**3GPP TSG-CT WG4 Meeting #97eC4-202147**

**E-Meeting, 15th – 24th April 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.274** | **CR** | **1984** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Support of inter-RAT HO from NR SA to EN-DC | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | NTT DOCOMO | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2020-04-08 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | As described in CR#2127 of TS 23.502 (available in S2-2002551), access restriction for subscription profile needs to be provided from AMF to MME during inter RAT handover from NR SA to EN-DC in order to support adequate SGW selection at MME, as well as to avoid allocating unnecessary resources for secondary RAT at EPC in case it is restricted. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that access restriction can be sent from AMF to MME for the purpose of (1) adequate SGW selection at MME based on subscription profile, and (2) to avoid allocating unnecessary resources for secondary RAT at EPC if it is restricted, during inter RAT handover from NR SA to EN-DC. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Mis-alignment with stage2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.38 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\***

## 8.38 MM Context

The MM Context information element contains the Mobility Management, UE security parameters that are necessary to transfer over S3/S16/S10/N26 interface.

All Spare bits are set to zeros by the sender and ignored by the receiver. Spare bits in MM Context IE shall be set to 1's before sending MM Context IE to Gn/Gp SGSN.

NOTE 1: The encoding of Spare bits in MM Context IE is different between GTPv1 and GTPv2. Spare bits in GTPv1 in MM Context IE there are set to 1s.

Security Mode indicates the type of security keys (GSM/UMTS/EPS) and Authentication Vectors (quadruplets /quintuplets/triplets) that are passed to the new MME/SGSN/AMF.

The DRX parameter coding is specified in clause 10.5.5.6 of 3GPP TS 24.008 [5]. If DRXI (DRX Indicator), bit 4 of octet 5, is set to "1", then the DRX parameter field is present, otherwise its octets are not present.

Uplink/downlink Subscribed UE AMBR (Aggregate Maximum Bit Rate) is coded as Unsigned32 integer values in kbps (1000 bps) for all non-GBR bearers according to the subscription of the user. The uplink/downlink Subscribed UE AMBR requires converting values in bits per second to kilobits per second when it is received from the HSS. If such conversions result in fractions, then the uplink/downlink Subscribed UE AMBR values shall be rounded upwards. If SAMBRI (Subscribed UE AMBR Indicator), bit 1 of octet 6, is set to "1", then the Uplink/downlink Subscribed UE AMBR parameter field is present, otherwise these parameters are not present. If no Subscribed UE AMBR is received from the HSS, the SAMBRI shall be set to "0".Uplink/downlink Used UE AMBR (Aggregate Maximum Bit Rate) is coded as Unsigned32 integer values in kbps (1000 bps) for all non-GBR bearers currently being used by the UE. If UAMBRI (Used UE AMBR Indicator), bit 2 of octet 6, is set to "1", then the Uplink/downlink Used UE AMBR parameter field is present, otherwise these parameters are not present.

The encoding of Mobile Equipment Identity (MEI) field shall be same as specified in clause 8.10 of this specification. If Length of Mobile Equipment Identity is zero, then the Mobile Equipment Identity parameter shall not be present. If the UE is emergency or RLOS attached and the UE is UICCless or the IMSI is unauthenticated, Mobile Equipment Identity (MEI) shall be used as the UE identity.

The UE Network Capability coding is specified in clause 9.9.3.34 of 3GPP TS 24.301 [23]. If Length of UE Network Capability is zero, then the UE Network Capability parameter shall not be present.

The MS Network Capability coding is specified in clause 10.5.5.12 of 3GPP TS 24.008 [5]. If Length of MS Network Caapability is zero, then the MS Network Capability parameter shall not be present.

The Voice Domain Preference and UE's Usage Setting coding is specified in clause 10.5.5.28 of 3GPP TS 24.008 [5]. If Length of Voice Domain Preference and UE's Usage Setting is zero, then the Voice Domain Preference and UE's Usage Setting parameter shall not be present.

Used Cipher indicates the GSM ciphering algorithm that is in use.

Used NAS Cipher indicates the EPS ciphering algorithm that is in use.

The Access restriction data is composed of UNA(UTRAN Not Allowed), GENA(GERAN Not Allowed), GANA(GAN Not Allowed), INA(I-HSPA-Evolution Not Allowed), ENA(WB-E-UTRAN Not Allowed), NBNA( NB-IoT Not Allowed), ECNA (Enhanced Coverage Not Allowed) and HNNA(HO-To-Non-3GPP-Access Not Allowed).

