**3GPP TSG-CT WG1 Meeting #125-eC1-20xxxx**

**Electronic meeting, 20-28 August 2020 (was C1-204728, 205271)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **2455** | **rev** | **2** | **Current version:** | **16.5.1** |  |
|  |
| *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:***  | Integrity protection of Payload container IE |
|  |  |
| ***Source to WG:*** | vivo, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17 |  | ***Date:*** | 2020-08-23 |
|  |  |  |  |  |
| ***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 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-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:*** | 1)CT1 agreed TS 24.501 CR#0357(C1-185721) that SOR transparent container IE can be carried in Payload container IE and in DL NAS TRANSPORT message, and the corresponding integrity checking of Payload container IE in DL NAS TRANSPORT message is specified in subclause 5.4.5.3.3 Network-initiated NAS transport of messages.Also, CT1 agreed TS 24.501 CR#0594(C1-188946) that the Payload container type IE can be set to "UE parameters update transparent container" in DL NAS TRANSPORT message and the integrity checking of the payload container IE is specified in subclause 5.4.5.3.3 too.However, the general specification of the integrity checking of the payload container IE when the Payload container type IE is set to "SOR transparent container" or "UE parameters update transparent container" is not captured in subclause 4.4.4.2 where the integrity checking of the SOR transparent container IE has been captured.Therefore, it is proposed to capture the general specification of the integrity checking of the payload container IE in subclause 4.4.4.2.Quote:"*5.4.5.3.3 Network-initiated NAS transport of messages**Upon reception of a DL NAS TRANSPORT message, the UE shall stop the timer T3346 if running.**Upon reception of a DL NAS TRANSPORT message, if the Payload container type IE is set to:**……**d) "SOR transparent container" and if the Payload container IE:**1) successfully passes the integrity check (see 3GPP TS 33.501 [24]), indicates a list of preferred PLMN/access technology combinations is provided and the list type indicates:**……**2) does not successfully pass the integrity check (see 3GPP TS 33.501 [24]) then the UE shall proceed with the behaviour as specified in 3GPP TS 23.122 [5] annex C.**……**i) "UE parameters update transparent container" and if the Payload container IE**1) successfully passes the integrity check (see 3GPP TS 33.501 [24]):**…..**2) does not successfully pass the integrity check (see 3GPP TS 33.501 [24]) then the UE shall discard the content of the payload container IE;*……"2)Moreover, due to the difference between the integrity protection of NAS messages and the integrity protection of NAS IEs, it is proposed to have a new subclause to sperate the integrity protection of NAS IEs from the integrity protection of NAS messages in subclause 4.4.3) The integrity protection of SOR transparent container IE in REGISTRATION COMPLETE message is missing in general subclause 4.4. |
|  |  |
| ***Summary of change:*** | 1)Propose to capture the general specification of the integrity protection of the payload container IE in subclause 4.4.2)Propose to sperate the specification of the integrity protection of NAS IEs from the integrity protection of NAS messages in general subclause 4.4.3)Propose to capture the integrity protection of SOR transparent container IE in REGISTRATION COMPLETE message in subclause 4.4. |
|  |  |
| ***Consequences if not approved:*** | 1)The general specification of integrity protection of NAS IEs is not complete.2)Including the specification of the integrity checking of the NAS IEs in the subclause 4.4.4 (i.e. Integrity protection of NAS signalling messages) can lead to confusion about the difference between the integrity protection of NAS messages and the integrity protection of NAS IEs. |
|  |  |
| ***Clauses affected:*** | 4.4.4.2, 4.4.x(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:*** |  |

\*\*\*\*\* start of change \*\*\*\*\*

#### 4.4.4.2 Integrity checking of NAS signalling messages in the UE

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

a) IDENTITY REQUEST (if requested identification parameter is SUCI);

b) AUTHENTICATION REQUEST;

c) AUTHENTICATION RESULT;

d) AUTHENTICATION REJECT;

e) REGISTRATION REJECT (if the 5GMM cause is not #76);

f) DEREGISTRATION ACCEPT (for non switch off); and

g) SERVICE REJECT (if the 5GMM cause is not #76).

NOTE: These messages are accepted by the UE without integrity protection, as in certain situations they are sent by the network before security can be activated.

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once the secure exchange of NAS messages has been established, the receiving 5GMM entity in the UE shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS in the UE shall discard that message. The processing of the SECURITY MODE COMMAND message that has not successfully passed the integrity check is specified in subclause 5.4.2.5. If any NAS signalling message is received as not integrity protected even though the secure exchange of NAS messages has been established by the network, then the NAS shall discard this message.

\*\*\*\*\* next change \*\*\*\*\*

### 4.4.X Integrity protection of NAS IEs

The network can provide the SOR transparent container IE during the registration procedure to the UE in the REGISTRATION ACCEPT message. The SOR transparent container IE is integrity protected by the HPLMN as specified in 3GPP TS 33.501 [24].

The UE can provide the SOR transparent container IE during the registration procedure to the network in the REGISTRATION COMPLETE message. The SOR transparent container IE is integrity protected by the UE as specified in 3GPP TS 33.501 [24].

The network can provide the Payload container IE during the Network-initiated NAS transport procedure to the UE in DL NAS TRANSPORT message. If the Payload container type IE is set to "SOR transparent container" or "UE parameters update transparent container", the Payload container IE is integrity protected by the HPLMN as specified in 3GPP TS 33.501 [24]. If the Payload container type IE is set to "Multiple payloads" and the payload container type field of the payload container entry is set to "SOR transparent container" or "UE parameters update transparent container", the payload container entry contents field of the payload container entry is integrity protected correspondingly.

The UE can provide the Payload container IE during the UE-initiated NAS transport procedure to the network in UL NAS TRANSPORT message. If the Payload container type IE is set to "SOR transparent container" or "UE parameters update transparent container", the Payload container IE is integrity protected by the UE as specified in 3GPP TS 33.501 [24]. If the Payload container type IE is set to "Multiple payloads" and the payload container type field of the payload container entry is set to "SOR transparent container" or "UE parameters update transparent container", the payload container entry contents field of the payload container entry is integrity protected correspondingly.

\*\*\*\*\* End of changes \*\*\*\*\*