**3GPP TSG- Meeting #**

**, , -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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 can be 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-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA6 has made some correction and simplified the original ISD message procedures, but these server and client procedures were also incompletely specified in CT1. Also, some O/M presence contents need adding/correcting | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | MCData client handling added.  Participating and Controlling server procedures included or referenced modelled on corresponding TS 24.282 SDS procedures with unnecessary features (request-type, group message, functional alias) removed.  Message contents aligned with Stage 2. O/M corrections  Backwards Compatibility analysis: this CR is Backwards Comptaible: it introduces missing behaviour as the original message was not implementable within current 3GPP specifications and so payload & O/M changes are 'void' from a BC perpsective. Stage 2 has also been changed in a non-BC way for all relevant releases and these Stage 3 changes will align with this. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment with Stage 2 behaviour. Incomplete functionality | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 1, 6.1X (new), 6.1X.1 (new), 6.1X.1.1 (new), 6.3.1.1, 17.1.2, 17.1.2.1 (new), 17.1.2.2 (new), 17.2.1, 17.X (new), 17.X.1 (new), 17.X.2 (new), 17.Y.1 (new), 17.Y.1.1 (new), 17.Y.2 (new), 17.Y.2.1 (new), 17.Y.2.2 (new), 17.Y.3 (new), 17.Y.3.1 (new), 17.Y.3.2 (new), | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | C1-254533 | | | | | | | | |

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

# 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]. Interworking-specific impacts on the MCData client and MCData server behaviour are also documented.

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

## 6.1X MCData client procedures

### 6.1X.1 Distinction of requests at the MCData client

#### 6.1X.1.1 SIP MESSAGE request

The MCData client needs to distinguish between the SIP MESSAGE requests for originations and terminations as described in 3GPP TS 24.282 [82] clause 6.2.1.1 with the following addition:

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

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

#### 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"; and

- 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"

In addition, the IWF shall perform the role of an MCData server in distinguishing the following SIP MESSAGE requests for originations and terminations:

- 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", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for Interworking Security Data for controlling MCData function"; and

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", and an ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata" in a P-Asserted-Service header field. Such requests are known as "SIP MESSAGE request for Interworking Security Data for terminating participating MCData 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.

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

### 17.1.2 IWF receives Interworking Security Data message

#### 17.1.2.1 IWF in the participating role

Upon receiving a "SIP MESSAGE request for Interworking Security Data message for terminating participating function", the actions towards the controlling MCData function are described below. Other 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 of scope of the present document.

If the IWF accepts the above SIP MESSAGE request, the IWF acting as the participating MCData function:

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [4]; and

2) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [4].

If the IWF rejects the above SIP MESSAGE request, the IWF acting as the participating MCData function:

1) shall generate a SIP 4xx, 5xx or 6xx response to the above SIP MESSAGE request according to 3GPP TS 24.229 [4];

2) shall include appropriate Warning header field(s) in the SIP response; and

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

#### 17.1.2.2 IWF in the controlling role

Upon receipt of a "SIP MESSAGE request for Interworking Security Data for controlling MCData function", 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 controlling MCData function 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 3GPP TS 24.282 [82] subclause 4.9, and shall not continue with the rest of the steps in this subclause;

3) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body contained in the SIP MESSAGE;

4) if the conditions in 3GPP TS 24.282 [82] subclause 11.1 indicate that the MCData user is not allowed to SDS communications due to message size as determined by step 3) of 3GPP TS 24.282 [82] subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "2XX user not authorised for one-to-one message due to message size" in a Warning header field as specified in 3GPP TS 24.282 [82] subclause 4.9, and shall not continue with the rest of the steps in this subclause.

5) if the SIP MESSAGE request:

a) does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall return a SIP 403 (Forbidden) response with the warning text set to "2XY unable to determine targeted user for one-to-one message" in a Warning header field as specified in 3GPP TS 24.282 [82] subclause 4.9, and skip the rest of the steps below; and

b) shall further process the message towards the targeted MCData user. Actions carried out by the IWF are out of scope of the present document.

6) shall generate a SIP 202 (Accepted) response in response to the "SIP MESSAGE request for Interworking Security Data for controlling MCData function"; and

7) shall send the SIP 202 (Accepted) response towards the originating participating MCData function according to 3GPP TS 24.229 [4].

