**3GPP TSG-CT WG1 Meeting #123-eC1-202xxx**

**Electronic meeting, 16-24 April 2020 (was C1-202104)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0002** | **rev** | **1** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | PC5 unicast link security establishment | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-04-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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:*** | | 1. At SA3#98e, SA3 agreed pCRs S3-200506 and S3-200507 to TS 33.536 specifying procedures for key derivation and security establishment for the PC5 unicast link. TS 24.587 needs to be updated accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. The place holders in TS 24.587 for the PC5 unicast link authentication procedure and the PC5 unicast link security mode control procedure were populated with contents based on the agreed SA3 pCRs, and the corresponding message contents and IEs were specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 1. The PC5 unicast link authentication procedure and the PC5 unicast link security mode control procedure will remain unspecified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.1, 3.2, 6.1.2.2.2, 6.1.2.2.3, 6.1.2.6.1, 6.1.2.6.2, 6.1.2.6.3, 6.1.2.6.4, 6.1.2.6.5, 6.1.2.6.6, 6.1.2.6.6.1 (New), 6.1.2.7.1, 6.1.2.7.2, 6.1.2.7.3, 6.1.2.7.4, 6.1.2.7.5, 6.1.2.7.6, 6.1.2.7.6.1 (New), 7.3.1.1, 7.3.1.x (New), 7.3.a (New), 7.3.a.1 (New), 7.3.b (New), 7.3.b.1 (New), 7.3.c (New), 7.3.c.1 (New), 7.3.d (New), 7.3.d.1 (New), 7.3.d.2 (New), 7.3.d.3 (New), 7.3.d.4 (New), 7.3.e (New), 7.3.e.1 (New), 7.3.e.2 (New), 7.3.e.3 (New), 7.3.e.4 (New), 7.3.f (New), 7.3.f.1 (New), 8.4.1, 8.4.9, 8.4.a (New), 8.4.b (New), 8.4.c (New), 8.4.d (New), 8.4.e (New), 8.4.f (New), 8.4.g (New), 8.4.h (New), 8.4.i (New), 8.4.j (New), 10.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[3] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[5] 3GPP TS 24.386 "User Equipment (UE) to V2X control function; protocol aspects; Stage 3".

[6] 3GPP TS 24.501: "Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[7] 3GPP TS 24.588: "Vehicle-to-Everything (V2X) services in 5G System (5GS); User Equipment (UE) policies; Stage 3".

[8] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[9] 3GPP TS 38.304: "User Equipment (UE) procedures in Idle mode and RRC Inactive state".

[10] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[11] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

[12] ETSI EN 302 636-3 v1.2.1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture".

[13] IEEE 1609.3 2016: "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services".

[14] IETF RFC 768: "User Datagram Protocol".

[15] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[16] IETF RFC 4862: "Neighbor Discovery for IP version 6 (IPv6)".

[17] ISO 29281-1 2013: "Intelligent transport systems -- Communication access for land mobiles (CALM) -- Non-IP networking -- Part 1: Fast networking & transport layer protocol (FNTP)".

[18] ISO TS 17419 ITS-AID AssignedNumbers: <http://standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers/TS17419_ITS-AID_AssignedNumbers.pdf>

[yy] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

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

**E-UTRA-PC5:** PC5 reference point over E-UTRA. The term E-UTRA-PC5 used in the present document corresponds to the term LTE PC5 defined in 3GPP TS 23.287 [3].

**NR-PC5:** PC5 reference point over NR. The term NR-PC5 used in the present document corresponds to the term NR PC5 defined in 3GPP TS 23.287 [3].

**PC5 QoS flow context:** A context which includes a V2X service identifier and a set of PC5 QoS parameters.

**PC5 QoS rule:** A rule which includes a PC5 QoS rule identifier, a PFI value, a precedence value and optionally a set of packet filters. The PC5 QoS rule is associated with a PC5 QoS flow context.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.287 [3] apply:

**V2X communication**

**V2X message**

**V2X service**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.501 [6] apply:

**5G-EA**

**5G-IA**

## 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].

E-UTRA Evolved Universal Terrestrial Radio Access

NR New Radio

NRPEK NR PC5 Encryption Key

NRPIK NR PC5 Integrity Key

V2X Vehicle-to-Everything

V2XP V2X Policy

PQFI PC5 QoS Flow ID

PQI PC5 5QI

\*\*\* Next change \*\*\*

##### 6.1.2.2.2 PC5 unicast link establishment procedure initiation by initiating UE

Editor’s note: This section needs to be revisited after SA3 have determined the full set of security requirements for unicast link establishment.

The initiating UE shall meet the following pre-conditions before initiating this procedure:

a) a request from upper layers to transmit the packet for V2X service over PC5;

b) the link layer identifier for the initiating UE (i.e. layer 2 ID used for unicast communication) is available (e.g. pre-configured or self-assigned);

c) the link layer identifier for the unicast initial signaling (i.e. destination layer 2 ID used for unicast initial signaling) is available to the initiating UE (e.g. pre-configured, obtained as specified in clause 5.2.3 or known via prior V2X communication);

d) the initiating UE is either authorised for V2X communication over PC5 in NR in the serving PLMN, or has a valid authorization for V2X communication over PC5 in NR when not served by E-UTRAN and not served by NR; and

e) there is no existing PC5 unicast link for the pair of peer application layer IDs and the network layer protocol of this PC5 unicast link are identical to those required by the upper layer in the initiating UE for this V2X service.

In order to initiate the PC5 unicast link establishment procedure, the initiating UE shall create a DIRECT LINK ESTABLISHMENT REQUEST message. The initiating UE:

a) shall include the source user info set to the initiating UE’s application layer ID received from upper layers;

b) shall include the V2X service identifier received from upper layer;

c) may include the target user info set to the target UE’s application layer ID if received from upper layers;

d) shall include the Key establishment information container;

NOTE 1: The Key establishment information container is provided by upper layers.

e) shall include a Nonce\_1 set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this PC5 unicast link;

f) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the security establishment of this PC5 unicast link;

g) shall include its UE PC5 unicast signalling security policy for this PC5 unicast link;

h) shall include the 8 MSBs of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [yy]; and

i) may include a KNRP ID if the initiating UE has an existing KNRP for the target UE.

