ETSI TS 124 587 V16.2.1 (2020-10)

5G;
Vehicle-to-Everything (V2X) services in 5G System (5GS);
Stage 3
(3GPP TS 24.587 version 16.2.1 Release 16)

Reference
RTS/TSGC-0124587vg21

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, certain modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

NOTE 1: The constructions “shall” and “shall not” are confined to the context of normative provisions, and do not appear in Technical Reports.

NOTE 2: The constructions “must” and “must not” are not used as substitutes for “shall” and “shall not”. Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

Should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

NOTE 3: The construction “may not” is ambiguous and is not used in normative elements. The unambiguous constructions “might not” or “shall not” are used instead, depending upon the meaning intended.

Can indicates that something is possible

cannot indicates that something is impossible

NOTE 4: The constructions “can” and “cannot” shall not to be used as substitutes for “may” and “need not”.

Will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

NOTE 5: The constructions “is” and “is not” do not indicate requirements.

1 Scope

The present document specifies the protocols for vehicle-to-everything (V2X) services network as specified in 3GPP TS 23.287 [3] for:

a) V2X communication among the UEs over the PC5 interface; and

b) V2X communication between the UE and the V2X application server over the Uu interface.

This specification also covers interworking with EPS for V2X services in 5GS.

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

[19] IETF RFC 1035: "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION".

[20] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[21] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[22] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[23] ISO/IEC 10118-3:2018: "IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[24] CCSA YD/T 3707-2020: "Technical requirements of network layer of LTE-based vehicular communication".

[25] IETF RFC 793: "Transmission Control Protocol."

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, a PQFI value and a set of PC5 QoS parameters.

PC5 QoS rule: A rule which includes a PC5 QoS rule identifier, a PQFI 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

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

UE local configuration

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] , 3GPP TS 24.501 [6] 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] and 3GPP TS 24.501 [6].

E-UTRA Evolved Universal Terrestrial Radio Access

FQDN	Fully Qualified Domain Name
LSB	Least Significant 8 Bits
MSB	Most Significant 8 Bits
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

4 General description

The present specification defines means for transport of V2X messages in 5GS and interworking to EPS. V2X messages are generated and consumed by upper layers of the UE and the V2X application server. V2X messages can contain IP data or non-IP data.

The V2X messages can be transported using:

a) V2X communication over PC5; and

b) V2X communication over Uu.

For case a above:

1) V2X communication over PC5 enables transfer of V2X messages among UEs;

2) both IP based and non-IP based V2X messages are supported over PC5; and

3) for V2X messages containing IP data, only IPv6 is used. IPv4 is not supported in this release of the specification.

For case b above:

1) V2X communication over Uu enables transfer of V2X messages between a UE and a V2X application server;

2) both IP based and non-IP based V2X messages are supported over Uu;

3) V2X messages are carried over Uu in payload of either a UDP/IP packet or TCP/IP packet towards a V2X application server address;

NOTE: Further details about the use of UDP or TCP as a transport layer protocol are described in 3GPP TS 23.287 [3] clause 5.2.3.1.

4) V2X messages carried over Uu are sent or received over unicast only in this release of the specification; and

5) V2X messages are carried over Uu using user data via user plane.

5 Provisioning of parameters for V2X configuration

5.1 General

V2X communication is configured by the use of V2X configuration parameters and their related procedures which allow configuration of necessary V2X configuration parameters.

5.2 Configuration and precedence of V2X configuration parameters

5.2.1 General

UE's usage of V2X communication is controlled by V2X communication parameters.

The V2X communication parameters consist of the configuration parameters for V2X communication over PC5 and the configuration parameters for V2X communication over Uu.

5.2.2 Precedence of V2X configuration parameters

The V2X configuration parameters can be:

a) pre-configured in the ME;

b) configured in the USIM;

c) provided as a V2XP using the UE policy delivery service as specified in 3GPP TS 24.501 [6] annex D;

d) provided by a V2X application server via V1 reference point; or

e) a combination of case d and either a, b, c or d above.

The UE shall use the V2X configuration parameters in the following order of decreasing precedence:

a) the V2X configuration parameters provided as a V2XP using the UE policy delivery service as specified in annex D of 3GPP TS 24.501 [6];

b) the V2X configuration parameters provided by a V2X application server via V1 reference point;

c) the V2X configuration parameters configured in the USIM; and

d) the V2X configuration parameters pre-configured in the ME.

5.2.3 Configuration parameters for V2X communication over PC5

The configuration parameters for V2X communication over PC5 consist of:

a) a validity timer for the validity of the configuration parameters for V2X communication over PC5;

b) a list of PLMNs and RATs in which the UE is authorized to use V2X communication over PC5 when the UE is served by E-UTRA or served by NR. Each entry of the list contains a PLMN ID and RATs in which the UE is authorized to use V2X communication over PC5;

c) an indication of whether the UE is authorized to use V2X communication over PC5 when the UE is not served by E-UTRA and not served by NR;

d) list of RATs in which the UE is authorized to use V2X communication over PC5 and the radio parameters of the RAT for V2X communication over PC5 applicable per geographical area with an indication of whether these radio parameters of the RAT are "operator managed" or "non-operator managed" when the UE is not served by E-UTRA and not served by NR;

e) void

f) optionally, a list of V2X service identifier to a PC5 RAT and Tx profiles mapping rules. Each mapping rule contains one or more V2X service identifiers, a PC5 RAT and Tx profile s corresponding to the PC5 RAT (i.e. either the Tx profiles for E-UTRA-PC5 or the Tx profiles for NR-PC5);

g) configuration parameters for privacy support, consisting of:

   1) a list of V2X services requiring privacy. Each entry of the list contains one or more V2X service identifiers and one or more geographical areas where the privacy is required; and

2) a privacy timer value as specified in 3GPP TS 24.588 [7] clause 5.3;

h) configuration parameters for a V2X communication over PC5 in E-UTRA-PC5, consisting of:

1) a list of V2X service identifier to destination layer-2 ID mapping rules. Each mapping rule contains one or more V2X service identifiers and the destination layer-2 ID;

2) optionally, a default destination layer-2 ID;

3) a list of PPPP to PDB mapping rules. Each mapping rule contains a ProSe Per-Packet Priority (PPPP) and a Packet Delay Budget (PDB);

4) optionally, list of V2X service identifier to V2X E-UTRA frequency mapping rules. Each mapping rule contains one or more V2X service identifiers and the V2X E-UTRA frequencies with associated geographical areas; and

5) optionally, a list of the V2X services authorized for ProSe Per-Packet Reliability (PPPR). Each entry of the list contains one or more V2X service identifiers and a ProSe Per-Packet Reliability (PPPR) value; and

i) configuration parameters for a V2X communication over PC5 in NR-PC5, consisting of:

1) optionally, a list of V2X service identifier to V2X NR frequency mapping rules. Each mapping rule contains one or more V2X service identifiers and the V2X NR frequencies with associated geographical areas;

2) a list of V2X service identifier to destination layer-2 ID for broadcast mapping rules. Each mapping rule contains one or more V2X service identifiers and the destination layer-2 ID for broadcast;

3) optionally, a default destination layer-2 ID for broadcast;

4) a list of V2X service identifier to destination layer-2 ID for groupcast mapping rules. Each mapping rule contains one or more V2X service identifiers and the destination layer-2 ID for groupcast;

5) a list of V2X service identifier to default destination layer-2 ID for unicast initial signaling mapping rules. Each mapping rule contains one or more V2X service identifiers and the default destination layer-2 ID for initial signalling to establish unicast connection;