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

### 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 | O | V | 1 |
| 78 | Payload | 3GPP TS 24.282 [82], clause 15.2.13 with Payload content type set to 'BINARY' | M | TLV-E | 3-x |

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

## 17.X MCData client

### 17.X.1 MCData client originates Interworking Security Data message

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

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 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 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];

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

6) shall include an application/resource-lists+xml MIME body with the MCData ID of the target MCData user or the functional alias to be called in the "uri" attribute of an <entry> element of a <list> element of the <resource-lists> element, according to rules and procedures of IETF RFC 4826 [89];

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

8) 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

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

### 17.X.2 MCData client receives Interworking Security Data message

Upon receiving a "SIP MESSAGE request for Interworking Security Data for terminating MCData client", the MCData client:

1) may reject the SIP MESSAGE request if there are not enough resources to handle the SIP MESSAGE request;

2) if the SIP MESSAGE request is rejected in step 1), shall respond toward participating MCData function with a SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this subclause;

Other actions performed by the MCData client 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.

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

## 17.Y MCData server

### 17.Y.1 Distinction of requests at the MCData server

#### 17.Y.1.1 SIP MESSAGE request

The MCData needs to distinguish between SIP MESSAGE requests for originations and terminations from 3GPP TS 24.282 [82] clause 6.3.1.1

In addition an MCData server in an MC System supporting the Interworking Security Data message shall distinguish the following SIP MESSAGE requests for originations and terminations:

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

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

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

### 17.Y.2 Participating MCData function procedures

#### 17.Y.2.1 Originating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for Interworking Security Data for originating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24] and skip the rest of the steps;

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

NOTE 1: The MCData ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in 3GPP TS 24.282 [82] clause 7.3.

3) if the participating MCData function cannot find a binding between the public user identity and an MCData ID or if the validity period of an existing binding has expired, then the participating MCData function shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9, and shall not continue with any of the remaining steps;

4) shall determine the public service identity of the controlling MCData function hosting the one-to-one standalone SDS service for the calling user;

5) if unable to identify the controlling MCData function for standalone SDS, it shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 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 3GPP TS 24.282 [82] clause 11.1;

7) if the procedures in 3GPP TS 24.282 [82] clause 11.1 indicate that the user identified by the MCData ID:

a) is not allowed to send MCData communications as determined by step 1) of 3GPP TS 24.282 [82] clause 11.1, shall reject the "SIP MESSAGE request for Interworking Security Data for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "200 user not authorised to transmit data" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9, and shall not continue with the rest of the steps in this clause;

b) is not allowed to initiate one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request as determined by step 7) of 3GPP TS 24.282 [82] clause 11.1, shall reject the "SIP MESSAGE request for Interworking Security Data for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "202 user not authorised for one-to-one MCData communications due to exceeding the maximum amount of data that can be sent in a single request" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9, and shall not continue with the rest of the steps in this clause; and

c) is not allowed to initiate one-to-one MCData communications to the targeted user as determined by step 1a) of 3GPP TS 24.282 [82] clause 11.1, shall reject the "SIP MESSAGE request for Interworking Security Data for originating participating MCData function" with a SIP 403 (Forbidden) response including warning text set to "229 one-to-one MCData communication not authorised to the targeted user" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9 and shall not continue with the rest of the steps;

8) if the payload size of the message is larger than the value contained in the <max-payload-size-sds-cplane-bytes> element in the MCData service configuration document as specified in 3GPP TS 24.484 [12], shall reject the "SIP MESSAGE request for Interworking Security Data for originating participating MCData function" with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "203 message too large to send over signalling control plane" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9;

NOTE 2: The term "payload size" refers to the "Length of Payload contents" of the payload IE of the Interworking Security Data message transported in the SIP MESSAGE request, minus 1 (to account for the added "Payload content type" field).

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

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

NOTE 3: The public service identity can identify the controlling MCData function in the local MCData system or in an interconnected MCData system.

NOTE 4: If the controlling MCData function is in an interconnected MCData system in a different trust domain, then the public service identity can identify the MCData gateway server that acts as an entry point in the interconnected MCData system from the local MCData system.

NOTE 5: If the controlling MCData function is in an interconnected MCData system in a different trust domain, then the local MCData system can route the SIP request through an MCData gateway server that acts as an exit point from the local MCData system to the interconnected MCData system.

NOTE 6: How the participating MCData function determines the public service identity of the controlling MCData function serving the target MCData ID or of the MCData gateway server in the interconnected MCData system is out of the scope of the present document.

NOTE 7: How the local MCData system routes the SIP request through an exit MCData gateway server is out of the scope of the present document.

11) shall copy all MIME bodies included in the incoming SIP MESSAGE request to the outgoing SIP MESSAGE request;

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

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

14) shall include a P-Asserted-Identity header field in the outgoing SIP MESSAGE request set to the public service identity of the participating MCData function; and

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

Upon receipt of a SIP 202 (Accepted) response in response to the SIP MESSAGE request in step 15):

1) shall generate a SIP 202 (Accepted) response as specified in 3GPP TS 24.229 [4]; and

2) shall send the SIP 202 (Accepted) response to the MCData client according to 3GPP TS 24.229 [4].

