**3GPP TSG-CT WG1 Meeting #133-eC1-216583**

**E-meeting, 11-19 November 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.301** | **CR** | 3619 | **rev** | **-** | **Current version:** | **17.4.1** |  |
|  |
| *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:***  | Introduction of user-plane integrity protection in EPS support indication |
|  |  |
| ***Source to WG:*** | Vodafone, Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-10-28 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The stage 2 requirements on user-plane integrity protection (EPS-UPIP) need to be implemented in stage 3.UEs supporting EPS-UPIP shall indicate this capability in the security algorithm octets of the UE Network Capability IE when sending the ATTACH REQUEST and TRACKING AREA UPDATE REQUEST message. Additionally, C1-211461 concluded that the EIA7 bit in the UE network capability IE, from a pure NAS protocol perspective, can be used to signal the EPS-UPIP capability. |
|  |  |
| ***Summary of change:*** | If the UE supports EPS-UPIP, the UE shall set the "EPS-UPIP supported" bit in the UE network capability IE of the ATTACH REQUEST and TRACKING AREA UPDATE REQUEST message. The EPS integrity algorithm EIA7 supported bit (octet 4, bit 1) of UE network capability information element is changed to indicate the EPS-UPIP supported by the UE.Interoperability impact analysisThe changes in this CR are backwards compatible with previous releases of this specification with the following analysis. Pre-Rel-17 MME interworking with Rel-17 UE compliant with this CR:The EIA7 bit in the UE network capability IE is defined to signal the support of “EPS integrity algorithm EIA7”. This bit does not yet have a real use in the NAS protocol and is typically encoded as 0 like a spare bit. Upon receiving this bit sent by a Rel-17 UE supporting EPS-UPIP compliant with this CR, the pre-Rel-17 MME can accept the IE without error diagnosis. |
|  |  |
| ***Consequences if not approved:*** | User-plane integrity protection in EPS does not work. |
|  |  |
| ***Clauses affected:*** | 3.2, 5.5.1.2.2, 5.5.3.2.2, 9.9.3.34, 9.9.3.36 |
|  |  |
|  | **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:*** | While 3GPP TSG-SA has agreed a Rel-17 WID and CRs on EPS-UPIP, 3GPP TSG RAN has not yet agreed a WID to do their stage 3 work. |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\* change \*\*\*\*\*

## 3.2 Abbreviations

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

4G-GUTI 4G-Globally Unique Temporary Identifier

5GCN 5G Core Network

5G-GUTI 5G-Globally Unique Temporary Identifier

5GMM 5GS Mobility Management

5G-RG 5G Residential Gateway

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5GS 5G System

5GSM 5GS Session Management

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G-TMSI 5G Temporary Mobile Subscription Identifier

5QI 5G QoS Identifier

ACS Auto-Configuration Server

AKA Authentication and Key Agreement

AKMA Authentication and Key Management for Applications

A-KID AKMA Key Identifier

A-TID AKMA Temporary Identifier

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

APN Access Point Name

ATSSS Access Traffic Steering, Switching and Splitting

AUSF Authentication Server Function

CAG Closed access group

CGI Cell Global Identity

CHAP Challenge Handshake Authentication Protocol

DDX Downlink Data Expected

DL Downlink

DN Data Network

DNN Data Network Name

DNS Domain Name System

eDRX Extended DRX cycle

DS-TT Device-Side TSN Translator

EUI Extended Unique Identifier

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAC Early Admission Control

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

EAS Edge Application Server

EASDF Edge Application Server Discovery Function

ECIES Elliptic Curve Integrated Encryption Scheme

ECS Edge Configuration Server

EEC Edge Enabler Client

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

EPS-UPIP User-plane integrity protection in EPS

ESM EPS Session Management

FN-RG Fixed Network RG

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

Gbps Gigabits per second

GFBR Guaranteed Flow Bit Rate

GUAMI Globally Unique AMF Identifier

IAB Integrated access and backhaul

IMEI International Mobile station Equipment Identity

IMEISV International Mobile station Equipment Identity and Software Version number

IMSI International Mobile Subscriber Identity

IP-CAN IP-Connectivity Access Network

KSI Key Set Identifier

LADN Local Area Data Network

LCS LoCation Services

LMF Location Management Function

LPP LTE Positioning Protocol

MAC Message Authentication Code

MA PDU Multi-Access PDU

MBS Multicast/Broadcast Services

Mbps Megabits per second

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MUSIM Multi-USIM

N3IWF Non-3GPP Inter-Working Function

N5CW Non-5G-Capable over WLAN

N5GC Non-5G Capable

NAI Network Access Identifier

NITZ Network Identity and Time Zone

NR New Radio

ngKSI Key Set Identifier for Next Generation Radio Access Network

NPN Non-public network

NSAC Network Slice Admission Control

NSACF Network Slice Admission Control Function

NSSAA Network slice-specific authentication and authorization

NSSAAF Network Slice-Specific and SNPN authentication and authorization Function

NSSAI Network Slice Selection Assistance Information

ON-SNPN Onboarding Standalone Non-Public Network

OS Operating System

OS Id OS Identity

PAP Password Authentication Protocol

PCO Protocol Configuration Option

PEI Permanent Equipment Identifier

PNI-NPN Public Network Integrated Non-Public Network

ProSe Proximity based Services

ProSeP 5G ProSe policy

PTI Procedure Transaction Identity

PVS Provisioning Server

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

RACS Radio Capability Signalling Optimisation

(R)AN (Radio) Access Network

RFSP RAT Frequency Selection Priority

RG Residential Gateway

RPLMN Registered PLMN

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSNPN Registered SNPN

S-NSSAI Single NSSAI

SA Security Association

SDF Service Data Flow

SMF Session Management Function

SGC Service Gap Control

SNN Serving Network Name

SNPN Stand-alone Non-Public Network

SOR Steering of Roaming

SOR-CMCI Steering of Roaming Connected Mode Control Information

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

Tbps Terabits per second

TMGI Temporary Mobile Group Identity

TNGF Trusted Non-3GPP Gateway Function

TSC Time Sensitive Communication

TSCTSF Time Sensitive Communication and Time Synchronization Function

TWIF Trusted WLAN Interworking Function

TSN Time-Sensitive Networking

UAS Uncrewed Aerial System

UAV Uncrewed Aerial Vehicle

UDM Unified Data Management

UL Uplink

UPDS UE policy delivery service

UPF User Plane Function

UPSC UE Policy Section Code

UPSI UE Policy Section Identifier

URN Uniform Resource Name

URSP UE Route Selection Policy

USS UAS Service Supplier

UUAA USS UAV Authorization/Authentication

V2X Vehicle-to-Everything

V2XP V2X policy

W-AGF Wireline Access Gateway Function

WLAN Wireless Local Area Network

WUS Wake-up signal

Editor's note: While 3GPP TSG-SA has agreed a Rel-17 WID and CRs on EPS-UPIP, 3GPP TSG- RAN has not yet agreed a WID to do their stage 3 work.

\*\*\*\*\* change \*\*\*\*\*

##### 5.5.1.2.2 Attach procedure initiation

In state EMM-DEREGISTERED, the UE initiates the attach procedure by sending an ATTACH REQUEST message to the MME, starting timer T3410 and entering state EMM-REGISTERED-INITIATED (see example in figure 5.5.1.2.2.1). If timer T3402 is currently running, the UE shall stop timer T3402. If timer T3411 is currently running, the UE shall stop timer T3411.

The UE shall include the IMSI in the EPS mobile identity IE in the ATTACH REQUEST message if the selected PLMN is neither the registered PLMN nor in the list of equivalent PLMNs and:

a) the UE is configured for "AttachWithIMSI" as specified in 3GPP TS 24.368 [15A] or 3GPP TS 31.102 [17]; or

b) the UE is in NB-S1 mode.