6) a list of V2X service identifier to PC5 QoS parameters mapping rules. The PC5 QoS parameters are specified in clause 5.4.2 of 3GPP TS 23.287 [3];

7) an AS configuration, including a list of SLRB mapping rules applicable when the UE is not served by E-UTRA and is not served by NR. Each SLRB mapping rule contains a PC5 QoS profile and an SLRB. The PC5 QoS profile contains the following parameters:

i) the PC5 QoS profile contains a PQI;

ii) if the PQI of the PC5 QoS profile identifies a GBR QoS, the PC5 QoS profile contains a PC5 flow bit rates consisting of a guaranteed flow bit rate (GFBR) and a maximum flow bit rate (MFBR);

iii) if the PQI of the PC5 QoS profile identifies a non-GBR QoS, the PC5 QoS profile contains the PC5 link aggregated bit rate consisting of a per link aggregate maximum bit rate (PC5 LINK-AMBR);

NOTE: PC5 link aggregated bit rate is only used for unicast mode communications over PC5.

iv) the PC5 QoS profile contains a range, which is only used for groupcast mode communications over PC5; and

v) the PC5 QoS profile can contain the priority level, the averaging window, and the maximum data burst volume. If one or more of the priority level, the averaging window or the maximum data burst volume are not contained in the PC5 QoS profile, their default values apply;

8) a list of NR-PC5 unicast security policies. Each entry in the list contains an NR-PC5 unicast security policy composed of:

i) one or more V2X service identifiers;

ii) the signalling integrity protection policy for the V2X service identifier(s);

iii) the signalling ciphering policy for the V2X service identifier(s);

iv) the user plane integrity protection policy for the V2X service identifier(s);

v) the user plane ciphering policy for the V2X service identifier(s); and

vi) one or more geographical areas where the NR-PC5 unicast security policy applies; and

8) a list of V2X service identifier to default mode of communication mapping rules. Each mapping rule contains one or more V2X service identifiers and the default mode of communication (one of unicast, groupcast or broadcast).

5.2.4 Configuration parameters for V2X communication over Uu

The configuration parameters for V2X communication over Uu consist of:

a) a validity timer for the validity of the configuration parameters for V2X communication over Uu to 5GCN;

b) optionally, a list of V2X service identifier to PDU session parameters mapping rules. Each mapping rule contains one or more V2X service identifiers of a the V2X service and one or more parameters for establishment of a PDU session for V2X communication over Uu for the V2X services:

1) one of the "IPv4", "IPv6", "IPv4v6" or "Unstructured" PDU session types;

2) an SSC mode;

3) a list of zero or more S-NSSAIs;

4) a list of zero or more DNNs; and

5) one of the UDP or TCP transport layer protocol if the PDU session type is "IPv4", "IPv6" or "IPv4v6"; and

c) a list of PLMNs in which the UE is configured to use V2X communication over Uu. For each PLMN, the list contains:

1) for transfer of a V2X message of a V2X service identified by a V2X service identifier:

i) a list of V2X service identifier to V2X application server address mapping rules, applicable when the UE is registered to the PLMN. Each mapping rule contains:

A) one or more V2X service identifiers;

B) a V2X application server address for unicast consisting of:

- an FQDN, or an IP address; and

- a UDP port for uplink transport, a UDP port for downlink transport, a TCP port for bidirectional transport or any combination of them; and

C) optionally a geographical area; and

ii) optionally, per type of data (IP and non-IP) and V2X message family (in case of non-IP) and optionally a geographical area, one or more default V2X application server addresses for the unicast V2X communication over Uu applicable when the UE is registered to the PLMN. Each V2X application server address consists of:

i) an FQDN, or an IP address; and

ii) a UDP port for uplink transport, a UDP port for downlink transport, a TCP port for bidirectional transport or any combination of them; and

2) for transfer of a V2X message of a V2X service not identified by a V2X service identifier:

i) a list of the V2X application servers per optional geographical area where usage of those V2X application servers applies, applicable when the UE is registered to the PLMN. Each entry of the list contains:

A) a V2X application server address consisting of an FQDN, or an IP address; and

B) optionally, a geographical area.

5.3 Procedures

5.3.1 General

The procedure for provisioning of parameters for V2X configuration allows the UE to obtain information necessary for V2X communication.

5.3.2 UE-requested V2X policy provisioning procedure

5.3.2.1 General

The UE-requested V2X policy provisioning procedure enables the UE to request V2X policy from the PCF in the following cases:

a) if the validity timer for a V2X policy expires; or

b) if there are no valid configuration parameters, e.g., for the current area, or due to abnormal situation.

The UE shall follow the principles of PTI handling for UE policy delivery service procedures defined in 3GPP TS 24.501 [6] clause D.1.2.

5.3.2.2 UE-requested V2X policy provisioning procedure initiation

In order to initiate the UE-requested V2X policy provisioning procedure, the UE shall create a UE POLICY PROVISIONING REQUEST message (see example in figure 5.3.2.2.1). The UE:

a) shall allocate a PTI value currently not used and set the PTI IE to the allocated PTI value;

b) shall include the Requested UE policies IE indicating whether the UE policies for V2X communication over PC5, the UE policies for V2X communication over Uu or both are requested;

c) shall transport the UE POLICY PROVISIONING REQUEST message using the NAS transport procedure as specified in 3GPP TS 24.501 [6] clause 5.4.5; and

d) shall start timer T5010.

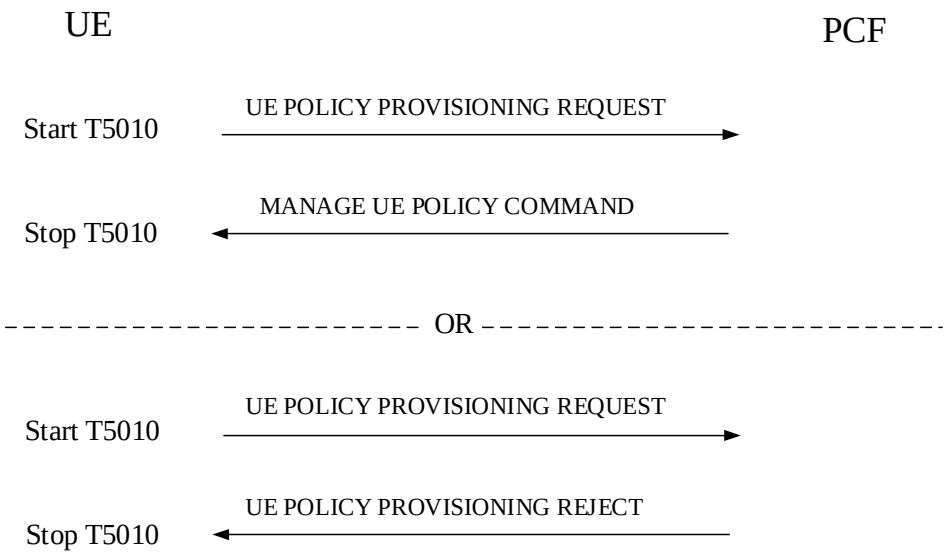

Figure 5.3.2.2.1: UE-requested V2X policy provisioning procedure

5.3.2.3 UE-requested V2X policy provisioning procedure accepted by the network

Upon receipt of and accepting the UE POLICY PROVISIONING REQUEST message, the PCF shall create a MANAGE UE POLICY COMMAND message and shall behave as described in clause D.2.1 of 3GPP TS 24.501 [6].

Upon receipt of the MANAGE UE POLICY COMMAND message with the same PTI as included in the UE POLICY PROVISIONING REQUEST message, the UE shall stop timer T5010 and handles the MANAGE UE POLICY COMMAND message as specified in clause D.2.1 of 3GPP TS 24.501 [6].