If the SGSN support the Higher bitrates than 16 Mbps flag, the Higher bitrates than 16 Mbps flag shall be included in the MM Context if:

- the source S4-SGSN has received "Higher bitrates than 16 Mbps flag" in the RANAP Initial UE Message or in RANAP Relocation Complete as defined in TS 25.413 [33] from the RNC, or

- the source S4-SGSN has stored the "Higher bitrates than 16 Mbps flag" (received from an SGSN via the Identification Response, Context Response or Forward Relocation Request during earlier procedures).

The S4-SGSN shall set the "Higher bitrates than 16 Mbps flag" to "1" if "Higher bitrates than 16 Mbps flag" is "allowed" and to "0" if it is "not allowed". The Length of Higher bitrates than 16 Mbps flag shall be set to zero if the S4-SGSN has not received the "Higher bitrates than 16 Mbps flag".

As depicted in Figure 8.38-1, the GSM Key, Used Cipher and Authentication Triplets that are unused in the old SGSN shall be transmitted to the new SGSN for the GSM subscribers. An array of at most 5 Authentication Triplets may be included. The field 'Number of Triplet' shall be set to the value '0' if no Authentication Triplet is included (i.e. octets '16 to h' are absent).

The Authentication Triplet coding is specified in Figure 8.38-7.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 | Type = 103 (decimal) | | | | | | | |  |
|  | 2 to 3 | Length = n | | | | | | | |  |
|  | 4 | Spare | | | | Instance | | | |  |
|  | 5 | Security Mode | | | Spare | DRXI | CKSN | | |  |
|  | 6 | Number of Triplet | | | Spare | | | UAMBRI | SAMBRI |  |
|  | 7 | Spare | | | | | Used Cipher | | |  |
|  | 8 to 15 | Kc | | | | | | | |  |
|  | 16 to h | Authentication Triplet [1..5] | | | | | | | |  |
|  | (h+1) to (h+2) | DRX parameter | | | | | | | |  |
|  | j to (j+3) | Uplink Subscribed UE AMBR | | | | | | | |  |
|  | (j+4) to (j+7) | Downlink Subscribed UE AMBR | | | | | | | |  |
|  | i to (i+3) | Uplink Used UE AMBR | | | | | | | |  |
|  | (i+4) to (i+7) | Downlink Used UE AMBR | | | | | | | |  |
|  | q | Length of UE Network Capability | | | | | | | |  |
|  | (q+1) to k | UE Network Capability | | | | | | | |  |
|  | k+1 | Length of MS Network Capability | | | | | | | |  |
|  | (k+2) to m | MS Network Capability | | | | | | | |  |
|  | m+1 | Length of Mobile Equipment Identity (MEI) | | | | | | | |  |
|  | (m+2) to r | Mobile Equipment Identity (MEI) | | | | | | | |  |
|  | r+1 | ECNA | NBNA | HNNA | ENA | INA | GANA | GENA | UNA |  |
|  | r+2 | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | |  |
|  | (r+3) to s | Voice Domain Preference and UE's Usage Setting | | | | | | | |  |
|  | (s+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |  |

Figure 8.38-1: GSM Key and Triplets

As depicted in Figure 8.38-2, the UMTS Key, Used Cipher and Authentication Quintuplets that are unused in the old SGSN shall be transmitted to the new SGSN when the UMTS subscriber is attached to a GSM BSS in the old system, in case the user has a ME capable of UMTS AKA. An array of at most 5 Authentication Quintuplets may be included. The field 'Number of Quintuplets' shall be set to the value '0' if no Authentication Quintuplet is included (i.e. octets '40 to h' are absent).

If the UGIPAI (Used GPRS integrity protection algorithm Indicator), bit 3 of octet 6, is set to 1, then bits 4 to 6 of octet 7 shall contain the Used GPRS integrity protection algorithm field, otherwise these bits shall be set to 0 and ignored by the receiver.

The GUPII (GPRS User Plane Integrity Indicator), bit 4 of octet 6, shall be set to 1 if the subscriber profile indicated that user plane integrity protection is required and set to 0 otherwise.

NOTE 2: The encoding of the bits is not identical with GTPv1 as the spare bits are encoded differently.

The source S4-SGSN shall include the IOV\_updates counter if it is supported and available. The IOV\_updates counter is encoded as an integer with a length of 1 octet. The use of the IOV\_updates counter is specified in 3GPP TS 43.020 [78]. If IOVI (IOV\_updates Indicator), bit 5 of octet 6, is set to "1", then the IOV\_updates counter parameter field shall be present, otherwise it shall not be present.

