**3GPP TSG-CT1 Meeting #134-e *C1-221xyz***

**Online, , 17th Feb 2022 - 25th Feb 2022**  **(was C1-221448)**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **24.282** | **CR** | **0311** | **rev** | **1** | **Current version:** | **16.8.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Corrections for multiple IPConn communications |
|  |  |
| ***Source to WG:*** | Kontron Transportation France |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | MONASTERY2 |  | ***Date:*** | 2022-02-09 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-16 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The current specification for MCDatat IP connectivity does not include the necessary details to handle multiple simultanious IP connectivity communications. This CR adds the required changes. |
|  |  |
| ***Summary of change:*** | * Add to 20.2.2 how to determine key for the GRE tunnel and include it in the SIP 200 (OK) response
* Add to 20.3.1 how to determine key for the outgoing leg of the GRE tunnel and include it in the SIP 200 (OK) response
* Add to 20.3.2 how to determine key for the outgoing leg of the GRE tunnel and include it in the SIP 200 (OK) response
* Add to 20.4.2 how to determine key for the outgoing leg of the GRE tunnel and include it in the SIP 200 (OK) response
* Add new definition for gre-tunnel-key element to XML schema
* Add gre-tunnel-key element to semantics
 |
|  |  |
| ***Consequences if not approved:*** | MCData IP connectivity will not be able to handle multiple simultanious communications |
|  |  |
| ***Clauses affected:*** | 20.1.1, 20.1.2, 20.1.3, 20.2.2, 20.3.1, 20.3.2, 20.4.2, D.1.2, D.1.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First Change \* \* \* \*

### 20.1.1 MC Data client SDP offer/answer generation

When a MCData client decides to establish an IP Connectivity session, or is answering an IP Connectivity request the MCData client shall include an SDP offer/answer according to subclause 6.1.2 of 3GPP TS 24.229 [5] with the following clarifications:

1) shall set the IP address of the MC Data client to the IP address to be used in the IP Connectivity session; and

NOTE: The MC service operator policy determines if the MC Data client should use an already assigned IP address or should request a new IP address following the procedures defined in 3GPP TS 24.301 [43].

2) shall add a zero port number value to the media descriptions of the SDP offer, in order to inform the network entities that media resources are not requested for the session.

### 20.1.2 MC Data participating server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data participating function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the participating MC Data function, if required; and

NOTE: Requirements can exist for the MC Data server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) shall ensure the port number is zero.

### 20.1.3 MC Data controlling server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data controlling function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the controlling MC Data function, if required; and

NOTE: Requirements can exist for the MC Data controlling server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) shall ensure the port number is zero.

### 20.1.2 MC Data participating server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data participating function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the participating MC Data function, if required; and

NOTE: Requirements can exist for the MC Data server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) shall ensure the port number is zero

### 20.1.3 MC Data controlling server SDP offer/answer generation

The SDP offer/answer is generated based on the received SDP offer/answer. The SDP offer/answer generated by the MC Data controlling function:

1) shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the controlling MC Data function, if required; and

NOTE: Requirements can exist for the MC Data controlling server to be in the path of the data exchange between authorized MC Data users in order to limit the exchange in terms of volume or time limits.

2) shall ensure the port number is zero.

\* \* \* Next Change \* \* \* \*

### 20.2.2 MCData client terminating procedures

Upon receipt of an "initial SIP INVITE request for IP Connectivity session for terminating MCData client"request, the MCData client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [5] with the clarifications below.

The MCData client:

1) may reject the SIP INVITE request if either of the following conditions are met:

a) MCData client does not have enough resources to handle the IP Connectivity session; or

b) any other reason outside the scope of this specification;

and skip the rest of the steps after step 2;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCData function either with appropriate reject code as specified in 3GPP TS 24.229 [5] and warning texts as specified in subclause 4.9 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

3) shall interact with the MCData user or user application providing the MCData ID of the inviting MCData user;

3A) may display to the MCData user the functional alias of the inviting MCData user, if provided;

4) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [5];

5) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

6) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [38]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

7) shall include the g.3gpp.mcdata.ipconn media feature tag in the Contact header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" in the Contact header field of the SIP 200 (OK) response;

9) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.1;

10) shall include in the SIP 200 (OK) response an application/vnd.3gpp.mcdata-info+xml MIME body as specified in clause D.1 with the <mcdatainfo> element containing the <mcdata-Params> element with the <anyExt> element containing the <gre-tunnel-key> element set to a value that is not already used by any other gre tunnel existing between the local IP address defined in clause 20.1.1 and the IP address received in the incoming SDP offer; and

11) shall send the SIP 200 (OK) response towards the MCData server according to rules and procedures of 3GPP TS 24.229 [5].