For all other cases, the UE shall handle the EPS mobile identity IE in the ATTACH REQUEST message as follows:

a) if the UE operating in the single-registration mode is performing an inter-system change from N1 mode to S1 mode or the UE was previously registered in N1 mode before entering state 5GMM-DEREGISTERED and:

1) the UE has received the interworking without N26 interface indicator set to "interworking without N26 interface supported" from the network and:

i) if the UE holds a valid GUTI, the UE shall include the valid GUTI into the EPS mobile identity IE, include Old GUTI type IE with GUTI type set to "native GUTI" and include the UE status IE with a 5GMM registration status set to:

- "UE is in 5GMM-REGISTERED state" if the UE is in 5GMM-REGISTERED state; or

- "UE is in 5GMM-DEREGISTERED state" if the UE is in 5GMM-DEREGISTERED state; or

ii) if the UE does not hold a valid GUTI, the UE shall include the IMSI in the EPS mobile identity IE; or

2) the UE has received the interworking without N26 interface indicator set to "interworking without N26 interface not supported" from the network and:

i) if the UE holds a valid 5G-GUTI, the UE shall include a GUTI, mapped from 5G-GUTI into the EPS mobile identity IE, include Old GUTI type IE with GUTI type set to "native GUTI" and include the UE status IE with a 5GMM registration status set to "UE is in 5GMM-DEREGISTERED state";

ii) if the UE holds a valid GUTI and does not hold a valid 5G-GUTI, the UE shall indicate the GUTI in the EPS mobile identity IE and include Old GUTI type IE with GUTI type set to "native GUTI"; or

iii) if the UE holds neither a valid GUTI nor a valid 5G-GUTI, the UE shall include the IMSI in the EPS mobile identity IE; or

NOTE 1: The value of the EMM registration status included by the UE in the UE status IE is not used by the MME.

b) otherwise:

1) if the UE supports neither A/Gb mode nor Iu mode, the UE shall include in the ATTACH REQUEST message a valid GUTI together with the last visited registered TAI, if available. In addition, the UE shall include Old GUTI type IE with GUTI type set to "native GUTI". If there is no valid GUTI available, the UE shall include the IMSI in the ATTACH REQUEST message; or

2) If the UE supports A/Gb mode or Iu mode or both and:

i) if the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI and RAI, the UE shall map the P-TMSI and RAI into the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "mapped GUTI". If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE. Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE;

NOTE 2: The mapping of the P-TMSI and the RAI to the GUTI is specified in 3GPP TS 23.003 [2].

ii) if the TIN indicates "GUTI" or "RAT-related TMSI" and the UE holds a valid GUTI, the UE shall indicate the GUTI in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI";

iii) if the TIN is deleted and:

- the UE holds a valid GUTI, the UE shall indicate the GUTI in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI";

- the UE does not hold a valid GUTI but holds a valid P-TMSI and RAI, the UE shall map the P-TMSI and RAI into the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "mapped GUTI". If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE; or

- the UE does not hold a valid GUTI, P-TMSI or RAI, the UE shall include the IMSI in the EPS mobile identity IE; or

iv) otherwise the UE shall include the IMSI in the EPS mobile identity IE.

If the UE is operating in the dual-registration mode and it is in 5GMM state 5GMM-REGISTERED, the UE shall include the UE status IE with the 5GMM registration status set to "UE is in 5GMM-REGISTERED state".

NOTE 3: The value of the EMM registration status included by the UE in the UE status IE is not used by the MME.

If the UE is attaching for emergency bearer services and does not hold a valid GUTI, P-TMSI or IMSI as described above, the IMEI shall be included in the EPS mobile identity IE.

If the UE in limited service state is attaching for access to RLOS and does not hold a valid GUTI, P-TMSI or IMSI as described above, the IMEI shall be included in the EPS mobile identity IE.

If the UE supports A/Gb mode or Iu mode or if the UE needs to indicate its UE specific DRX parameter to the network, the UE shall include the UE specific DRX parameter in the DRX parameter IE in the ATTACH REQUEST message. If the UE in NB-S1 mode needs to indicate the UE specific DRX parameter in NB-S1 mode to the network, it shall include the UE specific DRX parameter in NB-S1 mode in the DRX parameter in NB-S1 mode IE in the ATTACH REQUEST message.

If the UE supports eDRX and requests the use of eDRX, the UE shall include the extended DRX parameters IE in the ATTACH REQUEST message.

If the UE supports WUS assistance, then the UE shall set the WUSA bit to "WUS assistance supported" in the UE network capability IE, and if the UE is not attaching for emergency bearer services, the UE may include its UE paging probability information in the Requested WUS assistance information IE of the ATTACH REQUEST message.

If the UE supports SRVCC to GERAN/UTRAN, the UE shall set the SRVCC to GERAN/UTRAN capability bit to "SRVCC from UTRAN HSPA or E-UTRAN to GERAN/UTRAN supported".

If the UE supports vSRVCC from S1 mode to Iu mode, then the UE shall set the H.245 after handover capability bit to "H.245 after SRVCC handover capability supported" and additionally set the SRVCC to GERAN/UTRAN capability bit to "SRVCC from UTRAN HSPA or E-UTRAN to GERAN/UTRAN supported" in the ATTACH REQUEST message.

If the UE supports PSM and requests the use of PSM, then the UE shall include the T3324 value IE with a requested timer value in the ATTACH REQUEST message. When the UE includes the T3324 value IE and the UE indicates support for extended periodic timer value in the MS network feature support IE, it may also include the T3412 extended value IE to request a particular T3412 value to be allocated.

If the UE supports ProSe direct discovery, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe direct discovery bit to "ProSe direct discovery supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports ProSe direct communication, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe direct communication bit to "ProSe direct communication supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports acting as a ProSe UE-to-network relay, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe UE-to-network relay bit to "acting as a ProSe UE-to-network relay supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports NB-S1 mode, Non-IP or Ethernet PDN type, N1 mode, or if the UE supports DNS over (D)TLS (see 3GPP TS 33.501 [24]), then the UE shall support the extended protocol configuration options IE.

NOTE 4: Support of DNS over (D)TLS is based on the informative requirements as specified in 3GPP TS 33.501 [24].

If the UE supports the extended protocol configuration options IE, then the UE shall set the ePCO bit to "extended protocol configuration options supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports the restriction on use of enhanced coverage, then the UE shall set the RestrictEC bit to "Restriction on use of enhanced coverage supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports the control plane data back-off timer T3448, the UE shall set the CP backoff bit to "back-off timer for transport of user data via the control plane supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports EPS-UPIP, the UE shall set the EPS-UPIP bit to "EPS-UPIP supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE is in NB-S1 mode, then the UE shall set the Control plane CIoT EPS optimization bit to "Control plane CIoT EPS optimization supported" in the UE network capability IE of the ATTACH REQUEST message. If the UE is capable of NB-N1 mode, then the UE shall set the Control plane CIoT 5GS optimization bit to "Control plane CIoT 5GS optimization supported" in the N1 UE network capability IE of the ATTACH REQUEST message.

If the UE is in NB-S1 mode, supports NB-S1 mode only, and requests to attach for EPS services and "SMS only", the UE shall indicate the SMS only requested bit to "SMS only" in the additional update type IE and shall set the EPS attach type IE to "EPS attach" in the ATTACH REQUEST message.

If the UE supports CIoT EPS optimizations, it shall indicate in the UE network capability IE of the ATTACH REQUEST message whether it supports EMM-REGISTERED without PDN connection.

If the UE supports S1-U data transfer and multiple user plane radio bearers (see 3GPP TS 36.306 [44], 3GPP TS 36.331 [22]) in NB-S1 mode, then the UE shall set the Multiple DRB support bit to "Multiple DRB supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports control plane MT-EDT, then the UE shall set the CP-MT-EDT bit to "Control plane Mobile Terminated-Early Data Transmission supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports user plane MT-EDT, then the UE shall set the UP-MT-EDT bit to "User plane Mobile Terminated-Early Data Transmission supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports V2X communication over E-UTRA-PC5, then the UE shall set the V2X PC5 bit to "V2X communication over E-UTRA-PC5 supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports V2X communication over NR-PC5, then the UE shall set the V2X NR-PC5 bit to "V2X communication over NR-PC5 supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports service gap control, then the UE shall set the SGC bit to "service gap control supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports dual connectivity with New Radio (NR), then the UE shall set the DCNR bit to "dual connectivity with NR supported" in the UE network capability IE of the ATTACH REQUEST message and shall include the UE additional security capability IE in the ATTACH REQUEST message.

If the UE supports N1 mode for 3GPP access, the UE shall set the N1mode bit to "N1 mode for 3GPP access supported" in the UE network capability IE of the ATTACH REQUEST message and shall include the UE additional security capability IE in the ATTACH REQUEST message.

If the UE supports signalling for a maximum number of 15 EPS bearer contexts, then the UE shall set the 15 bearers bit to "Signalling for a maximum number of 15 EPS bearer contexts supported" in the UE network capability IE of the ATTACH REQUEST message.

If the UE supports ciphered broadcast assistance data and needs to obtain new ciphering keys, the UE shall include the Additional information requested IE with the CipherKey bit set to "ciphering keys for ciphered broadcast assistance data requested" in the ATTACH REQUEST message.

