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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.301** | **CR** | **3358** | **rev** | **1** | **Current version:** | **16.4.0** |  |
|  | | | | | | | | |
| *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:*** | Single-registration mode without N26 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc16 | | | | |  | ***Date:*** | | | 2020-03-26 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The UE supporting single-registration mode can work in single-registration mode in following two cases:   1. The network supports N26 interface; and 2. The network does not support N26 interface.   In sub 4.4.3.1, the mapped EPS security context can only be derived in case of N26 is supported.  Finally, the term “***UE operating in single-registration mode in a network supporting N26 interface***” defined in TS 24.501 needs to be resued in TS 24.301. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | For interworking with N1 mode, it proposes to specify that the mapped EPS security context can only be derived in case of N26 is supported. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | For interworking with N1 mode, it does not make sense to derive the mapped EPS security context in case of N26 is not supported. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.1, 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 \* \* \* \*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

The term "mobile station" (MS) in the present document is synonymous with the term "user equipment" (UE) as defined in 3GPP TR 21.905 [1].

**1x CS fallback capable UE:** A UE that uses a CS infrastructure for a voice call and other CS-domain services by falling back to cdma2000® 1x access network if the UE is served by E‑UTRAN when a CS service is requested.

**5G-EA:** 5GS encryption algorithms. The term 5G-EA, 5G-EA0, 128-5G-EA1-3 and 5G-EA4-7 used in the present document corresponds to the term NEA, NEA0, NEA1-3 and NEA4-7 defined in 3GPP TS 33.501 [56].

**5G-IA:** 5GS integrity algorithms. The term 5G-IA, 5G-IA0, 128-5G-IA1-3 and 5G-IA4-7 used in the present document corresponds to the term NIA, NIA0, NIA1-3 and NIA4-7 defined in 3GPP TS 33.501 [56].

**Aggregate maximum bit rate:** The maximum bit rate that limits the aggregate bit rate of a set of non-GBR bearers of a UE. Definition derived from 3GPP TS 23.401 [10].

**APN based congestion control:** Congestion control in session management where the network can reject session management requests from UEs or deactivate PDN connections when the associated APN is congested.

**Attached for emergency bearer services:** A UE is attached for emergency bearer services if it has only a PDN connection for emergency bearer services established.

**Attached for access to RLOS:** A UE is attached for access to RLOS if the UE requestsed access to RLOS during the attach procedure and has a PDN connection for RLOS established after completion of attach procedure.

**Chosen PLMN:** The same as selected PLMN as specified in 3GPP TS 23.122 [6].

**Control plane CIoT EPS optimization:** signalling optimizations to enable efficient transport of user data (IP, non-IP, Ethernet or SMS) over control plane via the MME including optional header compression of IP data.

**User plane CIoT EPS optimization:** signalling optimizations to enable efficient transport of user data (IP, non-IP or Ethernet) over the user plane.

**UE supporting CIoT EPS optimizations:** A UE that supports control plane CIoT EPS optimization or user plane CIoT EPS optimization and one or more other CIoT EPS optimizations when the UE is in S1 mode.

**Attached for EPS services with CP-CIoT EPS optimization:** A UE supporting CIoT EPS optimizations is attached for EPS services, and control plane CIoT EPS optimization along with one or more other CIoT EPS optimizations have been accepted by the network.

**Attached for EPS services with User plane CIoT EPS optimization:** A UE supporting CIoT EPS optimizations is attached for EPS services, and user plane CIoT EPS optimization along with one or more other CIoT EPS optimizations have been accepted by the network.

**Attached for EPS services with CIoT EPS optimization:** A UE is attached for EPS services with CP-CIoT EPS optimization or attached for EPS services with user plane CIoT EPS optimization.

**CS fallback cancellation request:** A request received from the MM sublayer to cancel a mobile originating CS fallback.

**CS fallback capable UE:** A UE that uses a CS infrastructure for a voice call and other CS-domain services by falling back to A/Gb or Iu mode if the UE is served by E‑UTRAN when a CS service is requested.

**CSG cell:** A cell in which only members of the CSG can get normal service. Depending on local regulation, the CSG cell can provide emergency bearer services also to subscribers who are not member of the CSG. Definition derived from 3GPP TS 23.401 [10].

