATION message

15.1.5.1 Message definition

This message is sent by the MCData client towards a participant homed in the IWF via the network and from the IWF towards MCData clients to share SDS disposition information. For the contents of the message see Table 15.1.5.1-1.

Message type: SDS NOTIFICATION

Direction: MCData server to IWF and IWF to MCData server

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 3GPP TS 24.282 [82] clause 15.2.5	M	V	1
	Date and time	Date and time 3GPP TS 24.282 [82] clause 15.2.8	M	V	5
	Conversation ID	Conversation ID 3GPP TS 24.282 [82] clause 15.2.9	M	V	16
	Message ID	Message ID 15.2.10	M	V	16
22	Application ID	Application ID 3GPP TS 24.282 [82] clause 15.2.7	O	TV	2
7D	Extended application ID	Extended application ID 3GPP TS 24.282 [82] clause 15.2.24	O	TLV-E	3-x

15.1.6 FD NOTIFICATION message

The IWF does not support the FD NOTIFICATION message.

15.1.7 SDS OFF-NETWORK MESSAGE

The IWF does not support the SDS OFF-NETWORK MESSAGE.

15.1.8 SDS OFF-NETWORK NOTIFICATION message

The IWF does not support the SDS OFF-NETWORK NOTIFICATION message.

15.1.9 FD NETWORK NOTIFICATION message

The IWF does not support the FD NETWORK NOTIFICATION message.

15.1.10 COMMUNICATION RELEASE message

15.1.10.1 Message definition

In this clause the term "MCData server" can apply to an MCData server or an IWF performing the role of an MCData server.

This message is sent by the MCData server to an MCData client or a participant homed in the IWF to indicate about an intention to release the MCData communication. This message is also sent by the MCData client or the IWF to the MCData server to request extension for the MCData communication. The MCData server responds back to the request using this message. For the contents of the message see Table 15.1.10.1-1.

Message type: COMMUNICATION RELEASE

Direction: MCData server to the IWF and IWF to MCData 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 3GPP TS 24.282 [82] clause 15.2.20	M	V	1
B-	Data query type	Data query type 3GPP TS 24.282 [82] clause 15.2.19	O	TV	1
C-	Extension response type	Extension response type 3GPP TS 24.282 [82] clause 15.2.21	O	TV	1

15.1.11 DEFERRED DATA REQUEST message

The IWF does not support the DEFERRED DATA REQUEST message.

15.1.12 DEFERRED DATA RESPONSE message

The IWF does not support the DEFERRED DATA RESPONSE message.

15.1.13 FD HTTP TERMINATION

The IWF does not support the FD HTTP TERMINATION message.

15.2 General message format and information elements coding

15.2.1 General

The message format and bit ordering used within the present document are as defined in clause 15.2.1 of 3GPP TS 24.282 [82].

15.2.2 Message type

The purpose of the Message type information element is to identify the type of the message.

The IWF shall support the following Message types as defined in clause 15.2.2 of 3GPP TS 24.282 [82]:

- SDS SIGNALING PAYLOAD;
- DATA PAYLOAD;
- SDS NOTIFICATION;
- COMMUNICATION RELEASE.

15.2.3 Void

15.2.4 Void

15.2.5 Void

15.2.6 Void

15.2.7 Void

15.2.8 Void

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.

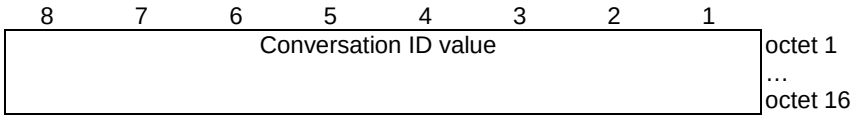

Figure 15.2.9-1: Conversation ID value

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 [67] with the exception of the following designated value shown in Table 15.2.9-2, denoted "UNKNOWN CONVERSATION".

Table 15.2.9-2: Conversation ID value "UNKNOWN CONVERSATION"

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	octet 1
0	0	0	0	0	0	0	0	…
0	0	0	0	0	0	0	0	octet 16

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.