On receipt of an SIP ACK message to the sent SIP 200 (OK) message, the MCData client shall:

1) shall interact with MC Data user or user application.

\* \* \* Next Change \* \* \* \*

### 20.3.1 Originating participating MCData function procedures

Upon receipt of a "SIP INVITE request for IP Connectivity session for originating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall determine the MCData ID of the calling user from the public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

4) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is:

a) set to a value of "one-to-one-ipconn", shall determine the public service identity of the controlling MCData function hosting the one-to-one IP Connectivity service for the calling user.

5) if unable to identify the controlling MCData function for IP Connectivity session, shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.9, and shall not continue with any of the remaining steps;

6) shall determine whether the MCData user identified by the MCData ID is authorised for MCData communications by following the procedures in subclause 11.1;

7) if the procedures in subclause 11.1 indicate that the user identified by the MCData ID is not allowed to initiate MCData communications, shall reject the "SIP INVITE request for IP Connectivity session for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in subclause 4.9, and shall not continue with the rest of the steps in this subclause;

8) shall generate a SIP INVITE request in accordance with 3GPP TS 24.229 [5];

9) shall include the option tag "timer" in the Supported header field;

10) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

11) shall set the Request-URI of the outgoing SIP INVITE request to the public service identity of the controlling MCData function as determined by step 4) in this subclause;

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

13) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn" (coded as specified in 3GPP TS 24.229 [5]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

14) shall set the P-Asserted-Identity in the outgoing SIP INVITE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP INVITE request;

15) shall include an SDP offer according to 3GPP TS 24.229 [5] based on the clause  20.1.2;

16) if the received SIP INVITE request contains an application/vnd.3gpp.mcdata-info+xml MIME body that contains a <functional-alias-URI> element, shall check if the status of the functional alias is activated for the MCData ID. If the functional alias status is activated, then the participating MCData function shall set the <functional-alias-URI> element of the application/vnd.3gpp.mcdata-info+xml MIME body in the outgoing SIP INVITE request to the received value, otherwise shall not include a <functional-alias-URI> element; and

17) shall send the SIP INVITE request as specified to 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the SIP INVITE request in step 16):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include the following in the Contact header field:

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

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

c) the isfocus media feature tag;

5) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

6) shall include an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP 200 (OK) response;

7) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response;

7a)shall set the <gre-tunnel-key> element contained in the <anyExt> element of the <mcdata-Params> element of the <mcdatainfo> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body contained in the incoming SIP response to a value that is not already used by any other gre tunnel existing between the local IP address to be used and the IP address received in the incoming SDP offer;

8) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15];

10) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [5];and

11) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP INVITE request in step 15) the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the MCData client according to 3GPP TS 24.229 [5].

### 20.3.2 Terminating participating MCData function procedures

Upon receipt of a "SIP INVITE request for IP Connectivity session for terminating participating MCData function", the participating MCData function:

1) if unable to process the request, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCData function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) shall use the MCData ID present in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

4) if the binding between the MCData ID and public user identity of the terminating MCData user does not exist, then the participating MCData function shall reject the SIP INVITE request with a SIP 404 (Not Found) response, and shall not continue with the rest of the steps;

5) shall generate a SIP INVITE request accordance with 3GPP TS 24.229 [5];

6) should include the Session-Expires header field according to IETF RFC 4028 [38]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

7) shall include the option tag "timer" in the Supported header field;

8) shall include the following in the Contact header field:

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

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

c) the isfocus media feature tag;

d) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the incoming SIP INVITE request; and

e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

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

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

11) shall populate the outgoing SIP INVITE request with the MIME bodies that were present in the incoming SIP INVITE request;

12) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

13) shall include in the SIP INVITE request an SDP offer according to 3GPP TS 24.229 [5] with the clarifications given in subclause 20.1.2; and

14) shall send the SIP INVITE request as specified in 3GPP TS 24.229 [5].

