**3GPP TSG-CT WG1 Meeting #126-eC1-20xxxx**

**Electronic meeting, 15-23 October 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.301** | **CR** | **3430** | **rev** | **2** | **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:*** | Clarification of NAS COUNT handling in 4G | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Vodafone, Deutsche Telekom | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SAES17 | | | | |  | ***Date:*** | | | 2020-09-30 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Based on GSMA requirements on 5G NAS COUNT handling, CT1 has agreed an R16 CR#2384 (C1-204054) to update the description given in TS 24.501 clause 4.4.3.1 on handling of estimated NAS COUNT at the receiver side to make it more prescriptive and unambiguous.  Actually before the CR#2384, the NAS COUNT handling given in TS 24.501 was fully copied from TS 24.301. Even GSMA has not provided the requirements on 4G but actually the same problem exists in 4G NAS COUNT handling as well.  One point is that the current spec only clearly specified the used UL/DL NAS COUNT value stored at the UE side while it is missing at the MME side.  Another point is it is true that the current NAS COUNT handling in 4G was specified since Rel-8. However, due to the lack of prescriptive and unambiguous description in the standard, it could exist different implementations based on different interpretation of the standard in the field. Typically, it would be beneficial to clearly document something in the standard on following typical case which was observed that has happened many times in the field:   1. *The UE sends two consecutive NAS messages with SN X, and X+1 in sequence; but* 2. *The network receives these two NAS messages with SN X+1, and X in sequence, i.e. out of sequence happens.*   In above typical case, message with SN X is not replayed and also not received by the network in the past, so it should be handled as not wrap around. How to guarantee a message with out of sequence NAS SN is not received in the past without wrap around is up to the UE implementation. Hence, it proposes to add a NOTE to provide informative information on how to estimate the NAS COUNT at the receiving side to cover this case. As Rel-16 was frozen, the proposed alignment is since Rel-17. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. It proposes to add the missed UL/DL NAS COUNT handling at the MME side to align with the UE side. 2. It proposes to add a NOTE to provide informative information on how to estimate the NAS COUNT at the receiving side in case of out of sequence of NAS SN happens without wrap around. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The use of UL/DL NAS COUNT value at the network side is missing.  It is unclear on how to estimate the NAS COUNT at the receiving side in case of out of sequence of NAS SN happens without wrap around. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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:*** | | The original revision was discussed in CT1#125e and postponed.  Rev#1 moves to R17 under SAES17 with updated cover page but without changing the change content.  Rev#2 changes the normative text to a NOTE. | | | | | | | | |

\* \* \* First Change \* \* \* \*

#### 4.4.3.1 General

Each EPS security context shall be associated with two separate counters NAS COUNT: one related to uplink NAS messages and one related to downlink NAS messages. The NAS COUNT counters use 24 bit internal representation and are independently maintained by UE and MME. 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 MME is the largest uplink NAS COUNT used in a successfully integrity checked NAS message.

The value of the downlink NAS COUNT stored in the MME 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 MME as part of the NAS signalling. After each new or retransmitted outbound security protected NAS 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 36.331 [22]). 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 NAS overflow counter shall also be incremented by one (see subclause 4.4.3.5). 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.

NOTE 0: If the estimated NAS COUNT is lower than or equal to the stored NAS COUNT, the receiving side can determine that the NAS message is a replay of an earlier NAS message and then handle it as described in subclause 4.4.3.2. If the receiving side can guarantee that the NAS message was not previously accepted then it can use an estimated NAS COUNT lower than its stored NAS COUNT.

After the derivation of a NAS token due to an inter-system change from S1mode to A/Gb mode or Iu mode in idle mode as specified in 3GPP TS 24.008 [13], the UE shall increase the uplink NAS COUNT by one.

When the MME receives a NAS token via SGSN during an idle mode inter-system change from S1 mode to A/Gb mode or Iu mode, the MME shall check the NAS token as specified in 3GPP TS 33.401 [19], subclause 9.1.1, and update its uplink NAS COUNT with the uplink NAS COUNT value used for the successful check of the NAS token.

NOTE 1: The MME does not check the NAS token if it is received via SGSN during a connected mode inter-system change from S1 mode to A/Gb mode or Iu mode.

During the handover from UTRAN/GERAN to E-UTRAN, when a mapped EPS security context is derived and taken into use, the MME shall set both the uplink and downlink NAS COUNT counters of this EPS security context to zero. The UE shall set both the uplink and downlink NAS COUNT counters to zero.

When a mapped EPS security context is derived as specified in 3GPP TS 33.501 [56] and taken into use in the following cases:

- during the inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode; or

- during the inter-system change from N1 mode to S1 mode in EMM-IDLE mode for the UE operating in single-registration mode in a network supporting N26 interface,

the MME shall store the mapped EPS NAS security context with the uplink and downlink NAS COUNT counters associated with the derived K'ASME key set to the uplink and downlink NAS COUNT counters of the mapped EPS NAS security context respectively. The UE shall set the uplink and downlink NAS COUNT counters to the uplink and downlink NAS COUNT counters of the current 5G NAS security context respectively.

During the handover from E-UTRAN to UTRAN/GERAN the MME signals the current downlink NAS COUNT value in a NAS security transparent container (see subclause 9.9.2.6).

During handover to or from E-UTRAN, the MME shall increment downlink NAS COUNT by one after it has created a NAS security transparent container (see subclause 9.9.2.6 and 9.9.2.7).

NOTE 2: During the handover from UTRAN/GERAN to E-UTRAN, the NAS security transparent container (see subclause 9.9.2.7) is treated as an implicit SECURITY MODE COMMAND message for the UE and the MME, and therefore the MME regards the sending of the NAS security transparent container as the sending of an initial SECURITY MODE COMMAND message in order to derive and take into use a mapped EPS security context for the purpose of the NAS COUNT handling.

In some NAS messages only 5 of the 8 NAS sequence number bits are transmitted. When this is the case, the receiver shall estimate the remaining 3 most significant bits of the sequence number.

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