For MUSIM capable UE if the UE needs to indicate an IMSI offset value to the network, the UE shall include the IMSI offset value in the Requested IMSI offset IE in the ATTACH REQUEST message.

If EMM-REGISTERED without PDN connection is not supported by the UE or the MME, or if the UE wants to request PDN connection with the attach procedure, the UE shall send the ATTACH REQUEST message together with a PDN CONNECTIVITY REQUEST message contained in the ESM message container IE.

If EMM-REGISTERED without PDN connection is supported by the UE and the MME, and the UE does not want to request PDN connection with the attach procedure, the UE shall send the ATTACH REQUEST message together with an ESM DUMMY MESSAGE contained in the ESM message container information element.

In WB-S1 mode, if the UE supports RACS, the UE shall:

a) set the RACS bit to "RACS supported" in the UE network capability IE of the ATTACH REQUEST message; and

b) if the UE has an applicable UE radio capability ID for the current UE radio configuration in the selected PLMN, set the URCIDA bit to "UE radio capability ID available" in the UE radio capability ID availability IE of the ATTACH REQUEST message.

If the attach procedure is initiated following an inter-system change from N1 mode to S1 mode in EMM-IDLE mode or the UE which was previously registered in N1 mode before entering state 5GMM-DEREGISTERED initiates the attach procedure:

a) if the UE has received an "interworking without N26 interface not supported" indication from the network and a valid 5G NAS security context exists in the UE, the UE shall integrity protect the ATTACH REQUEST message combined with the message included in the ESM message container IE using the 5G NAS security context;

b) otherwise:

1) if a valid EPS security context exists, the UE shall integrity protect the ATTACH REQUEST message combined with the message included in the ESM message container IE using the EPS security context; or

2) if the UE does not have a valid EPS security context, the ATTACH REQUEST message combined with the message included in the ESM message container IE is not integrity protected.



Figure 5.5.1.2.2.1: Attach procedure and combined attach procedure

\*\*\*\*\* change \*\*\*\*\*

##### 5.5.3.2.2 Normal and periodic tracking area updating procedure initiation

The UE in state EMM-REGISTERED shall initiate the tracking area updating procedure by sending a TRACKING AREA UPDATE REQUEST message to the MME,

a) when the UE detects entering a tracking area that is not in the list of tracking areas that the UE previously registered in the MME, unless the UE is configured for "AttachWithIMSI" as specified in 3GPP TS 24.368 [15A] or 3GPP TS 31.102 [17] and is entering a tracking area in a new PLMN that is neither the registered PLMN nor in the list of equivalent PLMNs;

b) when the periodic tracking area updating timer T3412 expires;

c) when the UE enters EMM-REGISTERED.NORMAL-SERVICE and the UE's TIN indicates "P-TMSI";

d) when the UE performs an inter-system change from S101 mode to S1 mode and has no user data pending;

e) when the UE receives an indication from the lower layers that the RRC connection was released with cause "load balancing TAU required";

f) when the UE deactivated EPS bearer context(s) locally while in EMM-REGISTERED, because it could not establish a NAS signalling connection, and then returns to EMM-REGISTERED.NORMAL-SERVICE and no EXTENDED SERVICE REQUEST message, CONTROL PLANE SERVICE REQUEST message or DETACH REQUEST message with detach type is "EPS detach" or "combined EPS/IMSI detach" is pending to be sent by the UE;

g) when the UE changes any one of the UE network capability information, the MS network capability information or the N1 UE network capability information;

h) when the UE changes the UE specific DRX parameter (in WB-S1 mode or NB-S1 mode);

i) when the UE receives an indication of "RRC Connection failure" from the lower layers and has no signalling or user uplink data pending (i.e. when the lower layer requests NAS signalling connection recovery);

j) when the UE enters S1 mode after 1xCS fallback or 1xSRVCC;

k) when due to manual CSG selection the UE has selected a CSG cell whose CSG identity and associated PLMN identity are not included in the UE's Allowed CSG list or in the UE's Operator CSG list;

l) when the UE reselects an E-UTRAN cell while it was in GPRS READY state or PMM-CONNECTED mode;

m) when the UE supports SRVCC to GERAN or UTRAN or supports vSRVCC to UTRAN and changes the mobile station classmark 2 or the supported codecs, or the UE supports SRVCC to GERAN and changes the mobile station classmark 3;

n) when the UE changes the radio capability for GERAN, or cdma2000® or both;

o) when the UE's usage setting or the voice domain preference for E-UTRAN change in the UE;

NOTE 1: For the change of UE's usage setting or the voice domain preference for E-UTRAN which results in disabling UE's E-UTRA capability, the UE can skip sending TRACKING AREA UPDATE REQUEST message and directly perform disabling of UE's E-UTRA capability.

p) when the UE activates mobility management for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.2, and the TIN indicates "RAT-related TMSI";

q) when the UE performs an inter-system change from A/Gb mode to S1 mode and the TIN indicates "RAT-related TMSI", but the UE is required to perform tracking area updating for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.4;

r) upon reception of a paging indication using S-TMSI and the UE is in state EMM-REGISTERED.ATTEMPTING-TO-UPDATE;

s) when the UE needs to update the network with EPS bearer context status due to local de-activation of EPS bearer context(s) as specified in clause 6.5.1.4A;

t) when the UE needs to request the use of PSM or needs to stop the use of PSM;

u) when the UE needs to request the use of eDRX or needs to stop the use of eDRX;

v) when a change in the eDRX usage conditions at the UE requires different extended DRX parameters;

w) when a change in the PSM usage conditions at the UE requires a different timer T3412 value or different timer T3324 value;

NOTE 2: A change in the PSM or eDRX usage conditions at the UE can include e.g. a change in the UE configuration, a change in requirements from upper layers or the battery running low at the UE.

x) when the CIoT EPS optimizations the UE needs to use, change in the UE;

y) when the Default\_DCN\_ID value changes, as specified in 3GPP TS 24.368 [15A] or in USIM file NASCONFIG as specified in 3GPP TS 31.102 [17];

NOTE 3: The tracking area updating procedure is initiated after deleting the DCN-ID list as specified in annex C.

z) when the UE performs inter-system change from N1 mode to S1 mode in EMM-IDLE mode, the UE operates in single-registration mode, and conditions specified in 3GPP TS 24.501 [54] apply;

za) when the UE in EMM-IDLE mode changes the radio capability for E-UTRAN;

zb) when the UE needs to request new ciphering keys for ciphered broadcast assistance data;

zc) when the UE in EMM-IDLE mode changes the radio capability for NG-RAN;

zd) when the UE performs inter-system change from N1 mode to S1 mode in EMM-CONNECTED mode;

ze) in WB-S1 mode, when the applicable UE radio capability ID for the current UE radio configuration changes due to a revocation of the network-assigned UE radio capability IDs by the serving PLMN;

zf) when the UE needs to use the WUS assistance, stop to use the WUS assistance, or change the conditions for using the WUS assistance; or

zg) when the MUSIM capable UE needs to request an IMSI Offset value as specified in 3GPP TS 23.401 [10] that is used for deriving the paging occasion as specified in 3GPP TS 36.304 [21].

If case b) is the only reason for initiating the normal and periodic tracking area updating procedure, the UE shall indicate "periodic updating" in the EPS update type IE; otherwise the UE shall indicate "TA updating".

For cases n, za and zc, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

If the UE is in the EMM-CONNECTED mode and the UE changes the radio capability for E-UTRAN or for NG-RAN, the UE may locally release the established NAS signalling connection and enter the EMM-IDLE mode. Then, the UE shall initiate the tracking area updating procedure including a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

For case l, if the TIN indicates "RAT-related TMSI", the UE shall set the TIN to "P-TMSI" before initiating the tracking area updating procedure.

For case r, the "active" flag in the EPS update type IE shall be set to 1. If a UE is only using EPS services with control plane CIoT EPS optimization, the "signalling active" flag in the Additional update type IE shall be set to 1.

If the UE is using only control plane CIoT EPS optimization, the case i only applies to the case that the UE has indicated to the network that subsequent to the uplink data transmission a downlink data transmission is expected during the transport of uplink user data via the control plane procedure (see clause 6.6.4).

If the UE has to request resources for ProSe direct discovery or Prose direct communication (see 3GPP TS 36.331 [22]), then the UE shall set the "active" flag to 1 in the TRACKING AREA UPDATE REQUEST message.

