**3GPP TSG-CT WG1 Meeting #127-eC1-20XXXX**

**Electronic meeting, 13-20 November 2020 (was C1-207237)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **2877** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | Protection of 5GSM message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | vivo | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2020-11-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 5GSM messages are security protected indirectly by being piggybacked by the security protected 5GMM messages (i.e. UL NAS TRANSPORT message and the DL NAS TRANSPORT message).  However, the specification in subclause 8.2.28 and 9.9 can lead to the misunderstanding that the plain 5GS NAS message IE of a security protected 5GS NAS message can also be a plain 5GSM message.  Quote from subclause 8.2.28 and 9.9:  *“This message is sent by the UE or the network to transfer a plain 5GS NAS message together with the sequence number and the message authentication code protecting the message. See table 8.2.28.1.1.*”  *“This IE includes a complete plain 5GS NAS message as specified in subclauses 8.2 and 8.3. The SECURITY PROTECTED 5GS NAS MESSAGE message (see subclause 8.2.28) is not plain 5GS NAS messages and shall not be included in this IE.”*  Therefore, it is proposed to clarify that the plain 5GS NAS message IE of a security protected 5GS NAS message includes only a plain 5GMM message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Propose to clarify that the plain 5GS NAS message in a security protected 5GS NAS message includes a complete plain 5GS NAS message as specified in subclauses 8.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The specification in subclause 8.2.28 and 9.9 can lead to the misunderstanding that the plain 5GS NAS message IE of a security protected 5GS NAS message can also be a plain 5GSM message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.2.28.1, 9.9 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 8.2.28.1 Message definition

This message is sent by the UE or the network to transfer a plain 5GS NAS message as specified in subclauses 8.2 together with the sequence number and the message authentication code protecting the message. See table 8.2.28.1.1.

Message type: SECURITY PROTECTED 5GS NAS MESSAGE

Significance: dual

Direction: both

Table 8.2.28.1.1: SECURITY PROTECTED 5GS NAS MESSAGE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Message authentication code | Message authentication code  9.8 | M | V | 4 |
|  | Sequence number | Sequence number  9.10 | M | V | 1 |
|  | Plain 5GS NAS message | Plain 5GS NAS message  9.9 | M | V | 3-n |

NOTE: The minimum length of Plain 5GS NAS message IE can be 2 octets if it includes a Test Mode Control message specified in 3GPP TS 38.509 [31AA].

\*\*\*\*\*\*\*\*Next change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 9.9 Plain 5GS NAS message

This IE includes a complete plain 5GS NAS message as specified in subclauses 8.2 and 8.3. The SECURITY PROTECTED 5GS NAS MESSAGE (see subclause 8.2.28) includes a complete plain 5GS NAS message as specified in subclauses 8.2. The SECURITY PROTECTED 5GS NAS MESSAGE message (see subclause 8.2.28) is not plain 5GS NAS messages and shall not be included in this IE.

\*\*\*\*\*\*\*\*end of Change\*\*\*\*\*\*\*\*