The Authentication Quintuplet coding is specified in Figure 8.38-8.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Bits | | | | | | | | | | | | | | | |  | |
|  | | Octets | | 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
|  | | 1 | | Type = 104 (decimal) | | | | | | | | | | | | | | | |  | |
|  | | 2 to 3 | | Length = n | | | | | | | | | | | | | | | |  | |
|  | | 4 | | Spare | | | | | | | | Instance | | | | | | | |  | |
|  | | 5 | | Security Mode | | | | | | Spare | | DRXI | | CKSN/KSI | | | | | |  | |
|  | | 6 | | Number of Quintuplets | | | | | | IOVI | | GUPII | | UGIPAI | | UAMBRI | | SAMBRI | |  | |
|  | | 7 | | Spare | | | | Used GPRS integrity protection algorithm | | | | | | Used Cipher | | | | | |  | |
|  | | 8 to 23 | | CK | | | | | | | | | | | | | | | |  | |
|  | | 24 to 39 | | IK | | | | | | | | | | | | | | | |  | |
|  | | 40 to h | | Authentication Quintuplet [1..5] | | | | | | | | | | | | | | | |  | |
|  | (h+1) to (h+2) | | DRX parameter | | | | | | | | | | | | | | | |  | |
|  | j to (j+3) | | Uplink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (j+4) to (j+7) | | Downlink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | i to (i+3) | | Uplink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (j+12) to (i+4) | | Downlink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | q | | Length of UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | (q+1) to k | | UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | k+1 | | Length of MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | (k+2) to m | | MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | m+1 | | Length of Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | (m+2) to r | | Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | r+1 | | ECNA | | NBNA | | HNNA | | ENA | | INA | | GANA | | GENA | | UNA | |  | |
|  | r+2 | | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | (r+3) to s | | Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | s+1 | | Length of Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | |  | |
|  | s+2 | | Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | |  | |
|  | s+3 | | IOV\_updates counter | | | | | | | | | | | | | | | |  | |
|  | (s+4) to (n+4) | | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | | | | |  | |

Figure 8.38-2: UMTS Key, Used Cipher and Quintuplets

As depicted in Figure 8.38-3, the GSM Key, Used Cipher and Authentication Quintuplets that are unused in the old SGSN shall be transmitted to the new SGSN when the UMTS subscriber is attached to a GSM BSS in the old system, in case the user has a ME no capable of UMTS AKA. An array of at most 5 Authentication Quintuplets may be included. The field 'Number of Quintuplets' shall be set to the value '0' if no Authentication Quintuplet is included (i.e. octets '16 to h' are absent).

The Authentication Quintuplet coding is specified in Figure 8.38-8.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Bits | | | | | | | | | | | | | | | |  | |
|  | | Octets | | 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
|  | | 1 | | Type = 105 (decimal) | | | | | | | | | | | | | | | |  | |
|  | | 2 to 3 | | Length = n | | | | | | | | | | | | | | | |  | |
|  | | 4 | | Spare | | | | | | | | Instance | | | | | | | |  | |
|  | | 5 | | Security Mode | | | | | | Spare | | DRXI | | CKSN/KSI | | | | | |  | |
|  | | 6 | | Number of Quintuplets | | | | | | Spare | | | | | | UAMBRI | | SAMBRI | |  | |
|  | | 7 | | Spare | | | | | | | | | | Used Cipher | | | | | |  | |
|  | | 8 to 15 | | Kc | | | | | | | | | | | | | | | |  | |
|  | | 16 to h | | Authentication Quintuplets [1..5] | | | | | | | | | | | | | | | |  | |
|  | (h+1) to (h+2) | | DRX parameter | | | | | | | | | | | | | | | |  | |
|  | j to (j+3) | | Uplink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (j+4) to (j+7) | | Downlink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | i to (i+3) | | Uplink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (i+4) to (i+7) | | Downlink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | q | | Length of UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | (q+1) to k | | UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | k+1 | | Length of MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | (k+2) to m | | MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | m+1 | | Length of Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | (m+2) to r | | Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | r+1 | | ECNA | | NBNA | | HNNA | | ENA | | INA | | GANA | | GENA | | UNA | |  | |
|  | r+2 | | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | (r+3) to s | | Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | s+1 | | Length of Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | |  | |
|  | s+2 | | Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | |  | |
|  | (s+3) to (n+4) | | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | | | | |  | |

Figure 8.38-3: GSM Key, Used Cipher and Quintuplets

As depicted in Figure 8.38-4, the UMTS Key, KSI and unused Authentication Quintuplets in the old SGSN may be transmitted to the new SGSN/MME when the UMTS subscriber is attached to UTRAN/GERAN in the old system, but it is not allowed to send quintuplets to an MME in a different serving network domain (see 3GPP TS 33.401 [12] clause 6.1.6). The MME may forward the UMTS Key, KSI and unused Authentication Quintuplets which were previously stored back to the same SGSN, for further details, refer to 3GPP TS 33.401 [12]. An array of at most 5 Authentication Quintuplets may be included. The field 'Number of Quintuplets' shall be set to the value '0' if no Authentication Quintuplet is included (i.e. octets '40 to h' are absent).