If the UE does not have any established PDN connection, and the inter-system change from N1 mode to S1 mode is not due to emergency services fallback, the "active" flag in the EPS update type IE shall be set to 0.

When the UE has user data pending and performs an inter-system change from S101 mode to S1 mode to a tracking area included in the TAI list stored in the UE, the UE shall perform a service request procedure instead of a tracking area updating procedure.

When initiating a tracking area updating procedure while in S1 mode, the UE shall use the current EPS NAS integrity key to integrity protect the TRACKING AREA UPDATE REQUEST message, unless the UE is performing inter-system change from N1 mode to S1 mode.

In order to indicate its UE specific DRX parameter for WB-S1 mode while in E-UTRAN coverage, the UE shall send the TRACKING AREA UPDATE REQUEST message containing the UE specific DRX parameter in the DRX parameter IE to the network, with the exception of the case if the UE had indicated its DRX parameter for WB-S1 mode (3GPP TS 24.008 [13]) to the network while in GERAN or UTRAN coverage. In this case, when the UE enters E-UTRAN coverage and initiates a tracking area updating procedure, the UE shall not include the UE specific DRX parameter in the DRX parameter IE in the TRACKING AREA UPDATE REQUEST message.

In NB-S1 mode, a UE that wishes to use or change a UE specific DRX parameter in NB-S1 mode shall include its requested value in every TRACKING AREA UPDATE REQUEST message except when initiating the periodic tracking area updating procedure.

If the UE supports eDRX and requests the use of eDRX, the UE shall include the extended DRX parameters IE in the TRACKING AREA UPDATE REQUEST message.

If the UE supports PSM and requests the use of PSM, the UE shall include the T3324 value IE with a requested timer value in the TRACKING AREA UPDATE REQUEST message. When the UE includes the T3324 value IE and the UE indicates support for extended periodic timer value in the MS network feature support IE, it may also include the T3412 extended value IE to request a particular T3412 value to be allocated.

If a UE supporting CIoT EPS optimizations in NB-S1 mode initiates the tracking area updating procedure for EPS services and "SMS only", the UE shall indicate "SMS only" in the Additional update type IE and shall set the EPS update type IE to "TA updating".

If the UE supports S1-U data transfer and multiple user plane radio bearers (see 3GPP TS 36.306 [44], 3GPP TS 36.331 [22]) in NB-S1 mode, then the UE shall set the Multiple DRB support bit to "Multiple DRB supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE is in NB-S1 mode, then the UE shall set the Control plane CIoT EPS optimization bit to "Control plane CIoT EPS optimization supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message. If the UE is capable of NB-N1 mode, then the UE shall set the Control plane CIoT 5GS optimization bit to "Control plane CIoT 5GS optimization supported" in the N1 UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE supports control plane MT-EDT, then the UE shall set the CP-MT-EDT bit to "Control plane Mobile Terminated-Early Data Transmission supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE supports user plane MT-EDT, then the UE shall set the UP-MT-EDT bit to "User plane Mobile Terminated-Early Data Transmission supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE supports EPS-UPIP, the UE shall set the EPS-UPIP bit to "EPS-UPIP supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE has to request resources for V2X communication over PC5 (see 3GPP TS 23.285 [47]), then the UE shall set the "active" flag to 1 in the TRACKING AREA UPDATE REQUEST message.

After sending the TRACKING AREA UPDATE REQUEST message to the MME, the UE shall start timer T3430 and enter state EMM-TRACKING-AREA-UPDATING-INITIATED (see example in figure 5.5.3.2.2.1). If timer T3402 is currently running, the UE shall stop timer T3402. If timer T3411 is currently running, the UE shall stop timer T3411. If timer T3442 is currently running, the UE shall stop timer T3442.

For all cases except cases z and zd:

1) if the UE supports neither A/Gb mode nor Iu mode, the UE shall include a valid GUTI in the Old GUTI IE in the TRACKING AREA UPDATE REQUEST message. In addition, the UE shall include Old GUTI type IE with GUTI type set to "native GUTI"; or

2) if the UE supports A/Gb mode or Iu mode or both, the UE shall handle the Old GUTI IE as follows:

- If the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI and RAI, the UE shall map the P-TMSI and RAI into the Old GUTI IE, and include Old GUTI type IE with GUTI type set to "mapped GUTI". If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE. Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE.

NOTE 4: The mapping of the P-TMSI and RAI to the GUTI is specified in 3GPP TS 23.003 [2].

- If the TIN indicates "GUTI" or "RAT-related TMSI" and the UE holds a valid GUTI, the UE shall indicate the GUTI in the Old GUTI IE, and include Old GUTI type IE with GUTI type set to "native GUTI".

If a UE has established PDN connection(s) and uplink user data pending to be sent via user plane when it initiates the tracking area updating procedure, or uplink signalling not related to the tracking area updating procedure when the UE does not support control plane CIoT EPS optimization, it may set the "active" flag in the TRACKING AREA UPDATE REQUEST message to indicate the request to establish the user plane to the network and to keep the NAS signalling connection after the completion of the tracking area updating procedure.

If a UE is using EPS services with control plane CIoT EPS optimization and has user data pending to be sent via control plane over MME but no user data pending to be sent via user plane, or uplink signalling not related to the tracking area updating procedure, the UE may set the "signalling active" flag in the TRACKING AREA UPDATE REQUEST message to indicate the request to keep the NAS signalling connection after the completion of the tracking area updating procedure.

For all cases except cases z and zd, if the UE has a current EPS security context, the UE shall include the eKSI (either KSIASME or KSISGSN) in the NAS Key Set Identifier IE in the TRACKING AREA UPDATE REQUEST message. Otherwise, the UE shall set the NAS Key Set Identifier IE to the value "no key is available". If the UE has a current EPS security context, the UE shall integrity protect the TRACKING AREA UPDATE REQUEST message with the current EPS security context. Otherwise the UE shall not integrity protect the TRACKING AREA UPDATE REQUEST message.

When the tracking area updating procedure is initiated in EMM-IDLE mode to perform an inter-system change from A/Gb mode or Iu mode to S1 mode and the TIN is set to "P-TMSI", the UE shall include the GPRS ciphering key sequence number applicable for A/Gb mode or Iu mode and a nonceUE in the TRACKING AREA UPDATE REQUEST message.

When the tracking area updating procedure is initiated in EMM-CONNECTED mode to perform an inter-system change from A/Gb mode or Iu mode to S1 mode, the UE shall derive the EPS NAS keys from the mapped K'ASME using the selected NAS algorithms, nonceMME and KSISGSN (to be associated with the mapped K'ASME) provided by lower layers as indicated in 3GPP TS 33.401 [19]. The UE shall reset both the uplink and downlink NAS COUNT counters of the mapped EPS security context which shall be taken into use. If the UE has a non-current native EPS security context, the UE shall include the KSIASME in the Non-current native NAS key set identifier IE and its associated GUTI, as specified above, either in the Old GUTI IE or in the Additional GUTI IE of the TRACKING AREA UPDATE REQUEST message. The UE shall set the TSC flag in the Non-current native NAS key set identifier IE to "native security context".

For the case z, if upper layers have indicated that IMS signalling or IMS emergency signalling was already ongoing in N1 mode before performing the inter-system change from N1 mode to S1 mode, or if the inter-system change from N1 mode to S1 mode is due to emergency services fallback, the "active" flag in the EPS update type IE shall be set to 1.

For the case z, the TRACKING AREA UPDATE REQUEST message shall be integrity protected using the 5G NAS security context available in the UE. If there is no valid 5G NAS security context available in the UE, the TRACKING AREA UPDATE REQUEST message shall be sent without integrity protection. The UE shall include a GUTI, mapped from 5G-GUTI (see 3GPP TS 23.501 [58] and 3GPP TS 23.003 [2]), in the Old GUTI IE in the TRACKING AREA UPDATE REQUEST message. In addition, the UE shall include Old GUTI type IE with GUTI set to "Native GUTI", and the UE shall include a UE status IE with a 5GMM registration status set to "UE is in 5GMM-REGISTERED state". Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE.

NOTE 5: The value of the EMM registration status included by the UE in the UE status IE is not used by the MME.

For the case zd, the TRACKING AREA UPDATE REQUEST message shall be integrity protected using the mapped EPS security context as derived when triggering the handover to E-UTRAN (see clause 4.4.2.2). The UE shall include a GUTI, mapped from 5G-GUTI (see 3GPP TS 23.501 [58] and 3GPP TS 23.003 [2]), in the Old GUTI IE in the TRACKING AREA UPDATE REQUEST message. In addition, the UE shall include Old GUTI type IE with GUTI set to "Native GUTI", and the UE shall include a UE status IE with a 5GMM registration status set to "UE is in 5GMM-REGISTERED state". Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE. If the UE has a non-current native EPS security context, the UE shall include the KSIASME in the Non-current native NAS key set identifier IE of the TRACKING AREA UPDATE REQUEST message. The UE shall set the TSC flag in the Non-current native NAS key set identifier IE to "native security context".