**CSG ID:** A CSG ID is a unique identifier within the scope of one PLMN defined in 3GPP TS 23.003 [2] which identifies a Closed Subscriber Group (CSG) in the PLMN associated with a cell or group of cells to which access is restricted to members of the CSG.

**CSG selection**: A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs. Definition derived from 3GPP TS 23.122 [6].

**Dedicated bearer:** An EPS bearer that is associated with uplink packet filters in the UE and downlink packet filters in the PDN GW where the filters only match certain packets. Definition derived from 3GPP TS 23.401 [10].

**Default bearer:** An EPS bearer that gets established with every new PDN connection. Its context remains established throughout the lifetime of that PDN connection. A default EPS bearer is a non-GBR bearer. Definition derived from 3GPP TS 23.401 [10].

**Emergency EPS bearer context:** A default EPS bearer context which was activated with request type "emergency" or "handover of emergency bearer services", or any dedicated EPS bearer context associated to this default EPS bearer context.

**EMM context:** An EMM context is established in the UE and the MME when an attach procedure is successfully completed.

**EMM-CONNECTED mode:** A UE is in EMM-CONNECTED mode when a NAS signalling connection between UE and network is established. The term EMM-CONNECTED mode used in the present document corresponds to the term ECM-CONNECTED state used in 3GPP TS 23.401 [10].

**EMM-IDLE mode:** A UE is in EMM-IDLE mode when no NAS signalling connection between UE and network exists or when RRC connection suspend has been indicated by lower layers. The term EMM-IDLE mode used in the present document corresponds to the term ECM-IDLE state used in 3GPP TS 23.401 [10].

**EPS security context:** In the present specification, EPS security context is used as a synonym for EPS NAS security context specified in 3GPP TS 33.401 [19].

**EPS services:** Services provided by PS domain. Within the context of this specification, EPS services is used as a synonym for GPRS services in 3GPP TS 24.008 [13].

**Evolved packet core network:** The successor to the 3GPP Release 7 packet-switched core network, developed by 3GPP within the framework of the 3GPP System Architecture Evolution (SAE).

**Evolved packet system:** The evolved packet system (EPS) or evolved 3GPP packet-switched domain consists of the evolved packet core network and the evolved universal terrestrial radio access network. Definition derived from 3GPP TS 23.401 [10].

**GBR bearer:** An EPS bearer that uses dedicated network resources related to a guaranteed bit rate (GBR) value, which are permanently allocated at EPS bearer establishment/modification. Definition derived from 3GPP TS 23.401 [10].

**General NAS level mobility management congestion control:** The type of congestion control that is applied at a general overload or congestion situation in the network, e.g. lack of processing resources.

**Group specific session management congestion control:** Type of congestion control at session management level that is applied to reject session management requests from UEs belonging to a particular group when one or more group congestion criteria as specified in 3GPP TS 23.401 [10] are met.

**Highest ranked ACDC category: The** ACDC category with the lowest value as defined in 3GPP TS 24.105 [35].

**Initial NAS message:** A NAS message is considered as an initial NAS message, if this NAS message can trigger the establishment of a NAS signalling connection. For instance, the ATTACH REQUEST message is an initial NAS message.

**IPv4v6 capability:** Capability of the IP stack associated with a UE to support a dual stack configuration with both an IPv4 address and an IPv6 address allocated.

**Kilobit:** 1000 bits.

**Last Visited Registered TAI:** A TAI which is contained in the TAI list that the UE registered to the network and which identifies the tracking area last visited by the UE.

**Linked Bearer Identity:** This identity indicates to which default bearer the additional bearer resource is linked.

**LIPA PDN connection:** A PDN connection, for which the default EPS bearer context or default PDP context was activated with an APN authorized to use LIPA. The network authorizes an APN for using LIPA based on the subscription profile (see 3GPP TS 29.272 [16C]) and subsequently the network considers this PDN connection a LIPA PDN connection.

**Lower layer failure**: A failure reported by the AS to the NAS that cannot be corrected on AS level. When the AS indicates a lower layer failure to NAS, the NAS signalling connection is not available.