If the UGIPAI (Used GPRS integrity protection algorithm Indicator), bit 3 of octet 6, is set to 1, then bits 1 to 3 of octet 7 shall contain the Used GPRS integrity protection algorithm field, otherwise these bits shall be set to 0 and ignored by the receiver.

The GUPII (GPRS User Plane Integrity Indicator), bit 4 of octet 6, shall be set to 1 if the subscriber profile indicated that user plane integrity protection is required and set to 0 otherwise.

NOTE 3: The encoding of the bits is not identical with GTPv1 as the spare bits are encoded differently.

The source S4-SGSN shall include the IOV\_updates counter if it is supported and available. The IOV\_updates counter is encoded as an integer with a length of 1 octet. The use of the IOV\_updates counter is specified in 3GPP TS 43.020 [78]. If IOVI (IOV\_updates Indicator), bit 5 of octet 6, is set to "1", then the IOV\_updates counter parameter field shall be present, otherwise it shall not be present.

The Extended Access Restriction Data is to store the extra access restriction data received from the HSS (other than ECNA, NBNA, HNNA, ENA, INA, GANA, GENA and UNA). If Length of Extended Access Restriction Data is zero, then the field of Extended Access Restriction Data shall not be present. The Extended Access Restriction Data is composed of NRSRNA (NR as Secondary RAT Not Allowed). The presence of the Extended Access Restriction Data for the case in UMTS Key as depicted in Figure 8.38-4 is optional.

NOTE: In Figure 8.34-4, including the Extended Access Restriction Data allows optimized selection of SGW in case of handover from GSM/UTRAN to E-UTRAN.

The Authentication Quintuplet coding is specified in Figure 8.38-8.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Bits | | | | | | | | | | | | | | | | |  | |
|  | | Octets | | 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | | |  | |
|  | | 1 | | Type = 106 (decimal) | | | | | | | | | | | | | | | | |  | |
|  | | 2 to 3 | | Length = n | | | | | | | | | | | | | | | | |  | |
|  | | 4 | | Spare | | | | | | | | Instance | | | | | | | | |  | |
|  | | 5 | | Security Mode | | | | | | Spare | | DRXI | | KSI | | | | | | |  | |
|  | | 6 | | Number of Quintuplets | | | | | | IOVI | | GUPII | | UGIPAI | | UAMBRI | | SAMBRI | | |  | |
|  | | 7 | | Spare | | | | | | | | | | Used GPRS integrity protection algorithm | | | | | | |  | |
|  | | 8 to 23 | | CK | | | | | | | | | | | | | | | | |  | |
|  | | 24 to 39 | | IK | | | | | | | | | | | | | | | | |  | |
|  | | 40 to h | | Authentication Quintuplet [1..5] | | | | | | | | | | | | | | | | |  | |
|  | (h+1) to (h+2) | | DRX parameter | | | | | | | | | | | | | | | | |  | |
|  | j to (j+3) | | Uplink Subscribed UE AMBR | | | | | | | | | | | | | | | | |  | |
|  | (j+4) to (j+7) | | Downlink Subscribed UE AMBR | | | | | | | | | | | | | | | | |  | |
|  | i to (i+3) | | Uplink Used UE AMBR | | | | | | | | | | | | | | | | |  | |
|  | (i+4) to (i+7) | | Downlink Used UE AMBR | | | | | | | | | | | | | | | | |  | |
|  | q | | Length of UE Network Capability | | | | | | | | | | | | | | | | |  | |
|  | (q+1) to k | | UE Network Capability | | | | | | | | | | | | | | | | |  | |
|  | k+1 | | Length of MS Network Capability | | | | | | | | | | | | | | | | |  | |
|  | (k+2) to m | | MS Network Capability | | | | | | | | | | | | | | | | |  | |
|  | m+1 | | Length of Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | | |  | |
|  | (m+2) to r | | Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | | |  | |
|  | r+1 | | ECNA | | NBNA | | HNNA | | ENA | | INA | | GANA | | GENA | | UNA | | |  | |
|  | r+2 | | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | | |  | |
|  | (r+3) to s | | Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | | |  | |
|  | s+1 | | Length of Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | | |  | |
|  | s+2 | | Higher bitrates than 16 Mbps flag | | | | | | | | | | | | | | | | |  | |
|  | s+3 | | IOV\_updates counter | | | | | | | | | | | | | | | | |  | |
|  | s+4 | | Length of Extended Access Restriction Data | | | | | | | | | | | | | | | | |  | |
|  | (s+5) to t | | Spare | | | | | | | | | | | | | | | | NRSRNA |  | |
|  | (t+1) to (n+4) | | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | | | | | |  | |