5.3.2.4 UE-requested V2X policy provisioning procedure not accepted by the network

Upon receipt and rejecting of the UE POLICY PROVISIONING REQUEST message, the PCF shall create a UE POLICY PROVISIONING REJECT message.

The PCF shall set the UPDS cause IE of the UE POLICY PROVISIONING REJECT message to indicate reason for rejecting the UE-requested V2X policy provisioning procedure.

The UPDS cause IE typically indicates one of the following UPDS cause values:

#31 request rejected, unspecified;

#32 service option not supported;

#34 service option temporarily out of order;

#35 PTI already in use; or

#95 – 111 protocol errors.

The PCF shall transport the UE POLICY PROVISIONING REJECT message to the UE via the AMF using the procedure specified in 3GPP TS 23.502 [4].

Upon receipt of the UE POLICY PROVISIONING REJECT message, the UE shall stop timer T5010.

5.3.2.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Indication from the lower layer of transmission failure of the UE POLICY PROVISIONING REJECT message.

   After receiving an indication from lower layer that the UE POLICY PROVISIONING REJECT message has not been successfully acknowledged (e.g. TCP ACK is not received), the PCF shall abort the procedure.

5.3.2.6 Abnormal cases on the UE

The following abnormal cases can be identified:

a) Tx expired.

   The UE shall, on the first expiry of the timer T5010, retransmit the UE POLICY PROVISIONING REQUEST message and shall reset and start timer T5010. This retransmission is repeated four times, i.e. on the fifth expiry of timer T5010, the UE shall abort the procedure and release the allocated PTI.

6 V2X communication

6.1 V2X communication over PC5

6.1.1 General

This clause describes the procedures at the UE, and between UEs, for V2X communication over PC5.

The UE shall support requirements for securing V2X communication over PC5.

Both IP based and non-IP based V2X communication over PC5 are supported. For IP based V2X communication, only IPv6 is used. IPv4 is not supported in this release of the present document.

V2X communication over NR-PC5 supports broadcast mode, groupcast mode, and unicast mode. If upper layer of the UE indicates the mode of communication, the UE shall set the mode of communication based on the request of the upper layer. Otherwise, the UE shall set the mode of communication based on the mapping rules between the V2X service identifier and the default mode of communication defined in clause 5.2.3.

NOTE: Further details about whether broadcast, unicast or groupcast can be used over PC5 are described in 3GPP TS 23.287 [3] clause 5.2.1.

6.1.2 Unicast mode communication over NR based PC5

6.1.2.1 Overview

This clause describes the PC5 signalling protocol procedures between two UEs for unicast mode of V2X communication. The following PC5 signalling protocol procedures are defined:

a) PC5 unicast link establishment;

b) PC5 unicast link modification;

c) PC5 unicast link release;

d) PC5 unicast link identifier update;

e) PC5 unicast link authentication;

f) PC5 unicast link security mode control;

g) PC5 unicast link keep-alive; and

h) PC5 unicast link re-keying procedure.

6.1.2.2 PC5 unicast link establishment procedure

6.1.2.2.1 General

The PC5 unicast link establishment procedure is used to establish a PC5 unicast link between two UEs. The UE sending the request message is called the "initiating UE" and the other UE is called the "target UE". The maximum number of NR PC5 unicast links established in a UE at a time shall not exceed an implementation-specific maximum number of established NR PC5 unicast links.

NOTE: The recommended maximum number of established NR PC5 unicasts link is 8.

6.1.2.2.2 PC5 unicast link establishment procedure initiation by initiating UE

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 communication mode is unicast mode (e.g. pre-configured as specified in clause 5.2.3 or indicated by upper layers);

c) 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) and is not being used by other existing PC5 unicast links within the initiating UE;

d) 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);

NOTE 1: In the case where different V2X services are mapped to distinct default destination layer-2 IDs, when the initiating UE intends to establish a single unicast link that can be used for more than one V2X service types, the UE can select any of the default destination layer-2 ID for unicast initial signalling.

e) the initiating UE is either authorised for V2X communication over PC5 in NR-PC5 in the serving PLMN, or has a valid authorization for V2X communication over PC5 in NR-PC5 when not served by E-UTRA and not served by NR. The UE considers that it is not served by E-UTRA and not served by NR if the following conditions are met:

   1) not served by NR and not served by E-UTRA for V2X communication over PC5;

   2) in limited service state as specified in 3GPP TS 23.122 [2], if the reason for the UE being in limited service state is one of the following;

      i) the UE is unable to find a suitable cell in the selected PLMN as specified in 3GPP TS 38.304 [9];

      ii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #11 "PLMN not allowed" as specified in 3GPP TS 24.501 [6]; or

      iii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #7 "5GS services not allowed" as specified in 3GPP TS 24.501 [6]; or

   3) in limited service state as specified in 3GPP TS 23.122 [2] for reasons other than i), ii) or iii) above, and located in a geographical area for which the UE is provisioned with "non-operator managed" radio parameters as specified in clause 5.2.3;

f) there is no existing PC5 unicast link for the pair of peer application layer IDs, or there is an existing PC5 unicast link for the pair of peer application layer IDs and:

   1) the network layer protocol of the existing PC5 unicast link is not identical to the network layer protocol required by the upper layer in the initiating UE for this V2X service; or

   2) the security policy (either signalling security policy or user plane security policy) corresponding to the V2X service identifier is not compatible with the security policy of the existing PC5 unicast link; and

g) the number of established PC5 unicast links is less than the implementation-specific maximum number of established NR PC5 unicast links allowed in the UE at a time.

After receiving the service data or request from the upper layers, the initiating UE shall derive the PC5 QoS parameters and assign the PQFI(s) for the PC5 QoS flows(s) to be established as specified in clause 6.1.2.12.

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(s) received from upper layer;

c) shall 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 if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred", and may include the Key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection not needed";

NOTE 2: 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 if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred";

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 the 8 MSBs of $K_{NRP-sess}$ ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred";

h) may include a K_{NRP} ID if the initiating UE has an existing K_{NRP} for the target UE; and

i) shall include its UE PC5 unicast signalling security policy. In the case where the different V2X services are mapped to the different PC5 unicast signalling security policies, when the initiating UE intends to establish a single unicast link that can be used for more than one V2X service, each of the signalling security polices of those V2X services shall be compatible, e.g. "signalling integrity protection not needed" and "signalling integrity protection required" are not compatible.

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 3: In order to ensure successful PC5 unicast link establishment, T5000 should be set to a value larger than the sum of T5006 and T5007.

