**3GPP TSG-SA3 Meeting #123 draft\_S3-252986**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.180** | **CR** | **0225** | **rev** | 1 | **Current version:** | **19.2.0** |  |
|  | | | | | | | | |
| *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:*** | Private one-to-one and point-to-point MCData communication Conidering the on-network and first-to-answer scenarios | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MCXSec4 | | | | |  | ***Date:*** | | | 2025-08-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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:*** | | Instead of the One-to-one communication, the MCData security also needs to support Point-to-Point MCData communications. This contribution aims to clarify this point. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Enhancing the MCData security to support private One-to-One and Point-to-Point MCData communications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No protection for the MCData in the private communications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.X | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 8.3 One-to-one and point-to-point communications

The purpose of key management is to establish a MCData Payload Protection Key (DPPK) for private one-to-one and point-to-point MCData communication channel between the pair of communicating clients. In the case of a one-to-one and point-to-point MCData communication, the DPPK shall be the PCK. The PCK is used for end-to-end protection of one-to-one (private) and point-to-point SDS or FD data payloads.

The PCK and PCK-ID are distributed within the SIP message used to initiate the session.

The PCK and PCK-ID is distributed using service-specific signalling. For all MCData services, SIP signalling is used to establish or send the MCData communication. The PCK and PCK-ID is distributed within a MIKEY payload contained within the SDP offer sent from the initiator to the receiver in the same way as for MCPTT and MCVideo. The procedures for PCK distribution are defined within clause 5.6.

For off-network MCData operations, an MCData payload containing a MIKEY\_SAKKE I-MESSAGE (clause 8.5.4.1) is used to distribute an MCData DPPK (PCK) from the initiating MCX client to the terminating MCX client.

This key distribution mechanism applies to the following messages defined in TS 23.282 [38]:

- MCData standalone data request

- MCData session data request

- MCData FD request

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

Once the PCK is established between the source and destination, SDS and FD exchanges between this same source and destination may continue to use the same PCK for subsequent MCData communications by simply providing the PCK-ID in every SDS message.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*