After the DIRECT LINK ESTABLISHMENT REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's Layer 2 ID for unicast communication and the destination layer 2 ID used for unicast initial signaling, and start timer T5000. The UE shall not send a new DIRECT LINK ESTABLISHMENT REQUEST message to the same target UE identified by the same application layer ID while timer T5000 is running.

NOTE 2: In order to ensure successful PC5 unicast link establishment, T5000 should be set to a value larger than the sum of T5aaa and T5bbb.



Figure 6.1.2.2.2: PC5 unicast link establishment procedure

##### 6.1.2.2.3 PC5 unicast link establishment procedure accepted by the target UE

Upon receipt of a DIRECT LINK ESTABLISHMENT REQUEST message, the target UE shall assign a layer-2 ID for this PC5 unicast link and store this assigned layer-2 ID and the source layer 2 ID used in the transport of this message provided by the lower layers. This pair of layer-2 IDs is associated with a PC5 unicast link context.

If:

a) the target user info IE is included in the DIRECT LINK ESTABLISHMENT REQUEST message and this IE includes the target UE’s application layer ID; or

b) the target user info IE is not included in the DIRECT LINK ESTABLISHMENT REQUEST message and the target UE is interested in the V2X service identified by the V2X service identifier in the DIRECT LINK ESTABLISHMENT REQUEST message;

then the target UE shall either:

a) identify an existing KNRP based on the KNRP ID included in the DIRECT LINK ESTABLISHMENT REQUEST message; or

b) if KNRP ID is not included in the DIRECT LINK ESTABLISHMENT REQUEST message, the target UE does not have an existing KNRP for the KNRP ID included in DIRECT LINK ESTABLISHMENT REQUEST message or the target UE wishes to derive a new KNRP, derive a new KNRP. This may require performing one or more PC5 unicast link authentication procedures as specified in subclause 6.1.2.6.

NOTE: How many times the PC5 unicast link authentication procedure needs to be performed to derive a new KNRP depends on the authentication method used.

After an existing KNRP was identified or a new KNRP was derived, the target UE shall initiate a PC5 unicast link security mode control procedure as specified in in subclause 6.1.2.7.

Upon successful completion of the PC5 unicast link security mode control procedure, in order to determine whether the DIRECT LINK ESTABLISHMENT REQUEST message can be accepted or not, in case of IP communication, the target UE checks whether there is at least one common IP address configuration option supported by both the initiating UE and the target UE.

If the target UE accepts the PC5 unicast link establishment procedure, the target UE shall create a DIRECT LINK ESTABLISHMENT ACCEPT message. The target UE:

a) shall include the source user info set to the target UE’s application layer ID received from upper layers;

b) shall include a PQFI and the corresponding PC5 QoS parameters;

c) may include an IP address configuration IE set to one of the following values if IP communication is used:

1) "IPv6 router" if only IPv6 address allocation mechanism is supported by the target UE, i.e. acting as an IPv6 router; or

2) "IPv6 address allocation not supported" if IPv6 address allocation mechanism is not supported by the target UE; and

d) may include a link local IPv6 address IE formed locally based on IETF RFC 4862 [16] if IP address configuration IE is set to "IPv6 address allocation not supported" and the received DIRECT LINK ESTABLISHMENT REQUEST message included a link local IPv6 address IE.

After the DIRECT LINK ESTABLISHMENT ACCEPT message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer 2 ID for unicast communication and the target UE's layer 2 ID for unicast communication.

\*\*\* Next change \*\*\*

#### 6.1.2.6 PC5 unicast link authentication procedure

##### 6.1.2.6.1 General

The PC5 unicast link authentication procedure is used to perform mutual authentication of UEs establishing a PC5 unicast link and to derive a new KNRP shared between two UEs during a PC5 unicast link establishment procedure or a PC5 unicast link re-keying procedure. After successful completion of the PC5 unicast link authentication procedure, the new KNRP is used for security establishment during the PC5 unicast link security mode control procedure as specified in clause 6.1.2.7. The UE sending the DIRECT LINK AUTHENTICATION REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

##### 6.1.2.6.2 PC5 unicast link authentication procedure initiation by the initiating UE

The initiating UE shall meet one of the following pre-conditions before initiating the PC5 unicast link authentication procedure:

a) the target UE has initiated a PC5 unicast link establishment procedure toward the initiating UE by sending a DIRECT LINK ESTABLISHMENT REQUEST message and:

1) the DIRECT LINK ESTABLISHMENT REQUEST message:

1) includes a target user info IE which includes the application layer ID of the initiating UE; or

2) does not include a target user info IE and the initiating UE is interested in the V2X service identified by the V2X service identifier in the DIRECT LINK ESTABLISHMENT REQUEST message; and

2) the KNRP ID is not included in the DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE does not have an existing KNRP for the KNRP ID included in DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE wishes to derive a new KNRP, derive a new KNRP; or

b) the target UE has initiated a PC5 unicast link re-keying procedure toward the initiating UE by sending a DIRECT LINK REKEYING REQUEST message and the DIRECT LINK REKYING REQUEST message includes a Re-authentication indication.

In order to initiate the PC5 unicast link authentication procedure, the initiating UE shall create a DIRECT LINK AUTHENTICATION REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container.

NOTE: The Key establishment information container is provided by upper layers.

After the DIRECT LINK AUTHENTICATION REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer 2 ID for unicast communication and the target UE's layer 2 ID for unicast communication.

The initiating UE shall start timer T5aaa. The UE shall not send a new DIRECT LINK AUTHENTICATION REQUEST message to the same target UE while timer T5aaa is running.