NOTE 6: The value of the EMM registration status included by the UE in the UE status IE is not used by the MME.

When the tracking area updating procedure is initiated in EMM-IDLE mode, the UE may also include an EPS bearer context status IE in the TRACKING AREA UPDATE REQUEST message, indicating which EPS bearer contexts are active in the UE. The UE shall include the EPS bearer context status IE in TRACKING AREA UPDATE REQUEST message:

a) for the case f;

b) for the case s;

c) for the case z;

d) if the UE has established PDN connection(s) of "non IP" or Ethernet PDN type; and

e) if the UE:

1) locally deactivated at least one dedicated EPS bearer context upon an inter-system mobility from WB-S1 mode to NB-S1 mode in EMM-IDLE mode;

2) locally deactivated at least one dedicated EPS bearer context upon an inter-system change from WB-N1 mode to NB-S1 mode in EMM-IDLE mode for the UE operating in single-registration mode (see clause 6.4.2.1); or

3) locally deactivated at least one default EPS bearer context upon an inter-system change from N1 mode to NB-S1 mode in EMM-IDLE mode for the UE operating in single-registration mode (see clause 6.5.0).

If the UE initiates the first tracking area updating procedure following an attach in A/Gb mode or Iu mode, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

If the UE initiates the first tracking area updating procedure following an initial registration in N1 mode and the UE is operating in the single-registration mode, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports SRVCC to GERAN/UTRAN, the UE shall set the SRVCC to GERAN/UTRAN capability bit in the MS network capability IE to "SRVCC from UTRAN HSPA or E-UTRAN to GERAN/UTRAN supported".

For all cases except case b, if the UE supports vSRVCC from S1 mode to Iu mode, then the UE shall set the H.245 after handover capability bit in the UE network capability IE to "H.245 after SRVCC handover capability supported" and additionally set the SRVCC to GERAN/UTRAN capability bit in the MS network capability IE to "SRVCC from UTRAN HSPA or E-UTRAN to GERAN/UTRAN supported" in the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports ProSe direct discovery, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe direct discovery bit to "ProSe direct discovery supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports ProSe direct communication, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe direct communication bit to "ProSe direct communication supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports acting as a ProSe UE-to-network relay, then the UE shall set the ProSe bit to "ProSe supported" and set the ProSe UE-to-network relay bit to "acting as a ProSe UE-to-network relay supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

If the UE supports NB-S1 mode, Non-IP or Ethernet PDN type, N1 mode, or if the UE supports DNS over (D)TLS (see 3GPP TS 33.501 [24]), then the UE shall support the extended protocol configuration options IE.

NOTE 7: Support of DNS over (D)TLS is based on the informative requirements as specified in 3GPP TS 33.501 [24].

For all cases except case b, if the UE supports the extended protocol configuration options IE, then the UE shall set the ePCO bit to "extended protocol configuration options supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports V2X communication over E-UTRAN-PC5, then the UE shall set the V2X PC5 bit to "V2X communication over E-UTRAN-PC5 supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports V2X communication over NR-PC5, then the UE shall set the V2X NR-PC5 bit to "V2X communication over NR-PC5 supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports the restriction on use of enhanced coverage, then the UE shall set the RestrictEC bit to "Restriction on use of enhanced coverage supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports the control plane data back-off timer T3448, the UE shall set the CP backoff bit to "backoff timer for transport of user data via the control plane supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports dual connectivity with NR, then the UE shall set the DCNR bit to "dual connectivity with NR supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message and shall include the UE additional security capability IE in the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports SGC, then the UE shall set the SGC bit to "service gap control supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports signalling for a maximum number of 15 EPS bearer contexts, then the UE shall set the 15 bearers bit to "Signalling for a maximum number of 15 EPS bearer contexts supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except cases b and zb, if the UE supports ciphered broadcast assistance data and the UE needs to obtain new ciphering keys, the UE shall include the Additional information requested IE with the CipherKey bit set to "ciphering keys for ciphered broadcast assistance data requested" in the TRACKING AREA UPDATE REQUEST message.

For case ee, the UE shall include the Additional information requested IE with the CipherKey bit set to "ciphering keys for ciphered broadcast assistance data requested" in the TRACKING AREA UPDATE REQUEST message.

For case a, if the UE supports ciphered broadcast assistance data and the UE detects entering a tracking area for which one or more ciphering keys stored at the UE is not applicable, the UE should include the Additional information requested IE with the CipherKey bit set to "ciphering keys for ciphered broadcast assistance data requested" in the TRACKING AREA UPDATE REQUEST message.

For case b, if the UE supports ciphered broadcast assistance data and the remaining validity time for one or more ciphering keys stored at the UE is less than timer T3412, the UE should include the Additional information requested IE with the CipherKey bit set to "ciphering keys for ciphered broadcast assistance data requested" in the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports N1 mode for 3GPP access, the UE shall set the N1mode bit to "N1 mode for 3GPP access supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message and shall include the UE additional security capability IE in the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, in WB-S1 mode, if the UE supports RACS the UE shall set the RACS bit to "RACS supported" in the UE network capability IE of the TRACKING AREA UPDATE REQUEST message.

For cases n, za and zc, in WB-S1 mode, if the UE supports RACS and the UE has an applicable UE radio capability ID for the new UE radio configuration in the selected PLMN, the UE shall set the URCIDA bit to "UE radio capability ID available" in the UE radio capability ID availability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except cases b, n, za and zc, in WB-S1 mode, if the UE has an applicable UE radio capability ID for the current UE radio configuration in the selected PLMN, the UE shall set the URCIDA bit to "UE radio capability ID available" in the UE radio capability ID availability IE of the TRACKING AREA UPDATE REQUEST message.

For all cases except case b, if the UE supports WUS assistance, then the UE shall set the WUSA bit to "WUS assistance supported" in the UE network capability IE, and if the UE is not attaching for emergency bearer services, the UE may include its UE paging probability information in the Requested WUS assistance information IE in the TRACKING AREA UPDATE REQUEST message.

For all cases, for a MUSIM capable UE if the UE needs to indicate an IMSI offset value to the network and the network has indicated to the UE that it supports paging timing collision control, the UE shall include the IMSI offset value in the Requested IMSI offset IE in the TRACKING AREA UPDATE REQUEST message.

If the UE supports MUSIM and requests the network to release the NAS signalling connection, the UE shall set Request type to "NAS signalling connection release" in the UE request type IE and may set the paging restriction preferences in the Paging restriction IE in the TRACKING AREA UPDATE REQUEST message. In addition, the UE shall

- set the "active" flag to 0 in the EPS update type IE; and

- set the "signalling active" flag to 0 in the Additional update type IE, if the Additional update type IE is included.

Editor's Note [MUSIM]: What is meant by "If the UE supports MUSIM" and all such statements in the specification is for FFS and will be specified subsequently



Figure 5.5.3.2.2.1: Tracking area updating procedure

\*\*\*\*\* change \*\*\*\*\*

#### 9.9.3.34 UE network capability

The purpose of the UE network capability information element is to provide the network with information concerning aspects of the UE related to EPS or interworking with GPRS and 5GS. The contents might affect the manner in which the network handles the operation of the UE. The UE network capability information indicates general UE characteristics and it shall therefore, except for fields explicitly indicated, be independent of the frequency band of the channel it is sent on.

The UE network capability information element is coded as shown in figure 9.9.3.34.1 and table 9.9.3.34.1.

The UE network capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 15 octets.

NOTE: The requirements for the support of UMTS security algorithms in the UE are specified in 3GPP TS 33.102 [18], and the requirements for the support of EPS security algorithms in 3GPP TS 33.401 [19].