Upon receipt of a SIP 200 (OK) response in response to the SIP MESSAGE request in step 15):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [4]; and

2) shall send the SIP 200 (OK) response to the MCData client according to 3GPP TS 24.229 [4].

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

1) shall generate a SIP response according to 3GPP TS 24.229 [4];

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 [4].

#### 17.Y.2.2 Terminating participating MCData function procedures

Upon receipt of a "SIP MESSAGE request for Interworking Security Data for terminating participating MCData function", the participating MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The participating MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [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 retrieve the binding between the MCData ID and public user identity of the terminating MCData user;

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

3a) if the <IncomingOne-to-OneCommunicationList> element exists in the MCData user profile document with one or more <One-to-One-CommunicationListEntry> elements (see the MCData user profile document in 3GPP TS 24.484 [50]) and:

i) if the <mcdata-calling-user-id> element of the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SIP MESSAGE request does not match with the <entry> element of any of the <One-to-One-CommunicationListEntry> elements in the <IncomingOne-to-OneCommunicationList> element of the MCData user profile document (see the MCData user profile document in 3GPP TS 24.484 [50]); and

ii) if configuration is not set in the MCData user profile document that allows the MCData user to receive one-to-one MCData communication from any user (see <allow-one-to-one-communication-from-any-user> element in MCData user profile document in 3GPP TS 24.484 [50]);

then:

i) shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "230 one-to-one MCData communication not authorised from this originating user" in a Warning header field as specified in 3GPP TS 24.282 [82] clause 4.9 and shall not continue with the rest of the steps;

4) shall generate an outgoing SIP MESSAGE request as specified in 3GPP TS 24.282 [82] clause 6.3.2.1;

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

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

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

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [4]; and

2) shall send the SIP 200 (OK) response to the controlling MCData function according to 3GPP TS 24.229 [4].

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

1) shall generate a SIP response according to 3GPP TS 24.229 [4];

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 [4].

### 17.Y.3 Controlling MCData function procedures

#### 17.Y.3.1 Originating controlling MCData function procedures

This subclause describes the procedures for sending a SIP MESSAGE from the controlling MCData function and is initiated by the controlling MCData function as a result of an action in subclause 17.Y.3.2.

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 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" along with parameters "require" and "explicit" according to IETF RFC 3841 [6] in the outgoing SIP MESSAGE request;

4) shall copy the following MIME bodies in the received SIP MESSAGE request into the outgoing SIP MESSAGE request by following the guidelines in 3GPP TS 24.282 [82] subclause 6.4:

a) application/vnd.3gpp.mcdata-info+xml MIME body;

b) application/vnd.3gpp.mcdata-signalling MIME body; and

c) application/vnd.3gpp.mcdata-payload MIME body

5) in the application/vnd.3gpp.mcdata-info+xml MIME body:

a) shall set the <mcdata-request-uri> element set to the MCData ID of the terminating user; and

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

7) shall copy the public user identity of the calling MCData user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request;

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

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

#### 17.Y.3.2 Terminating controlling MCData function procedures

Upon receipt of a "SIP MESSAGE request for Interworking Security Data for controlling MCData function", the controlling MCData function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling MCData function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [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 3GPP TS 24.282 [82] subclause 4.9, and shall not continue with the rest of the steps in this subclause;

3) shall decode the contents of the application/vnd.3gpp.mcdata-signalling MIME body contained in the SIP MESSAGE;

4) if the conditions in 3GPP TS 24.282 [82] subclause 11.1 indicate that the MCData user is not allowed to SDS communications due to message size as determined by step 3) of 3GPP TS 24.282 [82] subclause 11.1, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request, with warning text set to "2XX user not authorised for one-to-one message due to message size" in a Warning header field as specified in 3GPP TS 24.282 [82] subclause 4.9, and shall not continue with the rest of the steps in this subclause.

5) if the 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 return a SIP 403 (Forbidden) response with the warning text set to "2XY unable to determine targeted user for one-to-one message" in a Warning header field as specified in 3GPP TS 24.282 [82] subclause 4.9, and skip the rest of the steps below;

6) if the SIP MESSAGE request contains an application/resource-lists MIME body with exactly one <entry> element, shall send a SIP MESSAGE request to the MCData user identified in the <entry> element of the MIME body, as specified in subclause 17.Y.3.1;

7) shall generate a SIP 202 (Accepted) response in response to the "SIP MESSAGE request for Interworking Security Data 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].

\* \* \* End Change \* \* \* \*