Figure 6.1.2.6.2: PC5 unicast link authentication procedure

##### 6.1.2.6.3 PC5 unicast link authentication procedure accepted by the target UE

Upon receipt of a DIRECT LINK AUTHENTICATION REQUEST message, if the target UE determines that the DIRECT LINK AUTHENTICATION REQUEST message can be accepted, the target UE shall create a DIRECT LINK AUTHENTICATION RESPONSE message. In this message, the target UE:

a) shall include the Key establishment information container.

NOTE: The Key establishment information container is provided by upper layers.

After the DIRECT LINK AUTHENTICATION RESPONSE message is generated, the target UE shall pass this message to the lower layers for transmission along with the target UE's layer 2 ID for unicast communication and the initiating UE's layer 2 ID for unicast communication.

##### 6.1.2.6.4 PC5 unicast link authentication procedure completion by the initiating UE

Upon receiving a DIRECT LINK AUTHENTICATION RESPONSE message, the initiating UE shall stop timer T5aaa.

##### 6.1.2.6.5 PC5 unicast link authentication procedure not accepted by the target UE

If the DIRECT LINK AUTHENTICATION REQUEST message cannot be accepted, the target UE shall create a DIRECT LINK AUTHENTICATION REJECT message. In this message, the target UE shall include a PC5 signaling protocol cause IE indicating one of the following cause values:

#a: Authentication failure.

After the DIRECT LINK AUTHENTICATION REJECT message is generated, the target UE shall pass this message to the lower layers for transmission along with the initiating UE's layer 2 ID for unicast communication and the target UE's layer 2 ID for unicast communication.

The target UE shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link authentication procedure.

Upon receipt of the DIRECT LINK AUTHENTICATION REJECT message, the initiating UE shall stop timer T5aaa and abort the ongoing procedure that triggered the initiation of the PC5 unicast link authentication procedure.

##### 6.1.2.6.6 Abnormal cases

###### 6.1.2.6.6.1 Abnormal cases at the initiating UE

a) Timer T5aaa expires.

The initiating UE shall retransmit the DIRECT LINK AUTHENTICATION REQUEST message and restart timer T5aaa. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link authentication procedure and shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link authentication procedure.

NOTE: The maximum number of allowed retransmissions is UE implementation specific.

b) The need to use this PC5 unicast link no longer exists before the PC5 unicast link authentication procedure is completed.

The initiating UE shall abort the procedure and shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link authentication procedure.

#### 6.1.2.7 PC5 unicast link security mode control procedure

##### 6.1.2.7.1 General

The PC5 unicast link security mode control procedure is used to establish security between two UEs during a PC5 unicast link establishment procedure or a PC5 unicast link re-keying procedure. After successful completion of the PC5 unicast link security mode control procedure, the selected security algorithms and keys are used to integrity protect and cipher all PC5 signalling messages exchanged between the UEs and the security context can be used to protect all PC5 user plane data exchanged between the UEs. The UE sending the DIRECT LINK SECURITY MODE COMMAND message is called the "initiating UE" and the other UE is called the "target UE".

Editor’s note: It is FFS whether the user plane is protected by the security association.

##### 6.1.2.7.2 PC5 unicast link security mode control procedure initiation by the initiating UE

The initiating UE shall meet the following pre-conditions before initiating the PC5 unicast link security mode control procedure:

a) the target UE has initiated a PC5 unicast link establishment procedure toward the initiating UE by sending a DIRECT LINK ESTABLISHMENT REQUEST message and:

1) the DIRECT LINK ESTABLISHMENT REQUEST message:

i) includes a target user info IE which includes the application layer ID of the initiating UE; or

ii) does not include a target user info IE and the initiating UE is interested in the V2X service identified by the V2X service identifier in the DIRECT LINK ESTABLISHMENT REQUEST message; and

2) the initiating UE has either identified an existing KNRP based on the KNRP ID included in the DIRECT LINK ESTABLISHMENT REQUEST message or derived a new KNRP; or

b) the target UE has initiated a PC5 unicast link re-keying procedure toward the initiating UE by sending a DIRECT LINK REKEYING REQUEST message and:

1) if the target UE has included a Re-authentication indication in the DIRECT LINK REKEYING REQUEST message, the initiating UE has derived a new KNRP.

If a new KNRP has been derived by the initiating UE, the initiating UE shall generate the 16 MSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the initiating UE.

The initiating UE shall select security algorithms in accordance with its UE PC5 unicast signalling security policy and the target UE’s PC5 unicast signalling security policy. If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, the initiating UE shall not select the null integrity protection algorithm if the initiating UE or the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required". If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the initiating UE shall not select the null integrity protection algorithm if the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm.

Then the initiating UE shall:

a) generate a 128-bit Nonce\_2 value;

b) derive KNRP-sess from KNRP, Nonce\_2 and Nonce\_1 received in the DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.536 [yy];

c) derive the NR PC5 encryption key NRPEK and the NR PC5 integrity key NRPIK from KNRP-sess and the selected security algorithms as specified in 3GPP TS 33.536 [yy], and

d) create a DIRECT LINK SECURITY MODE COMMAND message. In this message, the initiating UE:

1) shall include the Key establishment information container if a new KNRP has been derived at the initiating UE and the authentication method used to generate KNRP requires sending information to complete the authentication procedure;

NOTE: The Key establishment information container is provided by upper layers.

2) shall include the MSB of KNRP ID if a new KNRP has been derived at the initiating UE;

3) shall include a Nonce\_2 set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this PC5 unicast link;

4) shall include the selected security algorithms;

5) shall include the UE security capabilities received from the target UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

6) shall include the 8 LSBs of KNPR-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [yy]; and

7) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, shall include the UE PC5 unicast signalling security policy received from the target UE in the DIRECT LINK ESTABLISHMENT REQUEST message.

The initiating UE shall form the KNPR-sess ID from the 8 MSBs of KNPR-sess ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNPR-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message.

The initiating UE shall not cipher the DIRECT LINK SECURITY MODE COMMAND message but shall integrity protect it with the new security context.