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE network capability IEI | octet 1 |
| Length of UE network capability contents | octet 2 |
| EEA0 | 128-EEA1 | 128-EEA2 | 128-EEA3 | EEA4 | EEA5 | EEA6 | EEA7 | octet 3 |
| EIA0 | 128-EIA1 | 128-EIA2 | 128-EIA3 | EIA4 | EIA5 | EIA6 | EPS-UPIP | octet 4 |
| UEA0 | UEA1 | UEA2 | UEA3 | UEA4 | UEA5 | UEA6 | UEA7 | octet 5\* |
| UCS2 | UIA1 | UIA2 | UIA3 | UIA4 | UIA5 | UIA6 | UIA7 | octet 6\* |
| ProSe-dd | ProSe | H.245-ASH | ACC-CSFB | LPP | LCS | 1xSRVCC | NF | octet 7\* |
| ePCO | HC-CP CIoT | ERw/oPDN | S1-U data | UP CIoT | CP CIoT | Prose-relay | ProSe-dc | octet 8\* |
| 15 bearers | SGC | N1mode | DCNR | CP backoff | RestrictEC | V2X PC5 | multipleDRB | octet 9\* |
| 0Spare | 0Spare | 0Spare | V2X NR-PC5 | UP-MT-EDT | CP-MT-EDT | WUSA | RACS | octet 10\* |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 11\* -15\* |
| Spare |

Figure 9.9.3.34.1: UE network capability information element

Table 9.9.3.34.1: UE network capability information element

|  |
| --- |
| EPS encryption algorithms supported (octet 3) |
|  |
| EPS encryption algorithm EEA0 supported (octet 3, bit 8) |
| 0 |  |  |  | EPS encryption algorithm EEA0 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA0 supported |
|  |
| EPS encryption algorithm 128-EEA1 supported (octet 3, bit 7) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA1 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA1 supported |
|  |
| EPS encryption algorithm 128-EEA2 supported (octet 3, bit 6) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA2 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA2 supported |
|  |
| EPS encryption algorithm 128-EEA3 supported (octet 3, bit 5) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA3 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA3 supported |
|  |
| EPS encryption algorithm EEA4 supported (octet 3, bit 4) |
| 0 |  |  |  | EPS encryption algorithm EEA4 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA4 supported |
|  |
| EPS encryption algorithm EEA5 supported (octet 3, bit 3) |
| 0 |  |  |  | EPS encryption algorithm EEA5 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA5 supported |
|  |
| EPS encryption algorithm EEA6 supported (octet 3, bit 2) |
| 0 |  |  |  | EPS encryption algorithm EEA6 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA6 supported |
|  |
| EPS encryption algorithm EEA7 supported (octet 3, bit 1) |
| 0 |  |  |  | EPS encryption algorithm EEA7 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA7 supported |
|  |
| EPS integrity algorithms supported (octet 4) |
|  |
| EPS integrity algorithm EIA0 supported (octet 4, bit 8) |
| 0 |  |  |  | EPS integrity algorithm EIA0 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA0 supported |
|  |
| EPS integrity algorithm 128-EIA1 supported (octet 4, bit 7) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA1 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA1 supported |
|  |
| EPS integrity algorithm 128-EIA2 supported (octet 4, bit 6) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA2 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA2 supported |
|  |
| EPS integrity algorithm 128-EIA3 supported (octet 4, bit 5) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA3 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA3 supported |
|  |
| EPS integrity algorithm EIA4 supported (octet 4, bit 4) |
| 0 |  |  |  | EPS integrity algorithm EIA4 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA4 supported |
|  |
| EPS integrity algorithm EIA5 supported (octet 4, bit 3) |
| 0 |  |  |  | EPS integrity algorithm EIA5 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA5 supported |
|  |
| EPS integrity algorithm EIA6 supported (octet 4, bit 2) |
| 0 |  |  |  | EPS integrity algorithm EIA6 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA6 supported |
|  |
| EPS-UPIP supported (octet 4, bit 1) |
| 0 |  |  |  | EPS-UPIP not supported |
| 1 |  |  |  | EPS-UPIP supported |
|  |
| UMTS encryption algorithms supported (octet 5) |
|  |
| UMTS encryption algorithm UEA0 supported (octet 5, bit 8) |
| 0 |  |  |  | UMTS encryption algorithm UEA0 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA0 supported |
|  |
| UMTS encryption algorithm UEA1 supported (octet 5, bit 7) |
| 0 |  |  |  | UMTS encryption algorithm UEA1 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA1 supported |
|  |
| UMTS encryption algorithm UEA2 supported (octet 5, bit 6) |
| 0 |  |  |  | UMTS encryption algorithm UEA2 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA2 supported |
|  |
| UMTS encryption algorithm UEA3 supported (octet 5, bit 5) |
| 0 |  |  |  | UMTS encryption algorithm UEA3 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA3 supported |
|  |
| UMTS encryption algorithm UEA4 supported (octet 5, bit 4) |
| 0 |  |  |  | UMTS encryption algorithm UEA4 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA4 supported |
|  |
| UMTS encryption algorithm UEA5 supported (octet 5, bit 3) |
| 0 |  |  |  | UMTS encryption algorithm UEA5 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA5 supported |
|  |
| UMTS encryption algorithm UEA6 supported (octet 5, bit 2) |
| 0 |  |  |  | UMTS encryption algorithm UEA6 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA6 supported |
|  |
| UMTS encryption algorithm UEA7 supported (octet 5, bit 1) |
| 0 |  |  |  | UMTS encryption algorithm UEA7 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA7 supported |
|  |
| UCS2 support (UCS2) (octet 6, bit 8) |
| This information field indicates the likely treatment of UCS2 encoded character strings by the UE. |
|  |
| 0 |  |  |  | The UE has a preference for the default alphabet (defined in  |
|  |  |  |  | 3GPP TS 23.038 [3]) over UCS2 (see ISO/IEC 10646 [29]). |
| 1 |  |  |  | The UE has no preference between the use of the default alphabet and  |
|  |  |  |  | the use of UCS2. |
|  |
| UMTS integrity algorithms supported (octet 6) |
|  |
| UMTS integrity algorithm UIA1 supported (octet 6, bit 7) |
| 0 |  |  |  | UMTS integrity algorithm UIA1 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA1 supported |
|  |
| UMTS integrity algorithm UIA2 supported (octet 6, bit 6) |
| 0 |  |  |  | UMTS integrity algorithm UIA2 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA2 supported |
|  |
| UMTS integrity algorithm UIA3 supported (octet 6, bit 5) |
| 0 |  |  |  | UMTS integrity algorithm UIA3 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA3 supported |
|  |
| UMTS integrity algorithm UIA4 supported (octet 6, bit 4) |
| 0 |  |  |  | UMTS integrity algorithm UIA4 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA4 supported |
|  |
| UMTS integrity algorithm UIA5 supported (octet 6, bit 3) |
| 0 |  |  |  | UMTS integrity algorithm UIA5 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA5 supported |
|  |
| UMTS integrity algorithm UIA6 supported (octet 6, bit 2) |
| 0 |  |  |  | UMTS integrity algorithm UIA6 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA6 supported |
|  |
| UMTS integrity algorithm UIA7 supported (octet 6, bit 1) |
| 0 |  |  |  | UMTS integrity algorithm UIA7 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA7 supported |
|  |
| NF capability (octet 7, bit 1) |
| 0 |  |  |  | notification procedure not supported |
| 1 |  |  |  | notification procedure supported |
|  |
| 1xSRVCC capability (octet 7, bit 2) |
| 0 |  |  |  | SRVCC from E-UTRAN to cdma2000® 1x CS not supported |
| 1 |  |  |  | SRVCC from E-UTRAN to cdma2000® 1x CS supported |
|  |  |  |  | (see 3GPP TS 23.216 [8]) |
|  |
| Location services (LCS) notification mechanisms capability (octet 7, bit 3) |
| 0 |  |  |  | LCS notification mechanisms not supported  |