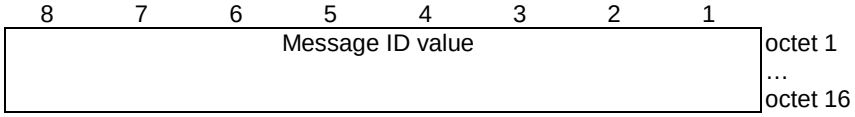

Figure 15.2.10-1: Message ID value

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 [67] with the exception of the designated value "UNKNOWN ORIGINATING MESSAGE ID" and "LMR MESSAGE ID" shown in Tables 15.2.10-2 and 15.2.10-3, where 'x' represents a variable value.

Table 15.2.10-2: Message ID value "UNKNOWN ORIGINATING MESSAGE ID"

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	octet 1
0	0	0	0	0	0	0	0	…
0	0	0	0	0	0	0	0	octet 16

Table 15.2.10-3: Message ID value "LMR MESSAGE ID"

8	7	6	5	4	3	2	1	
1	1	1	1	1	1	1	1	octet 1
1	1	1	1	1	1	1	1	…
1	1	1	1	1	1	1	1	octet 15
x	x	x	x	x	x	x	x	octet 16

15.2.11 Void

15.2.12 Void

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, Table 15.2.13-3 and Table 15.2.13-4.

The Payload information element is a type 6 information element.

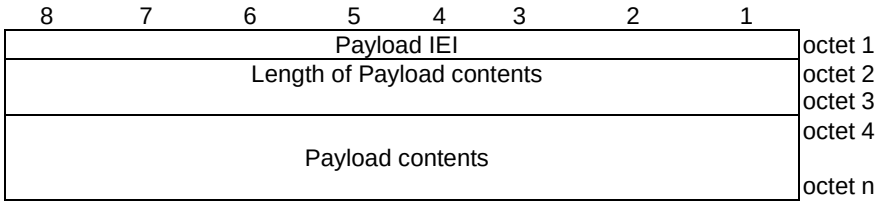

Figure 15.2.13-1: Payload information element

Table 15.2.13-1: Payload contents

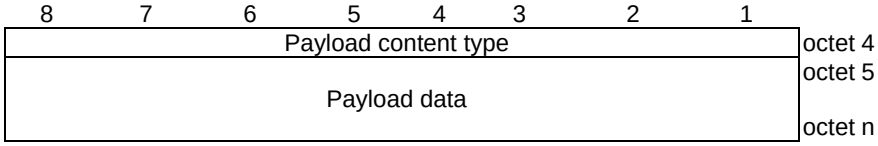

Table 15.2.13-2: Payload content type

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	LMR MESSAGE
All other values are reserved.	
NOTE: The LMR MESSAGE format identifies the payload content as a native LMR format message for transport between LMR aware endpoints as per 3GPP TS 23.283 [80]	

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 [86]. 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. If the Payload content type is "LMR MESSAGE" then the first octet of the payload data is encoded as specified in Table 15.2.13-4.

Table 15.2.13-4: First octet of Payload data for LMR MESSAGE Payload content type

Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	P25
0	0	0	0	0	0	1	0	TETRA
All other values are reserved.								

16 Media plane

No media plane procedures are specified in the present document.

17 Handling of Interworking Security Data messages

17.1 IWF

17.1.1 IWF originates Interworking Security Data message

Upon deciding to send an Interworking Security Data message, the IWF:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

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 [6];

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 [6];

4) 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

5) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" (coded as specified in 3GPP TS 24.229 [4]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [9];

6) shall set the Request-URI to the address of the terminating participating function associated with the MC service ID of the targeted MC service user;

7) shall include a P-Asserted-Identity header field set to the public service identity of the IWF;

8) shall include an application/vnd.3gpp.interworking-data MIME body with the Interworking Security Data message payload as defined in clause 17.2.1;

9) if a security context between the MCData client and the IWF needs to be established and the security context does not exist or if the existing security context has expired, procedures in clause 11.2.2 in 3GPP TS 33.180 [78] shall be followed; and

10) send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

17.1.2 IWF receives Interworking Security Data message

Upon receiving a "SIP MESSAGE request for Interworking Security Data message for participating function", the actions performed by the IWF are out of scope of the present document. The received message, described in clause 17.2, contains an opaque payload, the contents of which are out out of scope of the present document.

