**3GPP TSG-CT WG1 Meeting #124-eC1-204054**

**Electronic meeting, 2-10 June 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **2384** | **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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Clarification of NAS COUNT handling in 5G |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc16 |  | ***Date:*** | 2020-05-22 |
|  |  |  |  |  |
| ***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 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)* |
|  |  |
| ***Reason for change:*** | The LS (C1-200319) from GSMA FASG Coordinated Vulnerability Disclosure (CVD) Programmer indicated a 5G NAS COUNT reset attack which is described in details in the a research paper entitled “5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol”. TS 24.501 clause 4.4.3.1 currently says“The receiving side shall estimate the NAS COUNT used by the sending side. Specifically, if the estimated NAS sequence number wraps around, the NAS overflow counter shall be incremented by one.”It is unclear, if the NAS sequence number included in the received NAS message is smaller than that of the last successfully integrity verified message, whether the store NAS overflow counter will be incremented by one or kept unchanged.Hence, the GSMA LS strongly recommends that TS 24.501 needs to be modified to include more prescriptive and unambiguous text. |
|  |  |
| ***Summary of change:*** | It proposes to update the description given in clause 4.4.3.1 on handling of estimated NAS COUNT at the receiver side to it more prescriptive and unambiguous.Additionally, the clarification of the NAS COUNT stored in the AMF is added. |
|  |  |
| ***Consequences if not approved:*** | The current spec text on NAS COUNT handling is not prescriptive and unambiguous which may cause different implementation to creat security vulnerabilities. |
|  |  |
| ***Clauses affected:*** | 4.4.3.1 |
|  |  |
|  | **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 \* \* \* \*

#### 4.4.3.1 General

Each 5G NAS security context shall be associated with two separate counters NAS COUNT per access type in the same PLMN: one related to uplink NAS messages and one related to downlink NAS messages. If the 5G NAS security context is used for access via both 3GPP and non-3GPP access in the same PLMN, there are two NAS COUNT counter pairs associated with the 5G NAS security context. The NAS COUNT counters use 24 bit internal representation and are independently maintained by UE and AMF. The NAS COUNT shall be constructed as a NAS sequence number (8 least significant bits) concatenated with a NAS overflow counter (16 most significant bits).

When NAS COUNT is input to NAS ciphering or NAS integrity algorithms it shall be considered to be a 32-bit entity which shall be constructed by padding the 24-bit internal representation with 8 zeros in the most significant bits.

The value of the uplink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the value that shall be used in the next NAS message.

The value of the downlink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the largest downlink NAS COUNT used in a successfully integrity checked NAS message.

The value of the uplink NAS COUNT stored in the AMF is the largest uplink NAS COUNT used in a successfully integrity checked NAS message.

The value of the downlink NAS COUNT stored in the AMF is the value that shall be used in the next NAS message.

The NAS sequence number part of the NAS COUNT shall be exchanged between the UE and the AMF as part of the NAS signalling. After each new or retransmitted outbound SECURITY PROTECTED 5GS NAS MESSAGE message, the sender shall increase the NAS COUNT number by one, except for the initial NAS messages if the lower layers indicated the failure to establish the RRC connection (see 3GPP TS 38.331 [30]). Specifically, on the sender side, the NAS sequence number shall be increased by one, and if the result is zero (due to wrap around), the stored NAS overflow counter shall also be incremented by one (see subclause 4.4.3.5). If, through implementation-dependent means, the receiver determines that the NAS message is a replay of an earlier NAS message, then the receiver handles the received NAS message as described in subclause 4.4.3.2. Otherwise, in order to determine the estimated NAS COUNT value to be used for integrity verification of a received NAS message:

- The sequence number part of the estimated NAS COUNT value shall be equal to the sequence number in the received NAS message; and

- If the receiver can guarantee that this NAS message was not previously accepted, then the receiver may select the estimated NAS overflow counter so that the estimated NAS COUNT value is lower than the stored NAS COUNT value; otherwise, the receiver selects the estimated NAS overflow counter so that the estimated NAS COUNT value is higher than the stored NAS COUNT value.

During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, when a mapped 5G NAS security context is derived and taken into use, the AMF shall set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The UE shall set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero.

During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the AMF shall increment the downlink NAS COUNT by one after it has created an S1 mode to N1 mode NAS transparent container (see subclause 9.11.2.9).

During the inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode, the AMF shall increment the downlink NAS COUNT by one after it has created an N1 mode to S1 mode NAS transparent container (see subclause 9.11.2.7).

During N1 mode to N1 mode handover:

a) if the new 5G NAS security context is created with the same KAMF, the AMF shall signal the 8 least significant bits of the current downlink NAS COUNT value in an Intra N1 mode NAS transparent container (see subclause 9.11.2.6). The AMF shall then increment the downlink NAS COUNT by one; or

b) if the new 5G NAS security context is created with a new KAMF, the AMF shall signal the 8 least significant bits of the current downlink NAS COUNT value in an Intra N1 mode NAS transparent container (see subclause 9.11.2.6) and shall then set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The AMF shall then increment the downlink NAS COUNT by one. The UE shall also set both the uplink and downlink NAS COUNT counters to zero.

NOTE: During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the S1 mode to N1 mode NAS transparent container (see subclause 9.11.2.9) is treated as an implicit SECURITY MODE COMMAND message for the UE and the AMF, and therefore the AMF regards the sending of the S1 mode to N1 mode NAS transparent container as the sending of an initial SECURITY MODE COMMAND message in order to derive and take into use a mapped 5G NAS security context for the purpose of the NAS COUNT handling.

\* \* \* End of Change \* \* \* \*