| 1 |  |  |  | LCS notification mechanisms supported (see 3GPP TS 24.171 [13C]) |
|  |
| LTE Positioning Protocol (LPP) capability (octet 7, bit 4) |
| 0 |  |  |  | LPP not supported |
| 1 |  |  |  | LPP supported (see 3GPP TS 36.355 [22A]) |
| Access class control for CSFB (ACC-CSFB) capability (octet 7, bit 5) |
| 0 |  |  |  | eNodeB-based access class control for CSFB not supported |
| 1 |  |  |  | eNodeB-based access class control for CSFB supported(see 3GPP TS 22.011 [1A])  |
| H.245 After SRVCC Handover capability (H.245-ASH) (octet 7, bit 6)This bit indicates the capability for H.245 with support and use of pre-defined codecs, and if needed, H.245 codec negotiation after SRVCC handover. |
| 0 |  |  |  | H.245 after SRVCC handover capability not supported |
| 1 |  |  |  | H.245 after SRVCC handover capability supported(see 3GPP TS 23.216 [8]) |
| ProSe (octet 7, bit 7)This bit indicates the capability for ProSe. |
| 0 |  |  |  | ProSe not supported |
| 1 |  |  |  | ProSe supported |
| ProSe direct discovery (ProSe-dd) (octet 7, bit 8)This bit indicates the capability for ProSe direct discovery. |
| 0 |  |  |  | ProSe direct discovery not supported |
| 1 |  |  |  | ProSe direct discovery supported |
| ProSe direct communication (ProSe-dc) (octet 8, bit 1)This bit indicates the capability for ProSe direct communication. |
| 0 |  |  |  | ProSe direct communication not supported |
| 1 |  |  |  | ProSe direct communication supported |
| ProSe UE-to-network-relay (ProSe-relay) (octet 8, bit 2)This bit indicates the capability to act as a ProSe UE-to-network relay |
| 0 |  |  |  | Acting as a ProSe UE-to-network relay not supported |
| 1 |  |  |  | Acting as a ProSe UE-to-network relay supported |
| Control plane CIoT EPS optimization (CP CIoT) (octet 8, bit 3)This bit indicates the capability for control plane CIoT EPS optimization. |
| 0 |  |  |  | Control plane CIoT EPS optimization not supported |
| 1 |  |  |  | Control plane CIoT EPS optimization supported |
| User plane CIoT EPS optimization (UP CIoT) (octet 8, bit 4)This bit indicates the capability for user plane CIoT EPS optimization. |
| 0 |  |  |  | User plane CIoT EPS optimization not supported |
| 1 |  |  |  | User plane CIoT EPS optimization supported |
| S1-u data transfer (S1-U data) (octet 8, bit 5)This bit indicates the capability for S1-u data transfer. This bit shall be considered only if the Control plane CIoT EPS optimization (CP CIoT) bit (octet 8, bit 3) is set to 1. If the Control plane CIoT EPS optimization (CP CIoT) bit (octet 8, bit 3) is set to 0, the MME shall assume S1-u data transfer is supported by the UE. |
| 0 |  |  |  | S1-U data transfer not supported |
| 1 |  |  |  | S1-U data transfer supported |
| EMM-REGISTERED without PDN connection (ERw/oPDN) (octet 8, bit 6)This bit indicates the capability for EMM REGISTERED without PDN connectivity. |
| 0 |  |  |  | EMM-REGISTERED without PDN connection not supported |
| 1 |  |  |  | EMM-REGISTERED without PDN connection supported |
| Header compression for control plane CIoT EPS optimization (HC-CP CIoT) (octet 8, bit 7)This bit indicates the capability for header compression for control plane CIoT EPS optimization. |
| 0 |  |  |  | Header compression for control plane CIoT EPS optimization not supported |
| 1 |  |  |  | Header compression for control plane CIoT EPS optimization supported |
| Extended protocol configuration options (ePCO) (octet 8, bit 8)This bit indicates the support of the extended protocol configuration options IE. |
| 0 |  |  |  | Extended protocol configuration options IE not supported |
| 1 |  |  |  | Extended protocol configuration options IE supported |
| Multiple DRB support (multipleDRB) (octet 9, bit 1)This bit indicates the capability to support multiple user plane radio bearers (see 3GPP TS 36.306 [44], 3GPP TS 36.331 [22]) in NB-S1 mode. |
| 0 |  |  |  | Multiple DRB not supported |
| 1 |  |  |  | Multiple DRB supported |
| V2X communication over PC5 (V2X PC5) (octet 9, bit 2)This bit indicates the capability for V2X communication over E-UTRA-PC5. |
| 0 |  |  |  | V2X communication over E-UTRA-PC5 not supported |
| 1 |  |  |  | V2X communication over E-UTRA-PC5 supported |
| Restriction on use of enhanced coverage support (RestrictEC) (octet 9, bit 3)This bit indicates the capability to support restriction on use of enhanced coverage. |
| 0 |  |  |  | Restriction on use of enhanced coverage not supported |
| 1 |  |  |  | Restriction on use of enhanced coverage supported |
| Control plane data backoff support (CP backoff) (octet 9, bit 4)This bit indicates the support of back-off timer for transport of user data via the control plane.. |
| 0 |  |  |  | back-off timer for transport of user data via the control plane not supported |
| 1 |  |  |  | back-off timer for transport of user data via the control plane supported |
| Dual connectivity with NR (DCNR) (octet 9, bit 5)This bit indicates the capability for dual connecitivity with NR. |
| 0 |  |  |  | dual connectivity with NR not supported |
| 1 |  |  |  | dual connectivity with NR supported |
| N1 mode supported (N1mode) (octet 9, bit 6)This bit indicates the capability for N1 mode for 3GPP access. |
| 0 |  |  |  | N1 mode for 3GPP access not supported |
| 1 |  |  |  | N1 mode for 3GPP access supported |
| Service gap control (SGC) (octet 9, bit 7)This bit indicates the capability for service gap control |
| 0 |  |  |  | service gap control not supported |
| 1 |  |  |  | service gap control supported |
| Signalling for a maximum number of 15 EPS bearer contexts (15 bearers) (octet 9, bit 8)This bit indicates the support of signalling for a maximum number of 15 EPS bearer contexts |
| 0 |  |  |  | Signalling for a maximum number of 15 EPS bearer contexts not supported |
| 1 |  |  |  | Signalling for a maximum number of 15 EPS bearer contexts supported |
| Radio capability signalling optimisation (RACS) capability (octet 10, bit 1)This bit indicates the capability for RACS. |
| 0 |  |  |  | RACS not supported |
| 1 |  |  |  | RACS supported |
| Wake-up signal (WUS) assistance (octet 10, bit 2)This bit indicates the support of wake-up signal assistance |
| 0 |  |  |  | WUS assistance not supported |
| 1 |  |  |  | WUS assistance supported |
| Control plane Mobile Terminated-Early Data Transmission (CP-MT-EDT) (octet 10, bit 3)This bit indicates the support of control plane Mobile Terminated-Early Data Transmission |
| 0 |  |  |  | Control plane Mobile Terminated-Early Data Transmission not supported |
| 1 |  |  |  | Control plane Mobile Terminated-Early Data Transmission supported |
| User plane Mobile Terminated-Early Data Transmission (UP-MT-EDT) (octet 10, bit 4)This bit indicates the support of user plane Mobile Terminated-Early Data Transmission |
| 0 |  |  |  | User plane Mobile Terminated-Early Data Transmission not supported |
| 1 |  |  |  | User plane Mobile Terminated-Early Data Transmission supported |
| V2X communication over NR-PC5 (V2X NR-PC5) (octet 10, bit 5)This bit indicates the capability for V2X communication over NR-PC5. |
| 0 |  |  |  | V2X communication over NR-PC5 not supported |
| 1 |  |  |  | V2X communication over NR-PC5 supported |
| All other bits in octet 10 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. |
|  |
| NOTE 1: For a UE supporting dual connectivity with NR, if the UE supports one of the encryption algorithms for E-UTRAN (bits 8 to 5 of octet 3), it shall support the same algorithm for NR-PDCP as specified in 3GPP TS 33.401 [19]. The NR-PDCP is specified in 3GPP TS 38.323 [53].NOTE 2: For a UE supporting dual connectivity with NR, if the UE supports one of the integrity algorithms for E-UTRAN (bits 8 to 5 of octet 4), it shall support the same algorithm for NR-PDCP as specified in 3GPP TS 33.401 [19]. |