**Mapped EPS security context:** A mapped security context to be used in EPS. Definition derived from 3GPP TS 33.401 [19].

**Mapped GUTI:** A GUTI which is mapped from a P-TMSI and an RAI allocated previously by an SGSN. Mapping rules are defined in 3GPP TS 23.003 [2]. Definition derived from 3GPP TS 23.401 [10].

**Megabit:** 1,000,000 bits.

**Message header:** A standard L3 message header as defined in 3GPP TS 24.007 [12].

**MME area:** An area containing tracking areas served by an MME.

**MO MMTEL voice call is started**: the MO-MMTEL-voice-started indication was received from upper layers (see 3GPP TS 24.173 [13E]) and after reception of the MO-MMTEL-voice-started indication, the MO-MMTEL-voice-ended indication has not been received.

**MO MMTEL video call is started**: the MO-MMTEL-video-started indication was received from upper layers (see 3GPP TS 24.173 [13E]) and after reception of the MO-MMTEL-video-started indication, the MO-MMTEL-video-ended indication has not been received.

**MO SMSoIP is started**: the MO-SMSoIP-attempt-started indication was received from upper layers (see 3GPP TS 24.341 [15D]) and after reception of the MO-SMSoIP-attempt-started indication, the MO-SMSoIP-attempt-ended indication has not been received.

**NAS level mobility management congestion control:** Congestion control mechanism in the network in mobility management. "NAS level mobility management congestion control" consists of "subscribed APN based congestion control" and "general NAS level mobility management congestion control".

**NAS signalling connection:** A peer to peer S1 mode connection between UE and MME. A NAS signalling connection consists of the concatenation of an RRC connection via the "LTE-Uu" interface and an S1AP connection via the S1 interface. Additionally, for the purpose of optimized handover or idle mode mobility from cdma2000® HRPD access to E‑UTRAN (see 3GPP TS 23.402 [11]), the NAS signalling connection can consist of a concatenation of an S101‑AP connection and a signalling tunnel over a cdma2000® HRPD access network.

NOTE 1: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

**NAS signalling connection recovery**: A mechanism initiated by the NAS to restore the NAS signalling connection on indication of "RRC connection failure" by the lower layers.

**Native GUTI:** A GUTI previously allocated by an MME. Definition derived from 3GPP TS 23.401 [10].

**Non-access stratum protocols:** The protocols between UE and MSC or SGSN that are not terminated in the UTRAN, and the protocols between UE and MME that are not terminated in the E-UTRAN. Definition derived from 3GPP TR 21.905 [1].

**Non-emergency EPS bearer context:** Any EPS bearer context which is not an emergency EPS bearer context.

**Non-EPS services:** Services provided by CS domain. Within the context of this specification, non-EPS services is used as a synonym for non-GPRS services in 3GPP TS 24.008 [13]. A UE which camps on E-UTRAN can attach to both EPS services and non-EPS services.

**Non-GBR bearer:** An EPS bearer that uses network resources that are not related to a guaranteed bit rate (GBR) value. Definition derived from 3GPP TS 23.401 [10].

**PDN address:** An IP address assigned to the UE by the Packet Data Network Gateway (PDN GW).

**PDN connection for emergency bearer services:** A PDN connection for which the default EPS bearer context or default PDP context was activated with request type "emergency" or "handover of emergency bearer services".

**PDN connection for RLOS:** A PDN connection for which the default EPS bearer context was activated with request type "RLOS".

**Plain NAS message:** A NAS message with a header including neither a message authentication code nor a sequence number.

**Persistent EPS bearer context:** either a non-emergency EPS bearer context representing a GBR bearer with QoS equivalent to QoS of teleservice 11 and where there is a radio bearer associated with that context, or an emergency EPS bearer context where there is a radio bearer associated with that context.

NOTE 2: An example of a persistent EPS bearer context is a non-emergency EPS bearer context with QCI = 1 where there is a radio bearer associated with that context.

**Procedure Transaction Identity:** An identity which is dynamically allocated by the UE for the UE requested ESM procedures. The procedure transaction identity is released when the procedure is completed.

**RAT-related TMSI:** When the UE is camping on an E-UTRAN cell, the RAT-related TMSI is the GUTI; when it is camping on a GERAN or UTRAN cell, the RAT-related TMSI is the P-TMSI.