Figure 8.38-4: UMTS Key and Quintuplets

As depicted in Figure 8.38-5, the current EPS Security Context, a non-current EPS Security Context (if available), and unused Authentication Quadruplets in the old MME may be transmitted to the new MME/AMF. If the new MME/AMF is not in the same serving network domain, then only the current EPS Security Context may be transmitted. The mapping of an EPS security context to a 5G security context in the new AMF is specified in 3GPP TS 33.501 [86]. An array of at most 5 Authentication Quadruplets may be included. The field 'Number of Quadruplets' shall be set to the value '0' if no Authentication Quadruplet is included (i.e. octets '46 to g' are absent). Authentication Quintuplets shall not be transmitted to the new MME/AMF (i.e. octets 'g+1 to h' shall be absent) even if the old MME has the Authentication Quintuplets for this UE. The field 'Number of Quintuplets' shall be set to the value '0'. The reasons for not sending Quintuplets are specified in3GPP TS 33.401 [12] clause 6.1.6.

The current EPS Security Context may be transmitted by the old AMF to the new MME, where the mapping of a 5G security context to an EPS security context is specified in 3GPP TS 33.501 [86]. The field 'Number of Quadruplets' and 'Number of Quintuplets' shall be set to the value '0'. The AMF shall not transmit un-used authentication vectors to an MME and shall discard any un-used authentication vectors received from an MME, regardless of whether the MME and AMF pertain to the same or different serving network domains.

The Authentication Quintuplet and Authentication Quadruplet codings are specified in Figure 8.38-8 and Figure 8.38-9 respectively.

The value of the NAS Downlink Count shall be set to the value that shall be used to send the next NAS message.

The value of the NAS Uplink Count shall be set to the largest NAS Uplink Count that was in a successfully integrity verified NAS message.

In Figure 8.38-5, the fields for the Old EPS Security Context (i.e. octets from s to s+64) may be present only in S10 Forward Relocation Request message according to the Rules on Concurrent Running of Security Procedures, which are specified in 3GPP TS 33.401 [12]. The octets for Old EPS Security Context shall be present if the OSCI (Old Security Context Indicator), bit 1 of octet 6) is set to "1"; otherwise they shall not be present.

If NHI\_old (Next Hop Indicator for old EPS Security Context), bit 8 of octet s, is set to "1", then the parameters old NH (Next Hop) and old NCC (Next Hop Chaining Count) shall be present; otherwise the octets for old NH parameter shall not be present and the value of old NCC parameter shall be ignored by the receiver. .

Multiple APN Rate Control Statuses (including the number of packets still allowed in the given time unit, the number of additional exception reports still allowed in the given time unit and the termination time of the current APN Rate Control validity period) may be included by the MME.

The MM context shall contain the APN Rate Control Status(s) for PDN connection which are released and currentlty not re-established. Once a PDN connection is re-established, the related APN Rate Control Status shall be deleted.

The UAMBRI shall be set to "0" by the old AMF, and then the Uplink/downlink Used UE AMBR parameter field are not present.The SAMBRI shall be set to "1" by the old AMF, if the AMF has the Uplink/downlink Subscribed UE AMBR received from the MME, or the Uplink/downlink Subscribed UE AMBR in 5G.

