**3GPP TSG-CT WG1 Meeting #123-eC1-20xxxx**

**Electronic meeting, 16-24 April 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **2137** | **rev** | **1** | **Current version:** | **16.4.1** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | No messages without integrity protection processed after security activation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc16 | | | | |  | ***Date:*** | | | 2020-04-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | From the note in subclause 4.4.4.2, it is unclear whether a UE for which the secure exchange of NAS messages has been established is or is not required to process messages in bullets a) – g) of subclause 4.4.4.2 which are not integrity protected. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified that the messages a) – g) in subclause 4.4.4.2 are accepted by the UE without integrity protection if the secure exchange of NAS messages has not been established for the following reasons:   * It is aligned with the last paragraph in the subclause starting with “*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*”. * Subclause 4.4.4.1 says “*For the UE, integrity protected signalling is mandatory for the 5GMM NAS messages once a valid 5G NAS security context exists and has been taken into use*”. * If the UE is allowed to process those messages without integrity protection, this behaviour can be abused by an attacker. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | After security activation, some UEs may process those messages while other UEs may avoid it in case the messages are not integrity protected.  For those UEs processing the messages, faked messages like IDENTITY REQUEST sent by an attacker may be processed by the UE although NAS security is established, allowing the attacker to possibly mount other attacks. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

#### 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 N1 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 neither #31 nor #76);

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

g) SERVICE REJECT (if the 5GMM cause is neither #31 nor #76).

NOTE: These messages are accepted by the UE without integrity protection only before the secure exchange of NAS messages has been established, 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.

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].

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.