After the DIRECT LINK SECURITY MODE COMMAND message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer 2 ID for unicast communication and the target UE's layer 2 ID for unicast communication, and start timer T5bbb. The UE shall not send a new DIRECT LINK SECURITY MODE COMMAND message to the same target UE while timer T5bbb is running.



Figure 6.1.2.7.2: PC5 unicast link security mode control procedure

##### 6.1.2.7.3 PC5 unicast link security mode control procedure accepted by the target UE

Upon receipt of a DIRECT LINK SECURITY MODE COMMAND message, if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, the target UE shall check that the 8 LSBs of KNPR-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message are not set to the same value as those received from another UE in response to the target UE’s DIRECT LINK ESTABLISHMENT REQUEST message.

Then the target UE shall:

a) derive KNRP-sess from KNRP, Nonce\_1 and Nonce\_2 received in the DIRECT LINK SECURITY MODE COMMAND message as specified in 3GPP TS 33.536 [yy]; and

b) derive NRPEK and NRPIK from KNRP-sess and the selected security algorithms as specified in 3GPP TS 33.536 [yy].

The target UE shall determine whether or not the DIRECT LINK SECURITY MODE COMMAND message can be accepted by:

a) checking the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK;

b) checking that the received UE security capabilities have not been altered compared to the values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

c) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, checking that the received UE PC5 unicast signalling security policy has not been altered compared to the values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message;

d) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message do not include the null integrity protection algorithm if the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required"; and

e) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure and the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm, checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message do not include the null integrity protection algorithm.

If the target UE did not include a KNRP ID in the DIRECT LINK ESTABLISHMENT REQUEST message, the target UE included a Re-authentication indication in the DIRECT LINK REKEYING REQUEST message or the initiating UE has chosen to derive a new KNRP, the target UE shall derive KNRP as specified in 3GPP TS 33.536 [yy]. The target UE shall choose the 16 LSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the target UE. The target UE shall form KNRP ID from the received MSBs of KNRP ID and its chosen LSBs of KNRP ID and shall store the complete KNRP ID with KNRP.

If the target UE accepts the DIRECT LINK SECURITY MODE COMMAND message, the target UE shall create a DIRECT LINK SECURITY MODE COMPLETE message. In this message, the target UE:

a) shall include the PQFI and the corresponding PC5 QoS parameters;

b) if IP communication is used, shall include an IP address configuration IE set to one of the following values:

1) "IPv6 router" if only IPv6 address allocation mechanism is supported by the target UE, i.e. acting as an IPv6 router; or

2) "IPv6 address allocation not supported" if IPv6 address allocation mechanism is not supported by the target UE;

c) if IP communication is used and the IP address configuration IE is set to "IPv6 address allocation not supported", shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [6]; and

d) if a new KNRP was derived, shall include the 16 LSBs of KNRP ID; and

e) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, shall include its UE PC5 unicast user plane security policy for this PC5 unicast link.

Editor’s note: Whether the target UE includes is UE PC5 unicast user plane security policy in the DIRECT LINK SECURITY MODE COMPLETE is FFS.

The target UE shall form the KNPR-sess ID from the 8 MSBs of KNPR-sess ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNPR-sess ID received in the DIRECT LINK SECURITY MODE COMMAND message.

The target UE shall cipher and integrity protect the DIRECT LINK SECURITY MODE COMPLETE message with the new security context.

After the DIRECT LINK SECURITY MODE COMPLETE message is generated, the target UE shall pass this message to the lower layers for transmission along with the target UE's layer 2 ID for unicast communication and the initiating UE's layer 2 ID for unicast communication.

##### 6.1.2.7.4 PC5 unicast link security mode control procedure completion by the initiating UE

Upon receiving a DIRECT LINK SECURITY MODE COMPLETE message, the initiating UE shall stop timer T5bbb and check the integrity of the DIRECT LINK SECURITY MODE COMPLETE message. If the integrity check passes, the initiating UE shall then continue the procedure which triggered the PC5 unicast link security mode control procedure.

##### 6.1.2.7.5 PC5 unicast link security mode control procedure not accepted by the target UE

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted, the target UE shall send a DIRECT LINK SECURITY MODE REJECT message and abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure. The DIRECT LINK SECURITY MODE REJECT message contains a PC5 signalling protocol cause IE indicating one of the following cause values:

#a: Authentication failure;

#b: Integrity failure;

#c: UE security capabilities mismatch;

#d: UE PC5 unicast signalling security policy mismatch;

#e: LSBs of KNPR-sess ID conflict; or

#111: Protocol error, unspecified.

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message included the null integrity protection algorithm and the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required", the target UE shall include PC5 signalling protocol cause #d "UE PC5 unicast signalling security policy mismatch" in the SECURITY MODE REJECT message.

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm and the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message include the null integrity protection algorithm, the target UE, the target UE shall include PC5 signalling protocol cause #d "UE PC5 unicast signalling security policy mismatch" in the SECURITY MODE REJECT message.

Upon receipt of the DIRECT LINK SECURITY MODE REJECT message, the initiating UE shall stop timer T5bbb and:

a) if the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is set to #e, retransmit the DIRECT LINK SECURITY MODE COMMAND message with a different value for the 8 LSBs of KNPR-sess ID; and

b) otherwise, abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure.

##### 6.1.2.7.6 Abnormal cases

###### 6.1.2.7.6.1 Abnormal cases at the initiating UE

a) Timer T5bbb expires.

The initiating UE shall retransmit the DIRECT LINK SECURITY MODE COMMAND message and restart timer T5bbb. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link security mode control procedure and shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure.

NOTE: The maximum number of allowed retransmissions is UE implementation specific.

b) The need to use this PC5 unicast link no longer exists before the PC5 unicast link security mode control procedure is completed.

The initiating UE shall abort the procedure and shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure.

\*\*\* Next change \*\*\*

### 7.3.1 Direct link establishment request

#### 7.3.1.1 Message definition

This message is sent by a UE to another peer UE to establish a direct link. See table 7.3.1.1.1.