The RLOS indication flag (bit 7 of octet s) shall be set to 1 if the UE is RLOS attached.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Bits | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | Octets | | 8 | | | 7 | | | 6 | | | 5 | | | 4 | | | 3 | | | 2 | | 1 | |  | |
|  | | 1 | | Type = 107 (decimal) | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | 2 to 3 | | Length = n | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | 4 | | Spare | | | | | | | | | | | | Instance | | | | | | | | | |  | |
|  | | 5 | | Security Mode | | | | | | | | | NHI | | | DRXI | | | KSIASME | | | | | | |  | |
|  | | 6 | | Number of Quintuplets | | | | | | | | | Number of Quadruplet | | | | | | | | | UAMBRI | | OSCI | |  | |
|  | | 7 | | SAMBRI | | | Used NAS integrity protection algorithm | | | | | | | | | Used NAS Cipher | | | | | | | | | |  | |
|  | | 8 to 10 | | NAS Downlink Count | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | 11 to 13 | | NAS Uplink Count | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | 14 to 45 | | KASME | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | 46 to g | | Authentication Quadruplet [1..5] | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | (g+1) to h | | Authentication Quintuplet [1..5] | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | (h+1) to (h+2) | | DRX parameter | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | p to (p+31) | | NH | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | p+32 | | Spare | | | | | | | | | | | | | | | NCC | | | | | | |  | |
|  | j to (j+3) | | Uplink Subscribed UE AMBR | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (j+4) to (j+7) | | Downlink Subscribed UE AMBR | | | | | | | | | | | | | | | | | | | | | |  | |
|  | i to (i+3) | | Uplink Used UE AMBR | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (i+4) to (i+7) | | Downlink Used UE AMBR | | | | | | | | | | | | | | | | | | | | | |  | |
|  | q | | Length of UE Network Capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (q+1) to k | | UE Network Capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | k+1 | | Length of MS Network Capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (k+2) to m | | MS Network Capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | m+1 | | Length of Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (m+2) to r | | Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | | | | | | | |  | |
|  | r+1 | | ECNA | | | NBNA | | | HNNA | | | ENA | | | INA | | | GANA | | | GENA | | UNA | |  | |
|  | | s | | NHI\_old | | | RLOS | | | old KSIASME | | | | | | | | | old NCC | | | | | | |  | |
|  | (s+1) to (s+32) | | old KASME | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (s+33) to (s+64) | | old NH | | | | | | | | | | | | | | | | | | | | | |  | |
|  | w | | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (w+1) to t  (t+1) to (t+2)  (t+3) to u | | Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | | | | | | | |  | |
| Length of UE Radio Capability for Paging information | | | | | | | | | | | | | | | | | | | | | |
| UE Radio Capability for Paging information | | | | | | | | | | | | | | | | | | | | | |
|  | u+1 | | Length of Extended Access Restriction Data | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (u+2) to v | | Spare | | Spare | | | Spare | | | NRUNA | | | NRUSRNA | | | NRNA | | | USSRNA | | | NRSRNA | |  | |
|  | v+1 | | Length of UE additional security capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (v+2) to x | | UE additional security capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | x+1 | | Length of UE NR security capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (x+2) to y | | UE NR security capability | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (y+1) to (y+2) | | Length of APN Rate Control Statuses | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (y+3) to l | | APN Rate Control Status [1..z] | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (l+1) | | Length of Core Network Restrictions | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (l+2) to (l+5) | | Core Network Restrictions | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (l+6) | | Length of UE Radio Capability ID | | | | | | | | | | | | | | | | | | | | | |  | |
|  | (l+7) to z | | UE Radio Capability ID | | | | | | | | | | | | | | | | | | | | | |  | |
|  | l+1 to (n+4) | | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | | | | | | | | | | |  | |

Figure 8.38-5: EPS Security Context and Quadruplets

If NHI (Next Hop Indicator), bit 5 of octet 5, is set to "1", then the optional parameters NH (Next Hop) and NCC (Next Hop Chaining Count) are both present, otherwise their octets are not present.

The UE Radio Capability for Paging information is specified in the clause 9.2.1.98 of 3GPP TS 36.413 [10]. If Length of UE Radio Capability for Paging information is zero, then the UE Radio Capability for Paging information shall not be present. The old MME shall, when available, include UE Radio Capability for Paging information to the new MME as specified in the clause 5.11.4 of 3GPP TS 23.401 [4].

The Extended Access Restriction Data is composed of NRSRNA (NR as Secondary RAT Not Allowed), USSRNA (Unlicensed Spectrum in the form of LAA or LWA/LWIP as Secondary RAT Not Allowed), NRNA (NR in 5GS Not Allowed), NRUSRNA (New Radio Unlicensed as Secondary RAT Not Allowed), and of NRUNA (NR-U in 5GS Not Allowed).

NOTE: As specified in clause 4.11.1.2.1 of 3GPP TS 23.502 [83], NRSRNA can be provided via N26 during handover from 5GC to EPC in order to allow MME to make appropriate handling, e.g. SGW selection based on access restriction, or whether or not to allocate resources for secondary RAT during inter RAT handover.

The UE NR security capability coding is specified in clause 9.11.3.54 of 3GPP TS 24.501 [87]. If Length of UE NR security capability is zero, then the field UE NR security capability in octets "(x+2) to y" shall not be present.