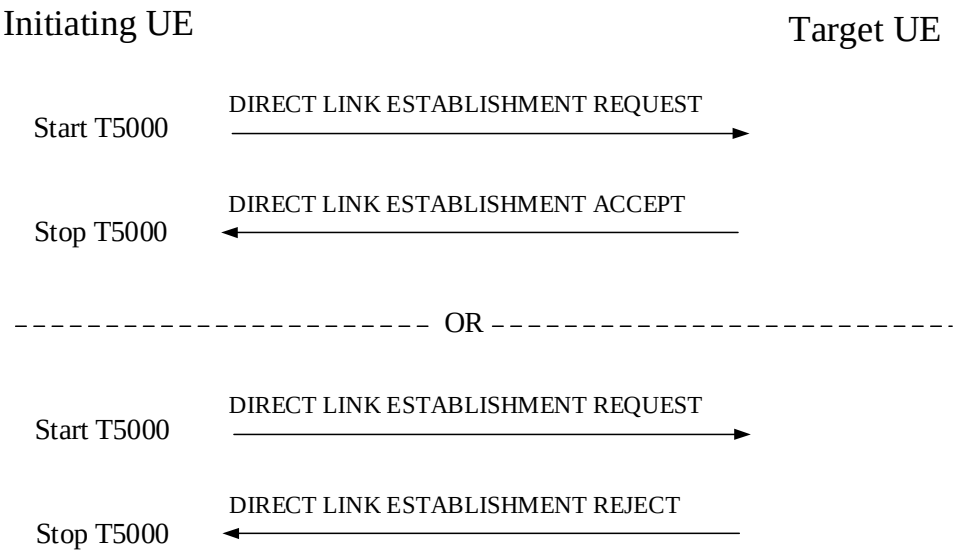

Figure 6.1.2.2.2: PC5 unicast link establishment procedure

6.1.2.2.3 PC5 unicast link establishment procedure accepted by the target UE

Upon receipt of a DIRECT LINK ESTABLISHMENT REQUEST message, if the target UE accepts this request, the target UE shall uniquely assign a PC5 link identifier, create a PC5 unicast link context and assign a layer-2 ID for this PC5 unicast link. Then the target UE shall store this assigned layer-2 ID and the source layer-2 ID used in the transport of this message provided by the lower layers in the 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(s) identified by the V2X service identifier IE in the DIRECT LINK ESTABLISHMENT REQUEST message;

then the target UE shall either:

a) identify an existing K_{NRP} based on the K_{NRP} ID included in the DIRECT LINK ESTABLISHMENT REQUEST message; or

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

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

After an existing K_{NRP} was identified or a new K_{NRP} was derived, the target UE shall initiate a PC5 unicast link security mode control procedure as specified 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 PQFI(s), the corresponding PC5 QoS parameters and the V2X service identifier(s) that the target UE accepts;

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

   1) "IPv6 router" if 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;

d) shall 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; and

e) shall include the configuration of UE PC5 unicast user plane security protection based on the agreed user plane security policy, as specified in 3GPP TS 33.536 [20].

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, NRPIK, NRPEK if applicable, $K_{NRP\text{-}sess}$ ID, and the selected security algorithm as specified in TS 33.536 [20], and shall start timer T5011 if the target UE has the privacy configuration as specified in clause 5.2.3.

After sending the DIRECT LINK ESTABLISHMENT ACCEPT message, the target UE shall provide the following information along with the layer-2 IDs to the lower layer, which enables the lower layer to handle the coming PC5 signalling or traffic data:

a) the PC5 link identifier self-assigned for this PC5 unicast link;

b) PQFI(s) and its corresponding PC5 QoS parameters;

c) an indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link, if applicable; and

e) an indication of activation of the PC5 unicast user plane security protection for the PC5 unicast link, if applicable.

If the target UE accepts the PC5 unicast link establishment request, then the target UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12.

6.1.2.2.4 PC5 unicast link establishment procedure completion by the initiating UE

Upon receipt of the DIRECT LINK ESTABLISHMENT ACCEPT message, the initiating UE shall stop timer T5000, uniquely assign a PC5 link identifier and create a PC5 unicast link context for this PC5 unicast link. Then the target UE shall store the source layer-2 ID and the destination layer-2 ID used in the transport of this message provided by the lower layers in the PC5 unicast link context. From this time onward the initiating UE shall use the established link for V2X communication over PC5 and additional PC5 signalling messages to the target UE.

After receiving the DIRECT LINK ESTABLISHMENT ACCEPT message, the initiating UE shall provide the following information along with the layer-2 IDs to the lower layer, which enables the lower layer to handle the coming PC5 signalling or traffic data:

a) the PC5 link identifier self-assigned for this PC5 unicast link;

b) PQFI(s) and its corresponding PC5 QoS parameters;

c) Indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link, if applicable; and

d) Indication of activation of the PC5 unicast user plane security protection for the PC5 unicast link, if applicable.

The initiating UE shall start timer T5011 if the initiating UE has the privacy configuration as specified in clause 5.2.3.

In addition, the initiating UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12.

6.1.2.2.5 PC5 unicast link establishment procedure not accepted by the target UE

If the DIRECT LINK ESTABLISHMENT REQUEST message cannot be accepted, the target UE shall send a DIRECT LINK ESTABLISHMENT REJECT message. The DIRECT LINK ESTABLISHMENT REJECT message contains a PC5 signalling protocol cause IE set to one of the following cause values:

#1 direct communication to the target UE not allowed;

#3 conflict of layer-2 ID for unicast communication is detected;

#5 lack of resources for PC5 unicast link; or

#111 protocol error, unspecified.

If the target UE is not allowed to accept this request .e.g. based on operator policy or configuration parameters for V2X communication over PC5 as specified in clause 5.2.3, the target UE shall send a DIRECT LINK ESTABLISHMENT REJECT message containing PC5 signalling protocol cause value #1 "direct communication to the target UE not allowed".

For a received DIRECT LINK ESTABLISHMENT REQUEST message from a layer-2 ID (for unicast communication), if the target UE already has an existing link established to the UE known to use this layer-2 ID or is currently processing a DIRECT LINK ESTABLISHMENT REQUEST message from the same layer-2 ID, and with one of following different from the existing link or the link going to be established:

a) the source user info;

b) type of data (e.g. IP or non-IP); or

c) security policy,

the target UE shall send a DIRECT LINK ESTABLISHMENT REJECT message containing PC5 signalling protocol cause value #3 "conflict of layer-2 ID for unicast communication is detected".

NOTE: The type of data (e.g. IP or non-IP) is indicated by the optional IP address configuration IE included in the corresponding DIRECT LINK SECURITY MODE COMPLETE message, i.e the type of data for the requested link is IP type if this IE is included, and the type of data for the requested link is non-IP if this IE is not included.

If the PC5 unicast link establishment fails due to the congestion problems, the implementation-specific maximum number of established NR PC5 unicast links has been reached, or other temporary lower layer problems causing resource constraints, the target UE shall send a DIRECT LINK ESTABLISHMENT REJECT message containing PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link".

For other reasons that causing the failure of link establishment, the target UE shall send a DIRECT LINK ESTABLISHMENT REJECT message containing PC5 signalling protocol cause value #111 "protocol error, unspecified".

Upon receipt of the DIRECT LINK ESTABLISHMENT REJECT message, the initiating UE shall stop timer T5000 and abort the PC5 unicast link establishment procedure. If the PC5 signalling protocol cause value in the DIRECT LINK ESTABLISHMENT REJECT message is #1 "direct communication to the target UE not allowed" or #5 "lack of resources for PC5 unicast link", then the UE shall not attempt to start PC5 unicast link establishment with the same target UE at least for a time period T.

NOTE: The length of time period T is UE implementation specific and can be different for the case when the UE receives PC5 signalling protocol cause value #1 "direct communication to the target UE not allowed" or when the UE receives PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link".

6.1.2.2.6 Abnormal cases

6.1.2.2.6.1 Abnormal cases at the initiating UE

If timer T5000 expires, the initiating UE shall retransmit the DIRECT LINK ESTABLISHMENT REQUEST message and restart timer T5000. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link establishment procedure and may notify the upper layer that the target UE is unreachable.

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

If the need to establish a link no longer exists before the procedure is completed, the initiating UE shall abort the procedure.

6.1.2.2.6.2 Abnormal cases at the target UE

For a received DIRECT LINK ESTABLISHMENT REQUEST message from a source layer-2 ID (for unicast communication), if the target UE already has an existing link established to the UE known to use the same source layer-2 ID, the same source user info, the same type of data (IP or non-IP) and the same security policy, the UE shall process the new request. However, the target UE shall only delete the existing link context after the new link establishment procedure succeeds.