Message type: DIRECT LINK ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.1.1.1: DIRECT LINK ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK ESTABLISHMENT REQUEST message identity | PC5 signalling message type  8.4.1 | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | V2X service identifier | V2X service identifier  8.4.3 | M | LV | 4 |
|  | Source user info | Application layer ID  8.4.4 | M | LV | 3-253 |
|  | Key establishment information container | Key establishment information container  8.4.a | M | LV-E | 3-n |
|  | Nonce\_1 | Nonce  8.4.b | M | V | 16 |
|  | UE security capabilities | UE security capabilities  8.4.c | M | LV | 3-9 |
|  | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy  8.4.d | M | V | 1 |
|  | MSBs of KNRP-sess ID | MSBs of KNRP-sess ID  8.4.e | M | V | 1 |
| 28 | Target user info | Application layer ID  8.4.4 | O | TLV | 3-253 |
| XX | KNRP ID | KNRP ID  8.4.f | O | TV | 5 |

\*\*\* Next change \*\*\*

#### 7.3.1.x KNRP ID

The UE may include this IE if it has an existing KNRP for the target UE.

\*\*\* Next change \*\*\*

### 7.3.a Direct link authentication request

#### 7.3.a.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link authentication procedure is initiated. See table 7.3.a.1.1.

Message type: DIRECT LINK AUTHENTICATION REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.a.1.1: DIRECT LINK AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK AUTHENTICATION REQUEST message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Key establishment information container | Key establishment information container  8.4.a | M | LV-E | 3-n |

### 7.3.b Direct link authentication response

#### 7.3.b.1 Message definition

This message is sent by a UE to another peer UE to respond to a DIRECT LINK AUTHENTICATION REQUEST message. See table 7.3.b.1.1.

Message type: DIRECT LINK AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to peer UE

Table 7.3.b.1.1: DIRECT LINK AUTHENTICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK AUTHENTICATION RESPONSE message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Key establishment information container | Key establishment information container  8.4.a | M | LV-E | 3-n |

### 7.3.c Direct link authentication reject

#### 7.3.c.1 Message definition

This message is sent by a UE to another peer UE to reject a DIRECT LINK AUTHENTICATION REQUEST message. See table 7.3.c.1.1.

Message type: DIRECT LINK AUTHENTICATION REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.c.1.1: DIRECT LINK AUTHENTICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK AUTHENTICATION REJECT message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | PC5 signalling protocol cause value | PC5 signalling protocol cause value  8.4.9 | M | V | 1 |

### 7.3.d Direct link security mode command

#### 7.3.d.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link security mode control procedure is initiated. See table 7.3.d.1.1.

Message type: DIRECT LINK SECURITY MODE COMMAND

Significance: dual

Direction: UE to peer UE

Table 7.3.d.1.1: DIRECT LINK SECURITY MODE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK SECURITY MODE COMMAND message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Nonce\_2 | Nonce  8.4.b | M | V | 16 |
|  | Selected security algorithms | Selected security algorithms  8.4.g | M | V | 1 |
|  | UE security capabilities | UE security capabilities  8.4.c | M | LV | 3-9 |
|  | LSBs of KNRP-sess ID | LSBs of KNRP-sess ID  8.4.h | M | V | 1 |
| XX | Key establishment information container | Key establishment information container  8.4.a | O | TLV-E | 4-n |
| YY | MSBs of KNRP ID | MSBs of KNRP ID  8.4.i | O | TV | 3 |
| ZZ | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy  8.4.d | O | TV | 2 |

#### 7.3.d.2 Key establishment information container

The UE shall include this IE if the UE has derived a new KNRP and the authentication method used to generate KNRP requires sending information to complete the authentication procedure.

#### 7.3.d.3 MSBs of KNRP ID

The UE shall include this IE if the UE has derived a new KNRP.

#### 7.3.d.4 UE PC5 unicast signalling security policy

The UE shall include this IE if the PC5 unicast link security mode control procedure is triggered during a PC5 unicast link establishment procedure.

### 7.3.e Direct link security mode complete

#### 7.3.e.1 Message definition

This message is sent by a UE to another peer UE to respond to a DIRECT LINK SECURITY MODE COMMAND message. See table 7.3.e.1.1.

Message type: DIRECT LINK SECURITY MODE COMPLETE

Significance: dual

Direction: UE to peer UE

Table 7.3.e.1.1: DIRECT LINK SECURITY MODE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK SECURITY MODE COMPLETE message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | QoS flow descriptions | PC5 QoS flow descriptions  8.4.5 | M | LV-E | 6-n |
| 57 | IP address configuration | IP address configuration  8.4.6 | O | TV | 2 |
| 58 | Link local IPv6 address | Link local IPv6 address  8.4.7 | O | TV | 17 |
| AA | LSBs of KNRP ID | LSBs of KNRP ID  8.4.j | O | TV | 3 |

Editor’s note: Whether the UE includes is UE PC5 unicast user plane security policy in the DIRECT LINK SECURITY MODE COMPLETE is FFS.

#### 7.3.e.2 IP address configuration

The UE shall include this IE if IP communication is used.

#### 7.3.e.3 Link local IPv6 address

The UE shall include this IE if IP communication is used and the IP address configuration is set to "IPv6 address allocation not supported".

#### 7.3.e.4 LSBs of KNRP ID

The UE shall include this IE if a new KNRP was derived.

### 7.3.f Direct link security mode reject

#### 7.3.f.1 Message definition

This message is sent by a UE to another peer UE to reject a DIRECT LINK SECURITY MODE COMMAND message. See table 7.3.f.1.1.

Message type: DIRECT LINK SECURITY MODE REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.f.1.1: DIRECT LINK SECURITY MODE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK SECURITY MODE REJECT message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | PC5 signalling protocol cause | PC5 signalling protocol cause  8.4.9 | M | V | 1 |

\*\*\* Next change \*\*\*

### 8.4.1 PC5 signalling message type

The purpose of the PC5 signalling message type information element is to indicate the type of messages used in PC5 signalling protocol.