**Registered PLMN**: The PLMN on which the UE is registered. The identity of the registered PLMN is provided to the UE within the GUTI.

**Relay node:** A network element in the E-UTRAN, wirelessly connected to an eNode B and providing relaying function to UEs served by the E-UTRAN. Definition derived from 3GPP TS 23.401 [10].

**Removal of eCall only mode restriction:** All the limitations as described in 3GPP TS 22.101 [46] for the eCall only mode do not apply any more.

**RLOS EPS bearer context:** A default RLOS EPS bearer context which was activated with request type "RLOS", or any dedicated EPS bearer context associated to this default EPS bearer context.

The label **(S1 mode only)** indicates that this subclause or paragraph applies only to a system which operates in S1 mode, i.e. with a functional division that is in accordance with the use of an S1 interface between the radio access network and the core network. The S1 mode includes WB-S1 mode and NB-S1 mode. In a multi-access system this case is determined by the current serving radio access network.

**In NB-S1 mode:** Indicates this paragraph applies only to a system which operates in NB-S1 mode. For a multi-access system this case applies if the current serving radio access network provides access to network services via E-UTRA by NB-IoT (see 3GPP TS 36.300 [20], 3GPP TS 36.331 [22], 3GPP TS 36.306 [44]).

**In WB-S1 mode:** Indicates this paragraph applies only to a system which operates in WB-S1 mode. For a multi-access system this case applies if the system operates in S1 mode, but not in NB-S1 mode.

**In WB-S1/CE mode:** Indicates this paragraph applies only when a UE, which is a CE mode B capable UE (see 3GPP TS 36.306 [44]), is operating in CE mode A or B in WB-S1 mode.

**SCEF PDN Connection:** A PDN connection established between the UE and the Service Capability Exposure Function (SCEF) for transmitting the UE's non-IP data related to a specific application.

**SGi PDN Connection:** A PDN connection established between the UE and the Packet Gateway (P-GW) for transmitting the UE's IP, non-IP or Ethernet data related to a specific application.

**S101 mode:** Applies to a system that operates with a functional division that is in accordance with the use of an S101 interface. For the definition of the S101 reference point, see 3GPP TS 23.402 [11].

**SIPTO at the local network PDN connection:** A PDN connection, for which the default EPS bearer context or default PDP context was activated with an APN authorized to use SIPTO at the local network and it was activated such that the traffic of the PDN connection will be using an L-GW. The network authorizes an APN for using SIPTO at the local network based on the subscription profile (see 3GPP TS 29.272 [16C]) and subsequently the network considers this PDN connection a SIPTO at the local network PDN connection. SIPTO at the local network PDN connection can be of IP, non-IP or Ethernet PDN type.

**SIPTO at the local network PDN connection with a collocated L-GW:** A SIPTO at the local network PDN connection which is established to a L-GW function collocated with the (H)(e)NodeB. The core-network entity (i.e. the MME or the SGSN) can be aware of whether the SIPTO at the local network PDN connection with a collocated L-GW is used when the PDN connection is established.

**SIPTO at the local network PDN connection with a stand-alone GW:** A SIPTO at the local network PDN connection which is established to a stand-alone GW (with collocated L-GW and S-GW). The core-network entity (i.e. the MME or the SGSN) can be aware of whether the SIPTO at the local network PDN connection with a stand-alone GW is used when the PDN connection is established.

**"SMS only":** A subset of services which includes only Short Message Service. A UE camping on E-UTRAN can attach to both EPS services and "SMS only".

**SMS over NAS**: refers to SMS in MME or SMS over SGs.

**SMS over S102**: refers to SMS which uses 1xCS procedures in EPS as defined in 3GPP TS 23.272 [9].

**Subscribed APN based congestion control:** Congestion control in mobility management where the network can reject attach requests from UEs with a certain APN in the subscription.

**TAI list:** A list of TAIs that identify the tracking areas that the UE can enter without performing a tracking area updating procedure. The TAIs in a TAI list assigned by an MME to a UE pertain to the same MME area.