The UE NR security capability coding is specified in clause 9.8.3.57 of 3GPP TS 24.501 [87]. If Length of UE NR security capability is zero, then the field UE NR security capability in octets "(x+2) to y" shall not be present.

The Core Network Restrictions coding is specified in clause 7.2.230 of 3GPP TS 29.272 [70]. If Length of Core Network Restrictions is zero, then the field of Core Network Restrictions in octets "(l+2) to (l+5)" shall not be present.

The UE Radio Capability ID is specified in the clause 9.9.3.60 of 3GPP TS24.301 [23]. If Length of UE Radio Capability ID is zero, then the UE Radio Capability ID shall not be present. When supporting the RACS feature, the old MME shall include the PLMN-assigned UE Radio Capability ID if available, otherwise it shall include the Manufacturer-assigned UE Radio Capability ID, to the new MME as specified in the clause 5.11.3a of 3GPP TS 23.401 [4].

As depicted in Figure 8.38-6, the old MME will derive CK' and IK' from KASME and transmit the CK' and IK' to the new SGSN. Authentication Quintuplets, if available, shall be transmitted to the SGSN if, and only if the MME received them from this SGSN earlier, according to 3GPP TS 33.401 [12] clause 6.1.5. An array of at most 5 Authentication Quintuplets may be included. The field 'Number of Quintuplets' shall be set to the value '0' if no Authentication Quintuplet is included (i.e. octets 'g+1 to h' are absent). An array of at most 5 Authentication Quadruplets may be included. The field 'Number of Quadruplets' shall be set to the value '0' if no Authentication Quadruplet is included (i.e. octets '40 to g' are absent). A key KASME shall never be transmitted to an SGSN according to 3GPP TS 33.401 [12] clause 6.4.

The Authentication Quintuplet and Authentication Quadruplet codings are specified in Figure 8.38-8 and Figure 8.38-9 respectively.

The old SGSN/MME may deliver both Authentication Quadruplets and Authentication Quintuplets it holds to the peer combo node to optimize the procedure.

NOTE: 3GPP TS 33.401 [12] states that "EPS authentication data shall not be forwarded from an MME towards an SGSN". The statement above assumes that the old MME can determine by local configuration that the peer node is a combo SGSN/MME (as opposed to a single SGSN).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Bits | | | | | | | | | | | | | | | |  | |
|  | | Octets | | 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
|  | | 1 | | Type = 108 (decimal) | | | | | | | | | | | | | | | |  | |
|  | | 2 to 3 | | Length = n | | | | | | | | | | | | | | | |  | |
|  | | 4 | | Spare | | | | | | | | Instance | | | | | | | |  | |
|  | | 5 | | Security Mode | | | | | | Spare | | DRXI | | KSIASME | | | | | |  | |
|  | | 6 | | Number of Quintuplets | | | | | | Number of Quadruplet | | | | | | UAMBRI | | SAMBRI | |  | |
|  | | 7 | | Spare | | | | | | | | | | | | | | | |  | |
|  | | 8 to 23 | | CK | | | | | | | | | | | | | | | |  | |
|  | | 24 to 39 | | IK | | | | | | | | | | | | | | | |  | |
|  | | 40 to g | | Authentication Quadruplet [1..5] | | | | | | | | | | | | | | | |  | |
|  | | (g+1) to h | | Authentication Quintuplet [1..5] | | | | | | | | | | | | | | | |  | |
|  | (h+1) to (h+2) | | DRX parameter | | | | | | | | | | | | | | | |  | |
|  | j to (j+3) | | Uplink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (j+4) to (j+7) | | Downlink Subscribed UE AMBR | | | | | | | | | | | | | | | |  | |
|  | i to (i+3) | | Uplink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | (i+4) to (i+7) | | Downlink Used UE AMBR | | | | | | | | | | | | | | | |  | |
|  | q | | Length of UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | (q+1) to k | | UE Network Capability | | | | | | | | | | | | | | | |  | |
|  | k+1 | | Length of MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | (k+2) to m | | MS Network Capability | | | | | | | | | | | | | | | |  | |
|  | m+1 | | Length of Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | (m+2) to r | | Mobile Equipment Identity (MEI) | | | | | | | | | | | | | | | |  | |
|  | r+1 | | ECNA | | NBNA | | HNNA | | ENA | | INA | | GANA | | GENA | | UNA | |  | |
|  | r+2 | | Length of Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | (r+3) to s | | Voice Domain Preference and UE's Usage Setting | | | | | | | | | | | | | | | |  | |
|  | (s+1) to (s+2) | | Length of APN Rate Control Statuses | | | | | | | | | | | | | | | |  | |
|  | (s+3) to l | | APN Rate Control Status [0..z] | | | | | | | | | | | | | | | |  | |
|  | (l+1) to (n+4) | | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | | | | |  | |