The value part of the PC5 signalling message type information element used in the PC5 signalling messages is coded as shown in table 8.4.1.1.

The PC5 signalling message type is a type 3 information element, with the length of 1 octet.

Table 8.4.1.1: PC5 signalling message type

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | |  |  |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | DIRECT LINK ESTABLISHMENT REQUEST |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |  | DIRECT LINK ESTABLISHMENT ACCEPT |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | DIRECT LINK ESTABLISHMENT REJECT |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |  | DIRECT LINK MODIFICATION REQUEST |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | DIRECT LINK MODIFICATION ACCEPT |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | DIRECT LINK MODIFICATION REJECT |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | DIRECT LINK RELEASE REQUEST |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |  | DIRECT LINK RELEASE ACCEPT |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |  | DIRECT LINK KEEPALIVE REQUEST |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | DIRECT LINK KEEPALIVE RESPONSE |
| a | a | a | a | a | a | a | a |  | DIRECT LINK AUTHENTICATION REQUEST |
| b | b | b | b | b | b | b | b |  | DIRECT LINK AUTHENTICATION RESPONSE |
| c | c | c | c | c | c | c | c |  | DIRECT LINK AUTHENTICATION REJECT |
| d | d | d | d | d | d | d | d |  | DIRECT LINK SECURITY MODE COMMAND |
| e | e | e | e | e | e | e | e |  | DIRECT LINK SECURITY MODE COMPLETE |
| f | f | f | f | f | f | f | f |  | DIRECT LINK SECURITY MODE REJECT |
|  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | |

Editor's note: The values of the other PC5 signalling messages are FFS.

\*\*\* Next change \*\*\*

### 8.4.9 PC5 signalling protocol cause

The purpose of the PC5 signalling protocol cause information element is to indicate the cause used in the PC5 signalling protocol procedures.

The PC5 signalling protocol cause is a type 3 information element with a length of 2 octets.

The PC5 signalling protocol cause information element is coded as shown in figure 8.4.9.1 and table 8.4.9.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PC5 signalling protocol cause IEI | | | | | | | | octet 1 |
| PC5 signalling cause value | | | | | | | | octet 2 |

Figure 8.4.9.1: PC5 signalling protocol cause information element

Table 8.4.9.1: PC5 signalling protocol cause information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PC5 signalling cause value (octet 2) | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | | 2 | | 1 | |  | |  | |
| 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | | 1 | |  | | Direct communication to the target UE not allowed | |
| 0 | 0 | 0 | 0 | 0 | 0 | | 1 | | 0 | |  | | Direct communication to the target UE no longer needed | |
| 0 | 0 | 0 | 0 | 0 | | 0 | | 1 | | 1 | |  | | Conflict of Layer 2 ID for unicast communication is detected | |
| 0 | 0 | 0 | 0 | 0 | 1 | | 0 | | 0 | |  | | Direct connection is not available anymore | |
| 0 | 0 | 0 | 0 | 0 | | 1 | | 0 | | 1 | |  | | Lack of resources for proposed link | |
| a | a | a | a | a | | a | | a | | a | |  | | Authentication failure | |
| b | b | b | b | b | | b | | b | | b | |  | | Integrity failure | |
| c | c | c | c | c | | c | | c | | c | |  | | UE security capabilities mismatch | |
| d | d | d | d | d | | d | | d | | d | |  | | UE PC5 unicast signalling security policy mismatch | |
| e | e | e | e | e | | e | | e | | e | |  | | LBSs of KNPR-sess ID conflict | |
|  |  |  |  |  | |  | |  | |  | |  | |  | |
| 0 | 1 | 1 | 0 | 1 | | 1 | | 1 | | 1 | |  | | Protocol error, unspecified | |
|  |  |  |  |  | |  | |  | |  | |  | |  | |
| Any other value received by the UE shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | | | | | | | |

\*\*\* Next change \*\*\*

### 8.4.a Key establishment information container

The Key establishment information container information element contains information for PC5 unicast link key establishment.

The Key establishment information container is a type 6 information element with a minimum length of 4 octets.

The Key establishment information container information element is coded as shown in figure 8.4.a.1 and table 8.4.a.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Key establishment information container IEI | | | | | | | | octet 1 |
| Length of key establishment information container contents | | | | | | | | octet 2  octet 3 |
| Key establishment information container contents | | | | | | | | octet 4 |
|  | | | | | | | | octet n |

Figure 8.4.a.1: Key establishment information container information element

Table 8.4.a.1: Key establishment information container information element

|  |
| --- |
| Key establishment information container contents (octet 4 to n)  This field contains the key establishment information container. |

### 8.4.b Nonce

The Nonce information element contains a 128-bit nonce used during PC5 unicast link security establishment.

The Nonce information element is a type 3 information element, with a length of 17 octets.

The Nonce information element is coded as shown in figure 8.4.b.1 and table 8.4.b.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Nonce IEI | | | | | | | | octet 1 |
| Nonce contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 17 |

Figure 8.4.b.1: Nonce information element

Table 8.4.b.1: Nonce information element

|  |
| --- |
| Nonce contents (octet 2 to 17)  This field contains the 128-bit nonce value. |

### 8.4.c UE security capabilities

The UE security capabilities information element is used to indicate which security algorithms are supported by the UE.

The UE security capabilities is a type 4 information element with a minimum length of 4 octets and a maximum length of 10 octets.