**Traffic flow aggregate:** A temporary aggregate of packet filters that are included in a UE requested bearer resource allocation procedure or a UE requested bearer resource modification procedure and that is inserted into a traffic flow template (TFT) for an EPS bearer context by the network once the UE requested bearer resource allocation procedure or UE requested bearer resource modification procedure is completed.

**UE configured for dual priority:** A UE which provides dual priority support is configured for NAS signalling low priority and also configured to override the NAS signalling low priority indicator (see 3GPP TS 24.368 [15A], 3GPP TS 31.102 [17]).

**UE configured to use AC11 – 15 in selected PLMN:** A UE configured with at least one access class in the range 11-15 on the USIM, and the access class is applicable in the selected PLMN according to 3GPP TS 22.011 [1A].

**UE's availability for voice calls in the IMS:** The indication of this availability or non-availability is provided by the upper layers of the UE as specified in 3GPP TS 24.229 [13D] in the annex relevant to the IP-Connectivity Access Network in use or determined in the NAS layer, as specified in subclause 4.3.1. If availability is indicated, the UE uses the IM CN Subsystem and can terminate or originate requests for SIP sessions including an audio component with codecs suited for voice.

**UE's usage setting:** This is a UE setting that indicates whether the UE has preference for voice services over data services or vice-versa. If a UE has preference for voice services, then the UE's usage setting is "voice centric". If a UE has preference for data services, then the UE's usage setting is "data centric". A UE whose setting is "data centric" may still require access to voice services. A UE whose setting is "voice centric" may still require access to data services. This definition is derived from 3GPP TS 23.221 [8A] and it applies to voice capable UEs. If the UE is capable of both S1 mode and N1 mode, there is a single UE's usage setting which applies to both 5GS and EPS (see 3GPP TS 24.501 [54]).

**UE using EPS services with control plane CIoT EPS optimization:** AUE that is attached for EPS services with the control plane CIOT EPS optimization accepted by the network.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.221 [8A] apply:

**Restricted local operator services**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [10] apply:

**APN rate control status**

**Cellular IoT (CIoT)**

**DCN-ID**

**eCall only mode**

**NarrowBand-IoT**

**Dedicated core network**

**PDN connection**

**Service Gap Control**

**UE paging probability information**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.272 [9] apply:

**CS fallback**

**SMS in MME**

**SMS over SGs**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.682 [11A] apply:

**SCEF**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.008 [13] apply:

**A/Gb mode**

**Access domain selection**

**Default PDP context**

**Extended idle-mode DRX cycle**

**Iu mode**

**Power saving mode**

**PS signalling connection**

**RR connection**

**TFT**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.102 [18] apply:

**UMTS security context**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.401 [19] apply:

**Current EPS security context**

**Full native EPS security context**

**KASME**

**K'ASME**

**Mapped security context**

**Native EPS security context**

**Non-current EPS security context**

**Partial native EPS security context**

**Data via MME**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [6] apply:

**Country**

**EHPLMN**

**HPLMN**

**Shared Network**

**Suitable Cell**

**VPLMN**

**Limited Service State**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.216 [8] apply:

**SRVCC**

**vSRVCC**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.011 [1A] apply:

**Extended Access Barring**

**Application specific Congestion control for Data Communication (ACDC)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.003 [10] apply:

**Local Home Network Identifier**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.303 [31] apply:

**ProSe direct communication**

**ProSe direct discovery**

**ProSe UE-to-Network Relay**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.161 [36] apply:

**Multi-access PDN connection**

**NBIFOM**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.167 [45] apply:

**eCall over IMS**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.501 [54] apply:

**5GMM-CONNECTED mode**

**5GMM-DEREGISTERED**

**5GMM-DEREGISTERED-INITIATED**

**5GMM-IDLE mode**

**5GMM-NULL**

**5GMM-****REGISTERED**

**5GMM-REGISTERED-INITIATED**

**5GMM-SERVICE-REQUEST-INITIATED**

**Applicable UE radio capability ID for the current UE radio configuration in the selected network**

**Control plane CIoT 5GS optimization**

**N1 mode**

**NB-N1 mode**

**UE operating in single-registration mode in a network supporting N26 interface**

**User plane CIoT 5GS optimization**

\* \* \* Next 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 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.

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 \* \* \* \*