Upon receipt of a SIP 200 (OK) response in response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

4) shall include the following in the Contact header field:

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

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

c) an MCData session identity mapped to the MCData session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCData function;

5) if the incoming SIP response contained an application/vnd.3gpp.mcdata-info+xml MIME body, shall copy the application/vnd.3gpp.mcdata-info+xml MIME body to the outgoing SIP 200 (OK) response;

5a) shall set the <gre-tunnel-key> element contained in the <anyExt> element of the <mcdata-Params> element of the <mcdatainfo> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body contained in the incoming SIP response to a value that is not already used by any other gre tunnel existing between the local IP address to be used and the IP address received in the incoming SDP offer;

6) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

7) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

8) shall interact with the media plane as specified in 3GPP TS 24.582 [15]; and

9) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [5].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCData function:

1) shall generate a SIP response according to 3GPP TS 24.229 [5];

2) shall include Warning header field(s) that were received in the incoming SIP response; and

3) shall forward the SIP response to the controlling MCData function according to 3GPP TS 24.229 [5].

\* \* \* Next Change \* \* \* \*

### 20.4.2 Terminating procedures

In the procedures in this subclause:

1) MCData ID in an incoming SIP INVITE request refers to the MCData ID of the originating user from the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP INVITE request;

2) MCData ID in an outgoing SIP INVITE request refers to the MCData ID of the called user in the <mcdata-request-uri> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the outgoing SIP INVITE request;

Upon receipt of a "SIP INVITE request for controlling MCData function for IP Connectivity session", the controlling MCData function:

1) if unable to process the request may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [4] and skip the rest of the steps;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

a) an Accept-Contact header field does not include the g.3gpp.mcdata.ipconn media feature tag; or

b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.ipconn";

3) shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported;

4) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [38];

5) if the <request-type> element in the application/vnd.3gpp.mcdata-info+xml MIME body of the SIP INVITE request is set to a value of "one-to-one-ipconn" and the SIP INVITE request:

a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "227 unable to determine targeted user for one-to-one IP Connectivity" in a Warning header field as specified in subclause 4.9, and skip the rest of the steps below;

b) contains an application/resource-lists MIME body with exactly one <entry> element, shall invite the MCData user identified by the <entry> element of the MIME body, as specified in subclause 20.4.1; and

c) can interact with the media plane, in case routing or transmission control is necessary.

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 20.4.1 and if the MCData ID in the SIP 200 (OK) response matches to the MCData ID in the corresponding SIP INVITE request. the controlling MCData function:

1) shall generate SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [5];

2) shall include the option tag "timer" in a Require header field;

3) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [38], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCData function;

5) shall include a SIP URI for the MCData session identity in the Contact header field identifying the MCData session at the controlling MCData function;

6) shall include the following in the Contact header field:

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

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

c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 20.1.2;

8a) shall set the <gre-tunnel-key> element contained in the <anyExt> element of the <mcdata-Params> element of the <mcdatainfo> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body contained in the incoming SIP response to a value that is not already used by any other gre tunnel existing between the local IP address to be used and the IP address received in the incoming SDP;

9) shall interact with the media plane as specified in 3GPP TS 24.582 [15]; and

10) shall send a SIP 200 (OK) response to the inviting MCData client according to 3GPP TS 24.229 [5].

\* \* \* Next Change \* \* \* \*

## D.1.2 XML schema

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

<xs:schema

 xmlns:xs="http://www.w3.org/2001/XMLSchema"

 targetNamespace="urn:3gpp:ns:mcdataInfo:1.0"

 xmlns:mcdatainfo="urn:3gpp:ns:mcdataInfo:1.0"

 elementFormDefault="qualified"

 attributeFormDefault="unqualified"

 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

 <xs:import namespace="http://www.w3.org/2001/04/xmlenc#" schemaLocation="http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd"/>

 <!-- root XML element -->

 <xs:element name="mcdatainfo" type="mcdatainfo:mcdatainfo-Type" id="info"/>

 <xs:complexType name="mcdatainfo-Type">

 <xs:sequence>

 <xs:element name="mcdata-Params" type="mcdatainfo:mcdata-ParamsType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>

 </xs:sequence>

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

 </xs:complexType>

 <xs:complexType name="mcdata-ParamsType">

 <xs:sequence>

 <xs:element name="mcdata-access-token" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="request-type" type="xs:string" minOccurs="0"/>