The UE security capabilities information element is coded as shown in figure 8.4.c.1 and table 8.4.c.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE security capabilities IEI | | | | | | | | octet 1 |
| Length of UE security capabilities contents | | | | | | | | octet 2 |
| 5G-EA0 | 128-  5G-EA1 | 128-  5G-EA2 | 128-  5G-EA3 | 5G-EA4 | 5G-EA5 | 5G-EA6 | 5G-EA7 | octet 3 |
| 5G-IA0 | 128-  5G-IA1 | 128-  5G-IA2 | 128-  5G-IA3 | 5G-IA4 | 5G-IA5 | 5G-IA6 | 5G-IA7 | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| Spare | | | | | | | | octet 5\* -10\* |

Figure 8.4.c.1: UE security capabilities information element

Table 8.4.c.1: UE security capabilities information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5GS encryption algorithms supported (octet 3) | | | | | |
|  | | | | | |
| 5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA0 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA0 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA1 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA1 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA2 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA2 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA3 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA3 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA4 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA4 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA5 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA5 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA6 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA6 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1) | | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA7 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA7 supported |
|  | | | | | |
| 5GS integrity algorithms supported (octet 4) | | | | | |
|  | | | | | |
| 5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA0 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA0 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA1 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA1 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA2 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA2 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA3 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA3 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA4 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA4 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA5 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA5 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA6supported (octet 4, bit 2) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA6 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA6 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1) | | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA7 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA7 supported |
|  | | | | | |

### 8.4.d UE PC5 unicast signalling security policy

The purpose of the UE PC5 unicast signalling security policy information element is to indicate the UE’s configuration for integrity protection and ciphering of PC5 signalling messages.

The UE PC5 unicast signalling security policy is a type 3 information element with a length of 2 octets.

The UE PC5 unicast signalling security policy information element is coded as shown in figure 8.4.d.1.1 and table 8.4.d.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE PC5 unicast signalling security policy IEI | | | | | | | | octet 1 |
| 0  spare | Signalling ciphering policy | | | 0  spare | Signalling integrity protection policy | | | octet 2 |

**Figure** **8.4.d.1: UE PC5 unicast signalling security policy information element**

**Table** **8.4.d.1: UE PC5 unicast signalling security policy information element**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signalling integrity protection policy (octet 2, bit 1 to 3) | | | | |
| Bits | | | | |
| **3** | **2** | **1** |  |  |
| 0 | 0 | 0 |  | Signalling integrity protection not needed |
| 0 | 0 | 1 |  | Signalling integrity protection preferred |
| 0 | 1 | 0 |  | Signalling integrity protection required |
| 0 | 1 | 1 |  |  |
| to Spare | | | | |
| 1 | 1 | 0 |  |  |
| 1 | 1 | 1 |  | Reserved |
|  | | | | |
| If the UE receives a signalling integrity protection policy value that the UE does not understand, the UE shall interpret the value as 010 "Signalling integrity protection required".  Signaling ciphering policy (octet 2, bit 5 to 7) | | | | |
| Bits | | | | |
| **7** | **6** | **5** |  |  |
| 0 | 0 | 0 |  | Signalling ciphering not needed |
| 0 | 0 | 1 |  | Signalling ciphering preferred |
| 0 | 1 | 0 |  | Signalling ciphering required |
| 0 | 1 | 1 |  |  |
| to Spare | | | | |
| 1 | 1 | 0 |  |  |
| 1 | 1 | 1 |  | Reserved |
|  | | | | |
| If the UE receives a signalling ciphering policy value that the UE does not understand, the UE shall interpret the value as 010 "Signalling ciphering required".  Bit 4 and 8 of octet 2 are spare and shall be coded as zero. | | | | |
|  | | | | |

### 8.4.e MSBs of KNRP-sess ID

The purpose of the MSBs of KNRP-sess ID information element is to carry the 8 most significant bits of the KNRP-sess ID.

The MSBs of KNRP-sess ID information element is a type 3 information element with a length of 2 octets.

The MSBs of KNRP-sess ID information element is coded as shown in figure 8.4.e.1 and table 8.4.e.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSBs of KNRP-sess ID IEI | | | | | | | | octet 1 |
| MSBs of KNRP-sess ID contents | | | | | | | | octet 2 |

Figure 8.4.e.1: MSBs of KNRP-sess ID information element

Table 8.4.e.1: MSBs of KNRP-sess ID information element

|  |
| --- |
| MSBs of KNRP-sess ID contents (octet 2)  This field contains the 8 most significant bits of KNRP-sess ID. |

### 8.4.f KNRP ID

The purpose of the KNRP ID information element is to carry the identity of the KNRP held by a UE.

The KNRP ID is a type 3 information element with a length of 5 octets.

The KNRP ID information element is coded as shown in figure 8.4.f.1 and table 8.4.f.1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| KNRP ID IEI | | | | | | | | octet 1 |
| KNRP ID contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 5 |

Figure 8.4.f.1: KNRP ID information element

Table 8.4.f.1: KNRP ID information element

|  |
| --- |
| KNRP ID contents (octet 2 to 5)  This field contains the 32-bit identifier of a KNRP. |

### 8.4.g Selected security algorithms

The purpose of the Selected security algorithms information element is to indicate the algorithms to be used for ciphering and integrity protection.

The Selected security algorithms is a type 3 information element with a length of 2 octets.

The Selected security algorithms information element is coded as shown in figure 8.4.g.1.1 and table 8.4.g.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Selected security algorithms IEI | | | | | | | | octet 1 |
| 0  spare | Type of ciphering algorithm | | | 0  spare | Type of integrity protection algorithm | | | octet 2 |