Figure 8.38-6: UMTS Key, Quadruplets and Quintuplets

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 16 | RAND | | | | | | | |  |
|  | 17 to 20 | SRES | | | | | | | |  |
|  | 21 to 28 | Kc | | | | | | | |  |

Figure 8.38-7: Authentication Triplet

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 16 | RAND | | | | | | | |  |
|  | 17 | XRES Length | | | | | | | |  |
|  | 18 to m | XRES | | | | | | | |  |
|  | (m+1) to (m+16) | CK | | | | | | | |  |
|  | (m+17) to (m+32) | IK | | | | | | | |  |
|  | m+33 | AUTN Length | | | | | | | |  |
|  | (m+34) to n | AUTN | | | | | | | |  |

Figure 8.38-8: Authentication Quintuplet

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 16 | RAND | | | | | | | |  |
|  | 17 | XRES Length | | | | | | | |  |
|  | 18 to k | XRES | | | | | | | |  |
|  | k+1 | AUTN Length | | | | | | | |  |
|  | (k+2) to m | AUTN | | | | | | | |  |
|  | (m+1) to (m+32) | KASME | | | | | | | |  |

Figure 8.38-9: Authentication Quadruplet

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 2 | Length of APN Rate control status | | | | | | | |  |
|  | 3 to 4 | Length of APN | | | | | | | |  |
|  | 5 to k | APN | | | | | | | |  |
|  | (k+1) to (k+4) | Uplink number of packets allowed | | | | | | | |  |
|  | (k+5) to (k+8) | Number of additional exception reports | | | | | | | |  |
|  | (k+9) to (k+12) | Downlink number of packets allowed | | | | | | | |  |
|  | (k+13) to (k+20) | APN Rate Control Status validity Time | | | | | | | |  |

Figure 8.38-10: APN Rate Control Status

For the encoding of APN field see clause 8.6.

Octets (k+13) to (k+20) (APN Rate Control Status validity Time) are coded as the time in seconds relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where binary encoding of the integer part is in the 32 most significant bits and binary encoding of the fraction part in the 32 least significant bits. The fraction part is expressed with a granularity of 1 /2\*\*32 second.

Table 8.38-1: Security Mode Values

|  |  |
| --- | --- |
| Security Type | Value (Decimal) |
| GSM Key and Triplets | 0 |
| UMTS Key, Used Cipher and Quintuplets | 1 |
| GSM Key, Used Cipher and Quintuplets | 2 |
| UMTS Key and Quintuplets | 3 |
| EPS Security Context and Quadruplets | 4 |
| UMTS Key, Quadruplets and Quintuplets | 5 |
| <spare> | 6-7 |

Table 8.38-2: Used NAS Cipher Values

|  |  |
| --- | --- |
| Cipher Algorithm | Value (Decimal) |
| No ciphering | 0 |
| 128-EEA1 | 1 |
| 128-EEA2 | 2 |
| 128-EEA3 | 3 |
| EEA4 | 4 |
| EEA5 | 5 |
| EEA6 | 6 |
| EEA7 | 7 |
| <spare> | 8-15 |

Table 8.38-3: Used Cipher Values

|  |  |
| --- | --- |
| Cipher Algorithm | Value (Decimal) |
| No ciphering | 0 |
| GEA/1 | 1 |
| GEA/2 | 2 |
| GEA/3 | 3 |
| GEA/4 | 4 |
| GEA/5 | 5 |
| GEA/6 | 6 |
| GEA/7 | 7 |

Table 8.38-4: Used NAS integrity protection algorithm Values

|  |  |
| --- | --- |
| Integrity protection Algorithm | Value (Decimal) |
| No integrity protection | 0 |
| 128-EIA1 | 1 |
| 128-EIA2 | 2 |
| 128-EIA3 | 3 |
| EIA4 | 4 |
| EIA5 | 5 |
| EIA6 | 6 |
| EIA7 | 7 |

Table 8.38-5: Used GPRS integrity protection algorithm Values

|  |  |
| --- | --- |
| Integrity protection Algorithm | Value (Decimal) |
| No integrity protection | 0 |
| spare | 1 |
| spare | 2 |
| spare | 3 |
| GIA4 | 4 |
| GIA5 | 5 |
| spare | 6 |
| spare | 7 |

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