\*\*\*\*\* change \*\*\*\*\*

#### 9.9.3.36 UE security capability

The UE security capability information element is used by the network to indicate which security algorithms are supported by the UE in S1 mode, Iu mode and Gb mode. Security algorithms supported in S1 mode are supported both for NAS and for AS security. If the UE supports S101 mode, then these security algorithms are also supported for NAS security in S101 mode.

The UE security capability information element is coded as shown in figure 9.9.3.36.1 and table 9.9.3.36.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 7 octets.

Octets 5, 6, and 7 are optional. If octet 5 is included, then also octet 6 shall be included and octet 7 may be included.

If a UE did not indicate support of any security algorithm for Gb mode, octet 7 shall not be included. If the UE did not indicate support of any security algorithm for Iu mode and Gb mode, octets 5, 6, and 7 shall not be included.

If the UE did not indicate support of any security algorithm for Iu mode but indicated support of a security algorithm for Gb mode, octets 5, 6, and 7 shall be included. In this case octets 5 and 6 are filled with the value of zeroes.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE security capability IEI | octet 1 |
| Length of UE security capability contents | octet 2 |
| EEA0 | 128-EEA1 | 128-EEA2 | 128-EEA3 | EEA4 | EEA5 | EEA6 | EEA7 | octet 3 |
| EIA0 | 128-EIA1 | 128-EIA2 | 128-EIA3 | EIA4 | EIA5 | EIA6 | EPS-UPIP | octet 4 |
| UEA0 | UEA1 | UEA2 | UEA3 | UEA4 | UEA5 | UEA6 | UEA7 | octet 5\* |
| 0spare | UIA1 | UIA2 | UIA3 | UIA4 | UIA5 | UIA6 | UIA7 | octet 6\* |
| 0spare | GEA1 | GEA2 | GEA3 | GEA4 | GEA5 | GEA6 | GEA7 | octet 7\* |

Figure 9.9.3.36.1: UE security capability information element

Table 9.9.3.36.1: UE security capability information element

|  |
| --- |
| EPS encryption algorithms supported (octet 3) |
|  |
| EPS encryption algorithm EEA0 supported (octet 3, bit 8) |
| 0 |  |  |  | EPS encryption algorithm EEA0 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA0 supported |
|  |
| EPS encryption algorithm 128-EEA1 supported (octet 3, bit 7) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA1 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA1 supported |
|  |
| EPS encryption algorithm 128-EEA2 supported (octet 3, bit 6) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA2 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA2 supported |
|  |
| EPS encryption algorithm 128-EEA3 supported (octet 3, bit 5) |
| 0 |  |  |  | EPS encryption algorithm 128-EEA3 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA3 supported |
|  |
| EPS encryption algorithm EEA4 supported (octet 3, bit 4) |
| 0 |  |  |  | EPS encryption algorithm EEA4 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA4 supported |
|  |
| EPS encryption algorithm EEA5 supported (octet 3, bit 3) |
| 0 |  |  |  | EPS encryption algorithm EEA5 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA5 supported |
|  |
| EPS encryption algorithm EEA6 supported (octet 3, bit 2) |
| 0 |  |  |  | EPS encryption algorithm EEA6 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA6 supported |
|  |
| EPS encryption algorithm EEA7 supported (octet 3, bit 1) |
| 0 |  |  |  | EPS encryption algorithm EEA7 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA7 supported |
|  |
| EPS integrity algorithms supported (octet 4) |
|  |
| EPS integrity algorithm EIA0 supported (octet 4, bit 8) |
| 0 |  |  |  | EPS integrity algorithm EIA0 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA0 supported |
|  |
| EPS integrity algorithm 128-EIA1 supported (octet 4, bit 7) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA1 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA1 supported |
|  |
| EPS integrity algorithm 128-EIA2 supported (octet 4, bit 6) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA2 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA2 supported |
|  |
| EPS integrity algorithm 128-EIA3 supported (octet 4, bit 5) |
| 0 |  |  |  | EPS integrity algorithm 128-EIA3 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA3 supported |
|  |
| EPS integrity algorithm EIA4 supported (octet 4, bit 4) |
| 0 |  |  |  | EPS integrity algorithm EIA4 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA4 supported |
|  |
| EPS integrity algorithm EIA5 supported (octet 4, bit 3) |
| 0 |  |  |  | EPS integrity algorithm EIA5 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA5 supported |
|  |
| EPS integrity algorithm EIA6 supported (octet 4, bit 2) |
| 0 |  |  |  | EPS integrity algorithm EIA6 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA6 supported |
|  |
| EPS-UPIP supported (octet 4, bit 1) |
| 0 |  |  |  | EPS-UPIP not supported |
| 1 |  |  |  | EPS-UPIP supported |
|  |
| UMTS encryption algorithms supported (octet 5) |
|  |
| UMTS encryption algorithm UEA0 supported (octet 5, bit 8) |
| 0 |  |  |  | UMTS encryption algorithm UEA0 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA0 supported |
|  |
| UMTS encryption algorithm UEA1 supported (octet 5, bit 7) |
| 0 |  |  |  | UMTS encryption algorithm UEA1 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA1 supported |
|  |
| UMTS encryption algorithm UEA2 supported (octet 5, bit 6) |
| 0 |  |  |  | UMTS encryption algorithm UEA2 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA2 supported |
|  |
| UMTS encryption algorithm UEA3 supported (octet 5, bit 5) |
| 0 |  |  |  | UMTS encryption algorithm UEA3 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA3 supported |
|  |
| UMTS encryption algorithm UEA4 supported (octet 5, bit 4) |
| 0 |  |  |  | UMTS encryption algorithm UEA4 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA4 supported |
|  |
| UMTS encryption algorithm UEA5 supported (octet 5, bit 3) |
| 0 |  |  |  | UMTS encryption algorithm UEA5 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA5 supported |
|  |
| UMTS encryption algorithm UEA6 supported (octet 5, bit 2) |
| 0 |  |  |  | UMTS encryption algorithm UEA6 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA6 supported |
|  |
| UMTS encryption algorithm UEA7 supported (octet 5, bit 1) |
| 0 |  |  |  | UMTS encryption algorithm UEA7 not supported |
| 1 |  |  |  | UMTS encryption algorithm UEA7 supported |
|  |
| UMTS integrity algorithms supported (octet 6) |
|  |
| Bit 8 of octet 6 is spare and shall be coded as zero. |
|  |
| UMTS integrity algorithm UIA1 supported (octet 6, bit 7) |
| 0 |  |  |  | UMTS integrity algorithm UIA1 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA1 supported |
|  |
| UMTS integrity algorithm UIA2 supported (octet 6, bit 6) |
| 0 |  |  |  | UMTS integrity algorithm UIA2 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA2 supported |
|  |
| UMTS integrity algorithm UIA3 supported (octet 6, bit 5) |
| 0 |  |  |  | UMTS integrity algorithm UIA3 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA3 supported |
|  |
| UMTS integrity algorithm UIA4 supported (octet 6, bit 4) |
| 0 |  |  |  | UMTS integrity algorithm UIA4 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA4 supported |
|  |
| UMTS integrity algorithm UIA5 supported (octet 6, bit 3) |
| 0 |  |  |  | UMTS integrity algorithm UIA5 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA5 supported |
|  |
| UMTS integrity algorithm UIA6 supported (octet 6, bit 2) |
| 0 |  |  |  | UMTS integrity algorithm UIA6 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA6 supported |
|  |
| UMTS integrity algorithm UIA7 supported (octet 6, bit 1) |
| 0 |  |  |  | UMTS integrity algorithm UIA7 not supported |
| 1 |  |  |  | UMTS integrity algorithm UIA7 supported |
|  |
| GPRS encryption algorithms supported (octet 7) |
|  |
| Bit 8 of octet 7 is spare and shall be coded as zero. |
|  |
| GPRS encryption algorithm GEA1 supported (octet 7, bit 7) |
| 0 |  |  |  | GPRS encryption algorithm GEA1 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA1 supported |
|  |
| GPRS encryption algorithm GEA2 supported (octet 7, bit 6) |
| 0 |  |  |  | GPRS encryption algorithm GEA2 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA2 supported |
|  |
| GPRS encryption algorithm GEA3 supported (octet 7, bit 5) |
| 0 |  |  |  | GPRS encryption algorithm GEA3 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA3 supported |
|  |
| GPRS encryption algorithm GEA4 supported (octet 7, bit 4) |
| 0 |  |  |  | GPRS encryption algorithm GEA4 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA4 supported |
|  |
| GPRS encryption algorithm GEA5 supported (octet 7, bit 3) |
| 0 |  |  |  | GPRS encryption algorithm GEA5 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA5 supported |
|  |
| GPRS encryption algorithm GEA6 supported (octet 7, bit 2) |
| 0 |  |  |  | GPRS encryption algorithm GEA6 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA6 supported |
|  |
| GPRS encryption algorithm GEA7 supported (octet 7, bit 1) |
| 0 |  |  |  | GPRS encryption algorithm GEA7 not supported |
| 1 |  |  |  | GPRS encryption algorithm GEA7 supported |
|  |
| NOTE 1: For a UE supporting dual connectivity with NR, if the UE supports one of the encryption algorithms for E-UTRAN (bits 8 to 5 of octet 3), it shall support the same algorithm for NR-PDCP as specified in 3GPP TS 33.401 [19].NOTE 2: For a UE supporting dual connectivity with NR, if the UE supports one of the integrity algorithms for E-UTRAN different from EIA0 (bits 7 to 5 of octet 4), it shall support the same algorithm for NR-PDCP as specified in 3GPP TS 33.401 [19]. |