**Figure** **8.4.g.1: Selected security algorithms information element**

**Table** **8.4.g.1: Selected security algorithms information element**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of integrity protection algorithm (octet 2, bit 1 to 3) | | | | |
| Bits | | | | |
| **3** | **2** | **1** |  |  |
| 0 | 0 | 0 |  | 5GS integrity algorithm 5G-IA0 (null integrity protection algorithm) |
| 0 | 0 | 1 |  | 5GS integrity algorithm 128-5G-IA1 |
| 0 | 1 | 0 |  | 5GS integrity algorithm 128-5G-IA2 |
| 0 | 1 | 1 |  | 5GS integrity algorithm 128-5G-IA3 |
| 1 | 0 | 0 |  | 5GS integrity algorithm 5G-IA4 |
| 1 | 0 | 1 |  | 5GS integrity algorithm 5G-IA5 |
| 1 | 1 | 0 |  | 5GS integrity algorithm 5G-IA6 |
| 1 | 1 | 1 |  | 5GS integrity algorithm 5G-IA7 |
|  | | | | |
| Type of ciphering algorithm (octet 2, bit 5 to 7) | | | | |
| Bits | | | | |
| **7** | **6** | **5** |  |  |
| 0 | 0 | 0 |  | 5GS encryption algorithm 5G-EA0 (null ciphering algorithm) |
| 0 | 0 | 1 |  | 5GS encryption algorithm 128-5G-EA1 |
| 0 | 1 | 0 |  | 5GS encryption algorithm 128-5G-EA2 |
| 0 | 1 | 1 |  | 5GS encryption algorithm 128-5G-EA3 |
| 1 | 0 | 0 |  | 5GS encryption algorithm 5G-EA4 |
| 1 | 0 | 1 |  | 5GS encryption algorithm 5G-EA5 |
| 1 | 1 | 0 |  | 5GS encryption algorithm 5G-EA6 |
| 1 | 1 | 1 |  | 5GS encryption algorithm 5G-EA7 |
|  | | | | |
| Bit 4 and 8 of octet 2 are spare and shall be coded as zero. | | | | |
|  | | | | |

### 8.4.h LSBs of KNRP-sess ID

The purpose of the LSBs of KNRP-sess ID information element is to carry the 8 least significant bits of the KNRP-sess ID.

The LSBs of KNRP-sess ID is a type 3 information element with a length of 2 octets.

The LSBs of KNRP-sess ID information element is coded as shown in figure 8.4.h.1 and table 8.4.h.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LSBs of KNRP-sess ID | | | | | | | | octet 1 |
| LSBs of KNRP-sess ID contents | | | | | | | | octet 2 |

Figure 8.4.h.1: LSBs of KNRP-sess ID information element

Table 8.4.h.1: LSBs of KNRP-sess ID information element

|  |
| --- |
| LSBs of KNRP-sess ID contents (octet 2)  This field contains the 8 least significant bits of KNRP-sess ID. |

### 8.4.i MSBs of KNRP ID

The purpose of the MSBs of KNRP ID information element is to carry the 16 most significant bits of the KNRP ID.

The MSBs of KNRP ID is a type 3 information element with a length of 3 octets.

The MSBs of KNRP ID information element is coded as shown in figure 8.4.i.1 and table 8.4.i.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSBs of KNRP ID IEI | | | | | | | | octet 1 |
| MSBs of KNRP ID contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |

Figure 8.4.i.1: MSBs of KNRP ID information element

Table 8.4.i.1: MSBs of KNRP ID information element

|  |
| --- |
| MSBs of KNRP ID contents (octet 2 to 3)  This field contains the 16 most significant bits of KNRP ID. |

### 8.4.j LSBs of KNRP ID

The purpose of the LSBs of KNRP ID information element is to carry the 16 least significant bits of the KNRP ID.

The LSBs of KNRP ID is a type 3 information element with a length of 3 octets.

The LSBs of KNRP ID information element is coded as shown in figure 8.4.j.1 and table 8.4.j.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LSBs of KNRP ID IEI | | | | | | | | octet 1 |
| LSBs of KNRP ID contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |

Figure 8.4.j.1: LSBs of KNRP ID information element

Table 8.4.j.1: LSBs of KNRP ID information element

|  |
| --- |
| LSBs of KNRP ID contents (octet 2 to 3)  This field contains the 16 least significant bits of KNRP ID. |

\*\*\* Next change \*\*\*

## 10.3 Timers of PC5 unicast link management procedures

Table 10.3.1: PC5 unicast link management timers

| TIMER NUM. | TIMER VALUE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- |
| T5000 |  | Upon sending a DIRECT LINK ESTABLISHMENT REQUEST message | Upon receiving a DIRECT LINK ESTABLISHMENT ACCEPT or DIRECT LINK ESTABLISHMENT REJECT message from the target UE | Retransmission of DIRECT LINK ESTABLISHMENT REQUEST message |
| T5001 |  | Upon sending a DIRECT LINK MODIFICATION REQUEST message | Upon receiving a DIRECT LINK MODIFICATION ACCEPT or DIRECT LINK MODIFICATION REJECT or DIRECT LINK RELEASE REQUEST message from the target UE | Retransmission of DIRECT LINK MODIFICATION REQUEST message |
| T5002 |  | Upon sending a DIRECT LINK RELEASE REQUEST message | Upon receiving a DIRECT LINK RELEASE ACCEPT message from the target UE | Retransmission of DIRECT LINK RELEASE REQUEST message |
| T5003 |  | Upon receiving a PC5 signalling message or PC5 user plane data | Upon PC5 unicast link release or upon initiating the PC5 unicast link keep-alive procedure | Initiate the PC5 unicast link keep-alive procedure |
| T5004 |  | Upon sending a DIRECT LINK KEEPALIVE REQUEST message | Upon receiving a PC5 signalling message or PC5 user plane data | Retransmission of the DIRECT LINK KEEPALIVE REQUEST message |
| T5005 |  | Upon receiving a Maximum inactivity period in a DIRECT LINK KEEPALIVE REQUEST message, receiving a PC5 signalling message or receiving PC5 user plane data | Upon receiving a PC5 signalling message or PC5 user plane data | Either initiate the PC5 unicast link keep-alive procedure or the PC5 unicast link release procedure |
| T5aaa |  | Upon sending a DIRECT LINK AUTHENTICATION REQUEST message | Upon receiving a DIRECT LINK AUTHENTICATION RESPONSE or DIRECT LINK AUTHENTICATION REJECT message from the target UE | Retransmission of DIRECT LINK AUTHENTICATION REQUEST message |
| T5bbb |  | Upon sending a DIRECT LINK SECURITY MODE COMMAND message | Upon receiving a DIRECT LINK SECURITY MODE COMPLETE or DIRECT LINK SECURITY MODE REJECT message from the target UE | Retransmission of DIRECT LINK SECURITY MODE COMMAND message |

\*\*\* End of changes \*\*\*