17.2 Interworking Security Data message payload

17.2.1 Message definition

This clause specifies the payload to be used when sending an Interworking Security Data message between the IWF and MCData clients. The Interworking Security Data (InterSD) message is defined as a MONP message.

Message type: InterSD-MESSAGE

Direction: IWF to MCData client, MCData client to IWF

Table 17.2.1-1: Interworking Security Data message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS signalling payload message identity	Message type 3GPP TS 24.282 [82]	M	V	1
	External network type	17.2.2	M	V	1
7D	URI of LMR key management functional entity	URI encoded as specified in IETF RFC 3986 [46]	O	TLV-E	3-x
78	Payload	3GPP TS 24.282 [82], clause 15.2.13 with Payload content type set to 'BINARY'	O	TLV-E	3-x

17.2.2 External network type

The purpose of the external network type information element is to identify the type of the network represented by the IWF.

The value part of the external network type information element is coded as shown in Table 17.2.2-1.

The external network type information element is a type 3 information element with a length of 1 octet.

Table 17.2.2-1: External network type

Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	P25
0	0	0	0	0	0	1	0	TETRA
All other values are reserved.								

Annex A (informative): Signalling flows

Annex B (normative): Timers

Annex C (normative): Counters

Annex D (normative): XML schemas

D.1 XML schema for transporting MCData identities and general services information

D.1.1 General

This clause defines XML schema and MIME type for transporting MCData identities and general services information. The XML schema elements and behaviour defined in this clause extend those in 3GPP TS 24.282 [82] or other 3GPP technical specifications as noted.

D.1.2 XML schema

This schema is as described in 3GPP TS 24.282 [82] Annex D.1.2.

D.1.3 Semantic

The semantic is as described in 3GPP TS 24.282 [82] Annex D.1.3 with the following modifications:

If the <mcdatainfo> contains the <mcdata-Params> element then:

1) 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 "notify" when the controlling MCData function needs to send a notification to the MCData client.

2) the <anyExt> element of the <mcdata-Params> element can be included with the following element in addition to those specified in 3GPP TS 24.282 [82] Annex D.1.3:

   a) a <request-type> of type "xs:string": set to value of "Interworking Security Data message" when requesting an Interworking Security Data message.

Annex E (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-05						Initial version	0.0.1
2019-10						Implementation of the following P-CR from CT1#120: C1-196237, C1-196247, C1-196250, C1-196251, C1-196252, C1-196253, C1-196633, C1-196636, C1-196637, C1-196638, C1-196639, C1-196643, C1-196644, C1-196645, C1-196647, C1-196648, C1-196670, C1-196673, C1-196676, C1-196820, C1-196821, C1-196822, C1-196824, C1-196825, C1-196826, C1-196828, C1-196830, C1-196831, C1-196868, C1-196869, C1-196871	0.1.0
2019-11						Implementation of the following P-CR from CT1#121: C1-198514	0.2.0
2019-12	CT-86	CP-193158				Presentation for information at TSG CT	1.0.0
2019-12	CT#86	CP-193291				A title updated	1.0.1
2020-03						Implementation of the following pCRs from CT1#122e: C1-200369, C1-200370, C1-200371,C1-200912, C1-200913, C1-200946, C1-200948	1.1.0
2020-03	CT-87e	CP-200175				Presentation for approval at TSG CT	2.0.0
2020-03	CT-87e					Version 16.0.0 created after approval	16.0.0
2020-06	CT-88e	CP-201120	0001	1	D	Editorial corrections	16.1.0
2020-09	CT-89e	CP-202161	0002	1	F	Introduction of text for Scope clause	16.2.0
2020-12	CT-90e	CP-203195	0006	1	F	Identifying LMR type in MCData SDS interworking	16.3.0
2022-03	CT-90e	CP-220230	0016	1	F	Correction to Disposition Notification handling when LMR system temporarily disables Disposition Notification	16.4.0
2022-06	CT-100	CP-231254	0020	1	F	Warning codes & warning text to handle interworking application mismatch	16.5.0

History

Document history		
V16.1.0	August 2020	Publication
V16.2.0	November 2020	Publication
V16.3.0	January 2021	Publication
V16.4.0	April 2022	Publication
V16.5.0	July 2023	Publication