 <xs:element name="mcdata-request-uri" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="mcdata-calling-user-id" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="mcdata-called-party-id" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="mcdata-calling-group-id" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="alert-ind" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="originated-by" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="mcdata-client-id" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:element name="mcdata-controller-psi" type="mcdatainfo:contentType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>

 </xs:sequence>

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

 </xs:complexType>

<!-- anyExt elements for MCData-Params-->

 <xs:element name="pre-established-session-ind" type="xs:boolean"/>

 <xs:element name="mcdata-communication-state" type="mcdatainfo:mcdataCommunicationStateType"/>

 <xs:simpleType name="mcdataCommunicationStateType">

 <xs:restriction base="xs:string">

 <xs:enumeration value="establish-request"/>

 <xs:enumeration value="establish-success"/>

 <xs:enumeration value="establish-fail"/>

 <xs:enumeration value="terminate-request"/>

 <xs:enumeration value="terminated"/>

 </xs:restriction>

 </xs:simpleType>

 <xs:element name="emergency-ind" type="xs:boolean"/>

 <xs:element name="alert-ind-rcvd" type="xs:boolean"/>

 <xs:element name="mc-org" type="xs:string"/>

 <xs:element name="functional-alias-URI" type="mcdatainfo:contentType"/>

 <xs:element name="multiple-devices-ind" type="mcdatainfo:contentType"/>

 <xs:element name="gre-tunnel-key" type="xs:unsignedInt"/>

 <xs:simpleType name="protectionType">

 <xs:restriction base="xs:string">

 <xs:enumeration value="Normal"/>

 <xs:enumeration value="Encrypted"/>

 </xs:restriction>

 </xs:simpleType>

 <xs:complexType name="contentType">

 <xs:choice>

 <xs:element name="mcdataURI" type="xs:anyURI"/>

 <xs:element name="mcdataString" type="xs:string"/>

 <xs:element name="mcdataBoolean" type="xs:boolean"/>

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

 <xs:element name="anyExt" type="mcdatainfo:anyExtType" minOccurs="0"/>

 </xs:choice>

 <xs:attribute name="type" type="mcdatainfo:protectionType"/>

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

 </xs:complexType>

 <xs:complexType name="anyExtType">

 <xs:sequence>

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

 </xs:sequence>

 </xs:complexType>

</xs:schema>

## D.1.3 Semantic

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

The <mcdatainfo> element is the root element of the XML document. The <mcdatainfo> element can contain subelements.

NOTE 1: The subelements of the <mcdata-info> are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <mcdata-info> element

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

1) the <mcdata-access-token>, <mcdata-request-uri>, <mcdata-controller-psi>, <mcdata-calling-user-id>, <mcdata-called-party-id>, <mcdata-calling-group-id>, <alert-ind>, <originated-by>, <mcdata-client-id>, <functional-alias-URI> and <multiple-devices-ind> elements can be included with encrypted content;

2) for each element in 1) that is included with content that is not encrypted:

a) the element has the "type" attribute set to "Normal";

b) if the element is the <mcdata-request-uri>, <mcdata-calling-user-id>, <mcdata-called-party-id>, <mcdata-calling-group-id>, <originated-by> or <functional-alias-URI> then the <mcdataURI> element is included;

c) if the element is the <mcdata-access-token> or <mcdata-client-id>, then the <mcdataString> element is included; and

d) if the element is <alert-ind> or <multiple-devices-ind> then the <mcdataBoolean> element is included;

3) for each element in 1) that is included with content that is encrypted:

a) the element has the "type" attribute set to "Encrypted";

b) the <xenc:EncryptedData> element from the "[http://www.w3.org/2001/04/xmlenc#](http://www.w3.org/2001/04/xmlenc)" namespace is included and:

i) can have a "Type" attribute can be included with a value of "<http://www.w3.org/2001/04/xmlenc#Content>";

ii) can include an <EncryptionMethod> element with the "Algorithm" attribute set to value of "http://www.w3.org/2009/xmlenc11#aes128-gcm";

iii) can include a <KeyInfo> element with a <KeyName> element containing the base 64 encoded XPK-ID; and

iv) includes a <CipherData> element with a <CipherValue> element containing the encrypted data.