NOTE: The type of data (e.g. IP or non-IP) is indicated by the optional IP address configuration IE included in the corresponding DIRECT LINK SECURITY MODE COMPLETE message, i.e the type of data for the requested link is IP type if this IE is included, and the type of data for the requested link is non-IP if this IE is not included.

6.1.2.3 PC5 unicast link modification procedure

6.1.2.3.1 General

The purpose of the PC5 unicast link modification procedure is to modify the existing PC5 unicast link to:

a) add new PC5 QoS flow(s) to the existing PC5 unicast link;

b) modify existing PC5 QoS flow(s) for updating PC5 QoS parameters of the existing PC5 QoS flow(s);

c) modify existing PC5 QoS flow(s) for associating new V2X service(s) with the existing PC5 QoS flow(s);

d) modify existing PC5 QoS flow(s) for removing the associated V2X service(s) from the existing PC5 QoS flow(s); or

e) remove existing PC5 QoS flow(s) from the existing PC5 unicast link.

In this procedure, the UE sending the DIRECT LINK MODIFICATION REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

6.1.2.3.2 PC5 unicast link modification procedure initiated by initiating UE

The initiating UE shall meet the following pre-conditions before initiating this procedure for adding a new V2X service to the existing PC5 unicast link:

a) there is a PC5 unicast link between the initiating UE and the target UE; and

b) the pair of application layer IDs and the network layer protocol of this PC5 unicast link are identical to those required by the application layer in the initiating UE for this V2X service.

c) the security policy corresponding to the V2X service identifier (e.g. ITS-AID of the new V2X service) is aligned with the security policy of the existing PC5 unicast link.

After receiving the service data or request from the upper layers, the initiating UE shall perform the PC5 QoS flow match as apecified in clause 6.1.2.13. If there is no matched PC5 QoS flow, the initiating UE shall derive the PC5 QoS parameters and assign the PQFI(s) for the PC5 QoS flows(s) to be established as specified in clause 6.1.2.12.

If the PC5 unicast link modification procedure is to add new PC5 QoS flow(s) to the existing PC5 unicast link, the initiating UE shall create a DIRECT LINK MODIFICATION REQUEST message. In this message, initiating UE:

a) shall include the PQFI(s) and the corresponding PC5 QoS parameters, including the V2X service identifier(s); and

b) shall include the link modification operation code set to "add new PC5 QoS flow(s) to the existing PC5 unicast link ".

If the PC5 unicast link modification procedure is to modify the PC5 QoS parameters for existing PC5 QoS flow(s) in the existing PC5 unicast link, the initiating UE shall create a DIRECT LINK MODIFICATION REQUEST message. In this message, the initiating UE:

a) shall include the PQFI(s) and the corresponding PC5 QoS parameters, including the V2X service identifier(s); and

b) shall include the link modification operation code set to "modify PC5 QoS parameters of the existing PC5 QoS flow(s)".

If the PC5 unicast link modification procedure is to associate new V2X service(s) with existing PC5 QoS flow(s), the initiating UE shall create a DIRECT LINK MODIFICATION REQUEST message. In this message, the initiating UE:

a) shall include the PQFI(s) and the corresponding PC5 QoS parameters, including the V2X service identifier(s); and

b) shall include the link modification operation code set to "associate new V2X service(s) with existing PC5 QoS flow(s)".

If the PC5 unicast link modification procedure is to remove the associated V2X service(s) from existing PC5 QoS flow(s), the initiating UE shall create a DIRECT LINK MODIFICATION REQUEST message. In this message, the initiating UE:

a) shall include the PQFI(s) and the corresponding PC5 QoS parameters including the V2X service identifier(s); and

b) shall include the link modification operation code set to "remove V2X service(s) from existing PC5 QoS flow(s)".

If the PC5 unicast link modification procedure is to remove any PC5 QoS flow(s) from the existing PC5 unicast link, the initiating UE shall create a DIRECT LINK MODIFICATION REQUEST message. In this message, the initiating UE:

a) shall include the PQFI(s); and

b) shall include the link modification operation code set to "remove existing PC5 QoS flow(s) from the existing PC5 unicast link".

After the DIRECT LINK MODIFICATION 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, and start timer T5001. The UE shall not send a new DIRECT LINK MODIFICATION REQUEST message to the same target UE while timer T5001 is running.

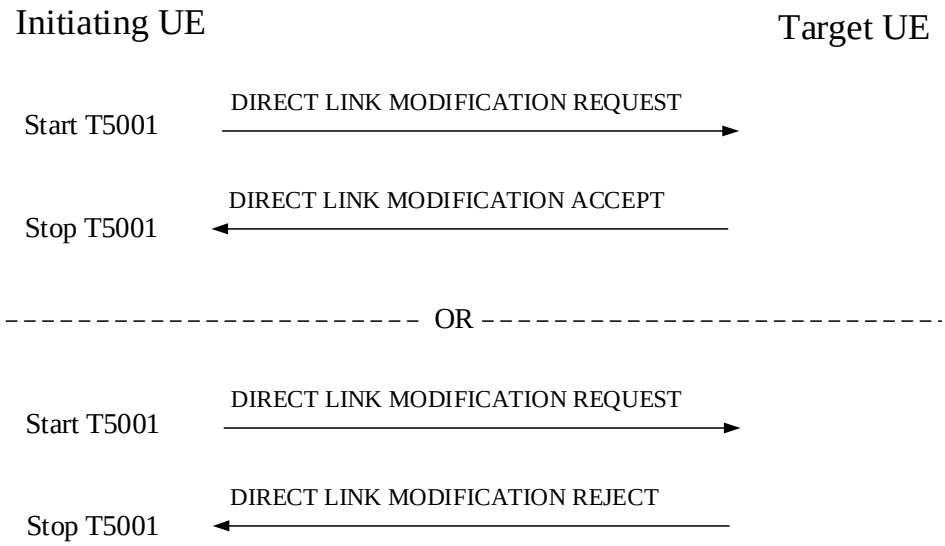

Figure 6.1.2.3.2: PC5 unicast link modification procedure

6.1.2.3.3 PC5 unicast link modification procedure accepted by the target UE

If the DIRECT LINK MODIFICATION REQUEST message is accepted, the target UE shall respond with the DIRECT LINK MODIFICATION ACCEPT message.

If the DIRECT LINK MODIFICATION REQUEST message is to add a new V2X service, add new PC5 QoS flow(s) or modify any existing PC5 QoS flow(s) in the PC5 unicast link, the target UE shall include in the DIRECT LINK MODIFICATION ACCEPT message:

a) the PQFI(s), the corresponding PC5 QoS parameters and the V2X service identifier(s) that the target UE accepts.

If the DIRECT LINK MODIFICATION REQUEST message is to remove an existing V2X service from the PC5 unicast link, the target UE shall delete the V2X service identifier received in the DIRECT LINK MODIFICATION REQUEST message and the corresponding PQFI(s) and PC5 QoS parameters from the profile associated with the PC5 unicast link.

If the DIRECT LINK MODIFICATION REQUEST message is to remove existing PC5 QoS flow(s) from the PC5 unicast link, the target UE shall delete the PQFI(s) and the corresponding PC5 QoS parameters from the profile associated with the PC5 unicast link.

