**3GPP TSG-SA3 Meeting #123 draft\_S3-252985-r1**

**Goteborg, Sweden, 25 - 29 August 2025**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.180** | **CR** | **0224** | **rev** | 1 | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Providing additional clarifications on MCData for Overview. | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MCXSec4 | | | | |  | ***Date:*** | | | 2025-08-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
| ***5*** |  | | | | | | | | | |
| ***Reason for change:*** | | Based on the progress of TS 23.282, we’ve added clarifications to the group communication aspects and have also taken point-to-point communication into account in the Overview clause.  Moreover, as specified in 3GPP TS 23.282 clause 7.2, the relationship between MCData user and the communication group needs to be clarified under 8.4. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | We've added some clarifications regarding the MCData user and have taken point-to-point communications into account. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not aligned with TS 23.280 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.1, 8.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 8 MCData

## 8.1 Overview

MCData SDS allows transmission of short data messages (SDS), either private or group, over both the signalling plane (reference point MCData-SDS-1) and media plane (reference point MCData-SDS-2).

MCData File Distribution (FD) also allows for transmission of files, either private or group, over the media plane or using HTTP. When distributed using HTTP, binary data representing the file is uploaded and downloaded using HTTP POST and HTTP GET.

MCData signalling parameters for SDS and File Distribution are routed within SIP messages. Protection for these signalling messages and files when distributed using HTTP, use the same key material as for MCPTT and MCVideo.

The MCData SDS or FD messages may also contain a MCData Data signalling payload or a MCData Data payload or both. These payloads may be within a SIP message should the signalling plane be used, or within a MSRP message should the media plane be used. The MCData Data payload may be end-to-end confidentiality and integrity protected according to an end to end security context payload.

The file when distributed using HTTP may be end-to-end confidentiality and integrity protected according to an end to end security context payload before being uploaded.

Components of MCData messages:

- **MCData signalling parameters**: generic Mission Critical Services signalling elements e.g. MCData Group ID, MCData user ID. These parameters are confidentiality protected between the MCData Client and the MCData server with signalling plane security mechanisms.

- **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 protected between the MCData Client and the MCData server with signalling plane security mechanisms.

- **End to end security parameters**: information specifying the cryptographic elements used to protect the data payload).

- **MCData** **Data payload**: the actual user payload for MCData user or application consumption. This payload is end to end confidentiality and integrity protected.

Components of the MCData message (MCData signalling parameters and MCData Data signalling payload) are integrity protected between the MCData Client and the MCData server with the signalling plane security mechanisms.



Figure 8.1-1: MCData message components

For the MCData one-to-one and point-to-point communication the PCK is used to protect the MCData data payload or the file when distributed using HTTP. For group communications, the GMK is used to protect the MCData data payload or the file when distributed using HTTP. The data payload or the file when distributed using HTTP may also be authenticated by the initiator.

Distribution of the PCK is within the signalling channel setup for the MCData private message (either SDS or FD). Distribution of the GMK is as defined in clause 5.7.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 8.4 Group communications

The purpose of key management is to establish a MCData Payload Protection Key (DPPK) for the group communication between the group of communicating clients, where the MCData user is affiliated to the respected group according to TS 23.282 [38] clause 7.2. In the case of group communication, the DPPK shall be the GMK. The GMK is distributed in the same way as for MCPTT and MCVideo group communications, as defined in clause 5.7.

When required by the MCData service provider, protection shall be applied to the MCData Data payloads using the GMK. Payload authentication may also be applied. The mechanisms used to secure these payloads are described in clause 8.5.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*