NOTE 2: When the optional attributes and elements are not included within the <xenc:EncryptedData> element, the information they contain is known to sender and the receiver by other means.

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

1) the <mcdata-access-token> can be included with the access token received during authentication procedure as described in 3GPP TS 24.382 [49];

2) the <request-type> can be included with:

a) a value of "one-to-one-sds" to indicate that the MCData client wants to initiate a one-to-one SDS request;

b) a value of "group-sds" to indicate the MCData client wants to initiate a group SDS request;

c) a value of "one-to-one-fd" to indicate that the MCData client wants to initiate a one-to-one FD request;

d) a value of "group-fd" to indicate that the MCData client wants to initiate a group FD request;

e) a value of "msf-disc-req" to indicate that the MCData client wishes to discover the absoluteURI of the media storage function for HTTP requests;

f) a value of "msf-disc-res" when the participating MCData function sends the absolute URI to the MCData client;

g) a value of "notify" when the controlling MCData function needs to send a notification to the MCData client;

h) a value of "one-to-one-sds-session" to indicate that the MCData client wants to initiate a one-to-one SDS session;

i) a value of "group-sds-session" to indicate the MCData client wants to initiate a group SDS session; or

j) a value of "functional-alias-status-determination" when a client initiates a subscription request to FA status;

3) the <mcdata-request-uri> can be included with an MCData group ID;

4) the <mcdata-calling-user-id> can be included, set to MCData ID of the originating user;

5) the <mcdata-called-party-id> can be included, set to the MCData ID of the terminating user;

6) the <mcdata-calling-group-id> can be included to indicate the MCData group identity to the terminating user;

7) the <alert-ind> can be:

a) set to "true" to indicate that an alert to be sent; or

b) set to "false" to indicate that an alert to is be cancelled;

8) the <originated-by> can be included, set to the MCData ID of the originating user of an MCData emergency alert when being cancelled by another authorised MCDATA user;

9) the <mcdata-client-id> can be included, set to the MCData client ID of the MCData client that originated a SIP INVITE request, SIP REFER request, SIP REGISTER request, SIP PUBLISH request or SIP MESSAGE request; and

10) the <mcdata-controller-psi> can be included, set to the PSI of the controlling MCData function that handled the one-to-one or group MCData data request; and

11) the <anyExt> can be included with the following elements:

a) a <pre-established-session-ind> element:

i) set to the value "true" by the MCData client in a pre-established session setup request to indicate to the MCData participating function about initiation of a pre-established session.

b) an <mcdata-communication-state> element can be included to indicate state of MCData communication within pre-established session. The <mcdata-communication-state> can be set to:

i) the value "establish-request" by the MCData participating function to indicate to the MCData client about an MCData communication establishment request within pre-established session;

ii) the value "establish-success" by the MCData participating function or MCData client to indicate that the MCData communication is established successfully;

iii) the value "establish-fail" by the MCData participating function or the MCData client to indicate that the MCData communication establishment is failed or rejected;

iv) the value "terminate-request" by the MCData participating function to indicate to the MCData client about an MCData communication termination request within a pre-established session; and

v) the value "terminated" by the MCData participating function or the MCData client to indicate that the MCData communication is terminated.

c) an <emergency-ind> element can be included and set to:

i) "true" to indicate that the communication that the MCData client is initiating is an emergency MCData communication; or

ii) "false" to indicate that the MCData client is cancelling an emergency MCData communication (i.e. converting it back to a non-emergency communication);

d) an <alert-ind-rcvd> element:

i) may be set to “true" and included in a SIP MESSAGE to indicate that the emergency alert or cancellation was received successfully;

e) an <mc-org> element may be:

i) set to the MCData user's Mission Critical Organization and included in an emergency alert sent by the MCData server to terminating MCData clients;

f) a <functional-alias-URI> element set to the value of the functional alias that is used together with the "mcdata-calling-user-id"; and

g) a <multiple-devices-ind> element can be included and set to:

i) "true" to indicate to the client that multiple clients are registered for the MCData user; or

ii) "false" to indicate to the client that no other clients are registered for the MCData user;

h) a <gre-tunnel-key> element set to the value of the key to be used in the gre tunnel that is being established.

The recipient of the XML ignores any unknown element and any unknown attribute.

\* \* \* Next Change \* \* \* \*

\* \* \* End of Changes \* \* \* \*