If the DIRECT LINK MODIFICATION REQUEST message is to add a new V2X service, add new PC5 QoS flow(s) or modify any existing PC5 QoS flow(s) in the PC5 unicast link, after sending the DIRECT LINK MODIFICATION ACCEPT message, the target UE shall provide the added or modified PQFI(s) and corresponding PC5 QoS parameters along with PC5 link identifier to the lower layer.

If the DIRECT LINK MODIFICATION REQUEST message is to remove an existing V2X service or to remove the existing PC5 QoS flow(s) from the PC5 unicast link, after sending the DIRECT LINK MODIFICATION ACCEPT message, the target UE shall provide the removed PQFI(s) along with the PC5 link identifier to the lower layer.

If the target UE accepts the PC5 unicast link modification request, then the target UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12 and perform the PC5 QoS flow match over PC5 unicast link as specified in clause 6.1.2.13.

6.1.2.3.4 PC5 unicast link modification procedure completion by the initiating UE

Upon receipt of the DIRECT LINK MODIFICATION ACCEPT message, the initiating UE shall stop timer T5001.

Upon receipt of the DIRECT LINK MODIFICATION ACCEPT message, if the DIRECT LINK MODIFICATION REQUEST message is to add a new V2X service, add new PC5 QoS flow(s) or modify any existing PC5 QoS flow(s) in the PC5 unicast link, the initiating UE shall provide the added or modified PQFI(s) and corresponding PC5 QoS parameters along with PC5 link identifier to the lower layer.

Upon receipt of the DIRECT LINK MODIFICATION ACCEPT message, if the DIRECT LINK MODIFICATION REQUEST message is to remove an existing V2X service or to remove the existing PC5 QoS flow(s) from the PC5 unicast link, the initiating UE shall provide the removed PQFI(s) along with the PC5 link identifier to the lower layer.

In addition, the initiating UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12.

6.1.2.3.5 PC5 unicast link modification procedure not accepted by the target UE

If the PC5 unicast link modification request cannot be accepted, the target UE shall send a DIRECT LINK MODIFICATION REJECT message. The DIRECT LINK MODIFICATION REJECT message contains a PC5 signalling protocol cause IE set to one of the following cause values:

#5 lack of resources for PC5 unicast link;

#11 required service not allowed;

#12 security policy not aligned; or

#111 protocol error, unspecified.

If the target UE is not allowed to accept this request, .e.g. because the V2X service to be added is not allowed per the operator policy or configuration parameters for V2X communication over PC5 as specified in clause 5.2.3, the target UE shall send a DIRECT LINK MODIFICATION REJECT message with PC5 signalling protocol cause value #11 "required service not allowed".

If the PC5 unicast link modification fails due to the congestion problems or other temporary lower layer problems causing resource constraints, the target UE shall send a DIRECT LINK MODIFICATION REJECT message with PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link".

If the link modification operation code is set to "associate new V2X service(s) with existing PC5 QoS flow(s)", and the security policy corresponding to the V2X service identifier(s) (e.g. ITS-AID of the new V2X service) is not aligned with the security policy applied to the existing PC5 unicast link, then the target UE shall send a DIRECT LINK MODIFICATION REJECT message with PC5 signalling protocol cause value #12 "security policy not aligned".

For other reasons causing the failure of link modification, the target UE shall send a DIRECT LINK MODIFICATION REJECT message with PC5 signalling protocol cause value #111 "protocol error, unspecified".

Upon receipt of the DIRECT LINK MODIFICATION REJECT message, the initiating UE shall stop timer T5001 and abort the PC5 unicast link modification procedure. If the PC5 signalling protocol cause value in the DIRECT LINK MODIFICATION REJECT message is #11 "required service not allowed" or #5 "lack of resources for PC5 unicast link", then the initiating UE shall not attempt to start PC5 unicast link modification with the same target UE to add the same V2X service, or to add or modify the same PC5 QoS flow(s) at least for a time period T.

NOTE: The length of time period T is UE implementation specific and can be different for the case when the UE receives PC5 signalling protocol cause value #11 "required service not allowed" or when the UE receives PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link". The length of time period T is not less than 30 minutes.

6.1.2.3.6 Abnormal cases at the initiating UE

The following abnormal cases can be identified:

a) If timer T5001 expires, the initiating UE shall retransmit the DIRECT LINK MODIFICATION REQUEST message and restart timer T5001. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link modification procedure and may notify the upper layer that the target UE is unreachable.

NOTE 1: The maximum number of allowed retransmissions is UE implementation specific.

NOTE 2: After reaching the maximum number of allowed retransmissions, whether the initiating UE releases this PC5 unicast link depends on its implementation.

b) For the same PC5 unicast link, if the initiating UE receives a DIRECT LINK RELEASE message during the initiating UE-requested PC5 unicast link modification procedure, the initiating UE shall abort the PC5 unicast link modification procedure and proceed with the PC5 unicast link release procedure.

c) For the same PC5 unicast link, if the initiating UE receives a DIRECT LINK MODIFICATION REQUEST message during the PC5 unicast link modification procedure, the initiating UE shall abort the PC5 unicast link modification procedure. Following handling is implementation dependent, e.g., the initiating UE waits for an implementation dependent time for initiating a new PC5 unicast link modification procedure, if still needed.

6.1.2.4 PC5 unicast link release procedure

6.1.2.4.1 General

The PC5 unicast link release procedure is used to release a secure PC5 unicast link between two UEs. The link can be released from either end point. The UE sending the DIRECT LINK RELEASE REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

If the UE receives an indication of radio link failure from the lower layer, the UE shall release the PC5 unicast link locally and may delete the K_{NRP} ID associated with this link after an implementation specific time.

6.1.2.4.2 PC5 unicast link release procedure initiation by initiating UE

The initiating UE shall initiate the procedure if a request from upper layers to release a PC5 unicast link with the target UE which uses a known layer-2 ID (for unicast communication) is received and there is an existing PC5 unicast link between these two UEs.

The initiating UE may initiate the procedure if the target UE has been non-responsive, e.g. no response in the PC5 unicast link modification procedure, PC5 unicast link identifier update procedure, PC5 unicast link re-keying procedure or PC5 unicast link keep-alive procedure.

The initiating UE may initiate the procedure to release an established PC5 unicast link if the UE has reached the maximum number of established PC5 unicast links and there is a need to establish a new PC5 unicast link. In this case, which PC5 unicast link is to be released is up to UE implementation.

In order to initiate the PC5 unicast link release procedure, the initiating UE shall create a DIRECT LINK RELEASE REQUEST message with a PC5 signalling protocol cause IE indicating one of the following cause values:

#1 direct communication with the target UE not allowed;

#2 direct communication to the target UE no longer needed;

#4 direct connection is not available anymore;

#5 lack of resources for PC5 unicast link; or

#111 protocol error, unspecified.

The initiating UE shall include the new MSB of K_{NRP} ID in the DIRECT LINK RELEASE REQUEST message.

After the DIRECT LINK RELEASE 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 and the target UE's layer-2 ID, and shall stop T5011 if running. The initiating UE shall release the direct link locally if the release reason is #4 "direct connection is not available anymore". Otherwise, the initiating UE shall start timer T5002.

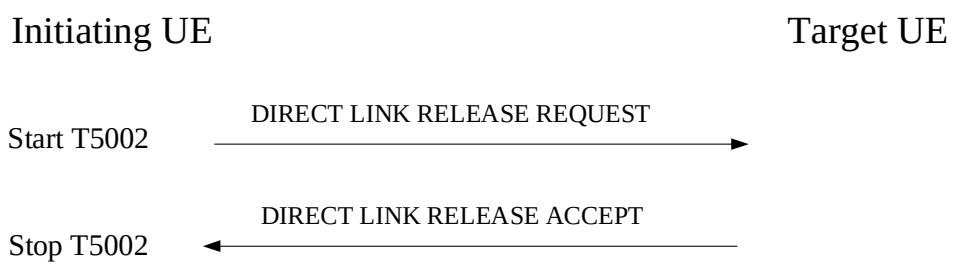

Figure 6.1.2.4.2.1: PC5 unicast link release procedure

6.1.2.4.3 PC5 unicast link release procedure accepted by the target UE

Upon receiving a DIRECT LINK RELEASE REQUEST message, the target UE shall stop all running timers for this PC5 unicast link and abort any other ongoing PC5 signalling protocol procedures on this PC5 unicast link. The target UE shall respond with a DIRECT LINK RELEASE ACCEPT message. The target UE shall include the new LSB of K_{NRP} ID in the DIRECT LINK RELEASE ACCEPT message. After the message is sent, the target UE shall release the PC5 unicast link by performing the following behaviors:

a) inform the lower layer along with the PC5 link identifier that the PC5 unicast link has been released; and

b) delete the PC5 unicast link context of the PC5 unicast link after an implementation specific time.

The target UE shall form the new K_{NRP} ID from the new MSB of K_{NRP} ID received in the DIRECT LINK RELEASE REQUEST message and the new LSB of K_{NRP} ID included in the DIRECT LINK RELEASE ACCEPT message. The target UE shall replace the existing K_{NRP} ID with the new K_{NRP} ID. The target UE may include the new K_{NRP} ID in DIRECT LINK ESTABLISHMENT REQUEST message with the initiating UE as specified in clause 6.1.2.2.2.

6.1.2.4.4 PC5 unicast link release procedure completion by the initiating UE

Upon receipt of the DIRECT LINK RELEASE ACCEPT message, the initiating UE shall stop timer T5002 and shall release the PC5 unicast link by performing the following behaviors:

a) inform the lower layer along with the PC5 link identifier that the PC5 unicast link has been released; and

b) delete the PC5 unicast link context of the PC5 unicast link after an implementation specific time.

The initiating UE shall form the new K_{NRP} ID from the MSB of K_{NRP} ID included in the DIRECT LINK RELEASE REQUEST message and the LSB of K_{NRP} ID received in the DIRECT LINK RELEASE ACCEPT message. The initiating UE shall replace the existing K_{NRP} ID with the new K_{NRP} ID. The initiating UE may include the new K_{NRP} ID in DIRECT LINK ESTABLISHMENT REQUEST message with the target UE as specified in clause 6.1.2.2.2.

6.1.2.4.5 Abnormal cases

6.1.2.4.5.1 Abnormal cases at the initiating UE

If retransmission timer T5002 expires, the initiating UE shall initiate the transmission of the DIRECT LINK RELEASE REQUEST message again and restart timer T5002.

If no response is received from the target UE after reaching the maximum number of allowed retransmissions, the initiating UE shall release the PC5 unicast link locally and delete the K_{NRP} ID associated with this link. From this time onward the initiating UE shall no longer send or receive any messages via this link.

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

6.1.2.5 PC5 unicast link identifier update procedure

6.1.2.5.1 General

The PC5 unicast link identifier update procedure is used to update and exchange the new identifiers (e.g. application layer ID, layer-2 ID, security information and IP address/prefix) between two UEs for a PC5 unicast link before using the new identifiers. The UE sending the DIRECT LINK IDENTIFIER UPDATE REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

6.1.2.5.2 PC5 unicast link identifier update procedure initiation by initiating UE

The initiating UE shall initiate the procedure if:

a) the initiating UE receives a request from upper layers to change the application layer ID and there is an existing PC5 unicast link associated with this application layer ID; or

b) the privacy timer (see clause 5.2.3) of the initiating UE's layer-2 ID expires for an existing PC5 unicast link.

If the PC5 unicast link identifier update procedure is triggered by a change of the initiating UE’s application layer ID, the initiating UE shall stop timer T5011 if running and create a DIRECT LINK IDENTIFIER UPDATE REQUEST message. In this message, the initiating UE

a) shall include the initiating UE’s new application layer ID received from upper layer;

b) shall include the initiating UE’s new layer-2 ID assigned by itself;

c) shall include the new MSB of $K_{NRP\text{-}sess}$ ID; and

d) may include the new IP address/prefix if IP communication is used.

If the PC5 unicast link identifier update procedure is triggered by the expiry of the initiating UE's privacy timer T5011 as specified in clause 5.2.3, the initiating UE shall create a DIRECT LINK IDENTIFIER UPDATE REQUEST message. In this message, the initiating UE

a) shall include the initiating UE's new layer-2 ID assigned by itself;

b) shall include the new MSB of $K_{NRP\text{-}sess}$ ID;

c) may include the initiating UE’s new application layer ID received from upper layer; and

d) may include the new IP address/prefix if IP communication is used.

After the DIRECT LINK IDENTIFIER UPDATE REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's old layer-2 ID and the target UE's layer-2 ID, and start timer T5009. The UE shall not send a new DIRECT LINK IDENTIFIER UPDATE REQUEST message to the same target UE while timer T5009 is running.

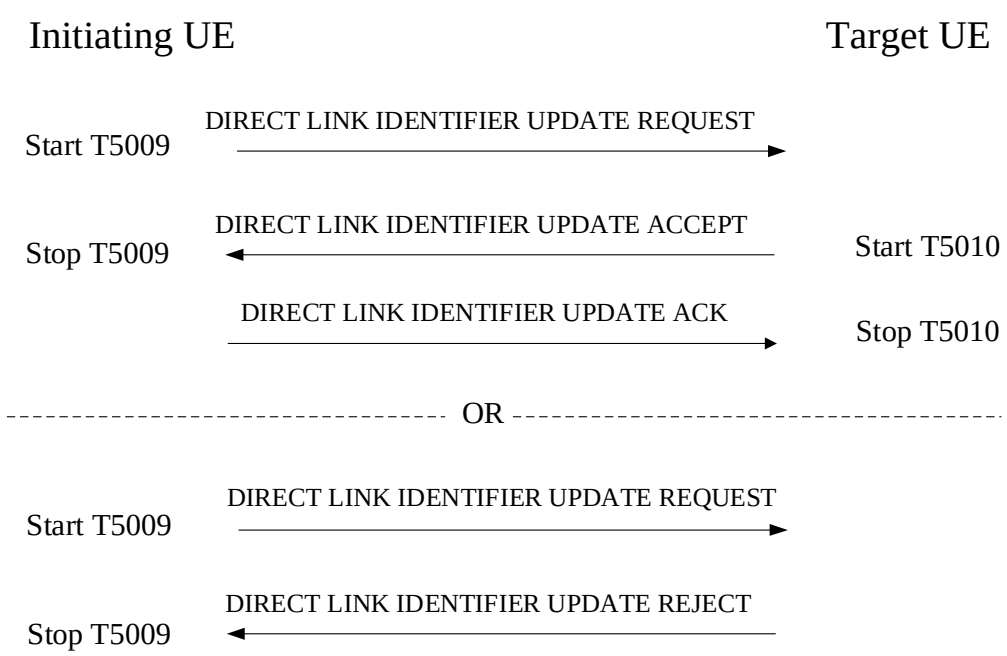

Figure 6.1.2.5.2.1: PC5 unicast link identifier update procedure

6.1.2.5.3 PC5 unicast link identifier update procedure accepted by the target UE

Upon receipt of a DIRECT LINK IDENTIFIER UPDATE REQUEST message, if the target UE determines:

a) the PC5 unicast link associated with this request message is still valid; and

b) the timer T5010 for the PC5 unicast link identified by this request message is not running,

then the target UE accepts this request, stops timer T5011 if running and responds with a DIRECT LINK IDENTIFIER UPDATE ACCEPT message.

The target UE shall create the DIRECT LINK IDENTIFIER UPDATE ACCEPT message. In this message, the target UE:

a) shall include the target UE's new layer-2 ID assigned by itself;

b) shall include the new LSB of $K_{NRP\text{-}sess}$ ID;

c) shall include the initiating UE's new MSB of $K_{NRP\text{-}sess}$ ID;

d) shall include the initiating UE's new layer-2 ID;

e) may include the target UE’s new application layer ID if received from upper layer;

f) may include the initiating UE's new IP address/prefix if IP communication is used;

g) may include the initiating UE's new application layer ID; and

h) may include the target UE's new IP address/prefix if IP communication is used.

After the DIRECT LINK IDENTIFIER UPDATE ACCEPT message is generated, the target UE shall pass this message to the lower layers for transmission along with the initiating UE's old layer-2 ID and the target UE's old layer-2 ID, and start timer T5010. The UE shall not send a new DIRECT LINK IDENTIFIER UPDATE ACCEPT message to the same initiating UE while timer T5010 is running.

Before target UE receives the traffic using the new layer-2 IDs, the target UE shall continue to receive the traffic with the old layer-2 IDs (i.e. initiating UE’s old layer-2 ID and target UE’s old layer-2 ID) from initiating UE.

Before target UE receives the DIRECT LINK IDENTIFIER UPDATE ACK message from initiating UE, the target UE shall keep sending traffic to the initiating UE using the old layer-2 IDs (i.e. initiating UE's old layer-2 ID and target UE's old layer-2 ID).

6.1.2.5.4 PC5 unicast link identifier update procedure acknowledged by the initiating UE

Upon receipt of the DIRECT LINK IDENTIFIER UPDATE ACCEPT message, the initiating UE shall stop timer T5009 and respond with a DIRECT LINK IDENTIFIER UPDATE ACK message. In this message, the initiating UE:

a) shall include the target UE's new layer-2 ID;

b) shall include the target UE's new LSB of $K_{NRP-sess}$ ID;

c) may include the target UE's new application layer ID, if received; and

d) may include the target UE's new IP address/prefix, if received.

After the DIRECT LINK IDENTIFIER UPDATE ACK message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's old layer-2 ID and the target UE's old layer-2 ID and shall start timer T5011 as configured.

Upon sending the DIRECT LINK IDENTIFIER UPDATE ACK message, the initiating UE shall update the associated PC5 unicast link context with the new identifiers and pass the new layer-2 IDs (i.e. initiating UE's new layer-2 ID and target UE's new layer-2 ID if changed) along with the PC5 link identifier down to the lower layer. Then the initiating UE shall use the new layer-2 IDs (i.e. initiating UE's new layer-2 ID and target UE's new layer-2 ID if changed) to transmit the PC5 signalling message and PC5 user plane data.

The initiating UE shall continue to receive traffic with the old layer-2 IDs (i.e. initiating UE's old layer-2 ID and target UE's old layer-2 ID) from the target UE until it receives traffic with the new layer-2 IDs (i.e. initiating UE's new layer-2 ID and target UE's new layer-2 ID if changed) from the target UE.

6.1.2.5.5 PC5 unicast link identifier update procedure completion by the target UE

Upon receipt of the DIRECT LINK IDENTIFIER UPDATE ACK message, the target UE shall update the associated PC5 unicast link context with the new identifiers, pass the new layer-2 IDs (i.e. initiating UE's new layer-2 ID and target UE's new layer-2 ID if changed) down to the lower layer, stop timer T5010 and start timer T5011 as configured. Then the target UE shall use the new layer-2 IDs (i.e. initiating UE's new layer-2 ID and target UE's new layer-2 ID if changed) to transmit the PC5 signalling message and PC5 user plane data.

6.1.2.5.6 PC5 unicast link identifier update procedure not accepted by the target UE

If the DIRECT LINK IDENTIFIER UPDATE REQUEST message cannot be accepted, the target UE shall send a DIRECT LINK IDENTIFIER UPDATE REJECT message. The DIRECT LINK IDENTIFIER UPDATE REJECT message contains a PC5 signalling protocol cause IE set to one of the following cause values:

#3 conflict of layer-2 ID for unicast communication is detected; or

#111 protocol error, unspecified.

For a received DIRECT LINK IDENTIFIER UPDATE REQUEST message from a layer-2 ID (for unicast communication), if the target UE already has an existing link using this layer-2 ID or is currently processing a DIRECT LINK IDENTIFIER UPDATE REQUEST message from the same layer-2 ID, but with user info different from the user info IE included in this new incoming message, the target UE shall send a DIRECT LINK IDENTIFIER UPDATE REJECT message with PC5 signalling protocol cause value #3 "conflict of layer-2 ID for unicast communication is detected".

NOTE: After receiving the DIRECT LINK IDENTIFIER UPDATE REJECT message, whether the initiating UE initiates the PC5 unicast link release procedure or initiates another PC5 unicast link identifier update procedure with a new layer-2 ID depends on UE implementation.

For other reasons causing the failure of link identifier update, the target UE shall send a DIRECT LINK IDENTIFIER UPDATE REJECT message with PC5 signalling protocol cause value #111 "protocol error, unspecified".

Upon receipt of the DIRECT LINK IDENTIFIER UPDATE REJECT message, the initiating UE shall stop timer T5009 and abort this PC5 unicast link identifier update procedure.

6.1.2.5.7 Abnormal cases

6.1.2.5.7.1 Abnormal cases at the initiating UE

The following abnormal cases can be identified:

a) If timer T5009 expires, the initiating UE shall retransmit the DIRECT LINK IDENTIFIER UPDATE REQUEST message and restart timer T5009. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link identifier update procedure and may notify the upper layer that the target UE is unreachable.

NOTE 1: The maximum number of allowed retransmissions is UE implementation specific.

NOTE 2: After reaching the maximum number of allowed retransmissions, whether the initiating UE releases this PC5 unicast link depends on its implementation.

b) For the same PC5 unicast link, if the initiating UE receives a DIRECT LINK IDENTIFIER UPDATE REQUEST message during the PC5 unicast link identifier update procedure, the initiating UE shall abort the PC5 unicast link identifier update procedure. Following handling is implementation dependent, e.g., the initiating UE waits for an implementation dependent time for initiating a new PC5 unicast link identifier update procedure, if still needed.

6.1.2.5.7.2 Abnormal cases at the target UE

The following abnormal cases can be identified:

a) If timer T5010 expires, the target UE shall retransmit the DIRECT LINK IDENTIFIER UPDATE ACCEPT message and restart timer T5010. After reaching the maximum number of allowed retransmissions, the target UE shall abort the PC5 unicast link identifier update procedure and may notify the upper layer that the initiating UE is unreachable.

NOTE 1: The maximum number of allowed retransmissions is UE implementation specific.

NOTE 2: After reaching the maximum number of allowed retransmissions, whether the target UE releases this PC5 unicast link depends on its implementation.

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 K_{NRP} 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 K_{NRP} 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 if signalling integrity protection is activated based on the decision of the initiating UE, 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:

      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 K_{NRP} ID is not included in the DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE does not have an existing K_{NRP} for the K_{NRP} ID included in DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE derives a new K_{NRP}; 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 REKEYING 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 IE.

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 T5006. The UE shall not send a new DIRECT LINK AUTHENTICATION REQUEST message to the same target UE while timer T5006 is running.

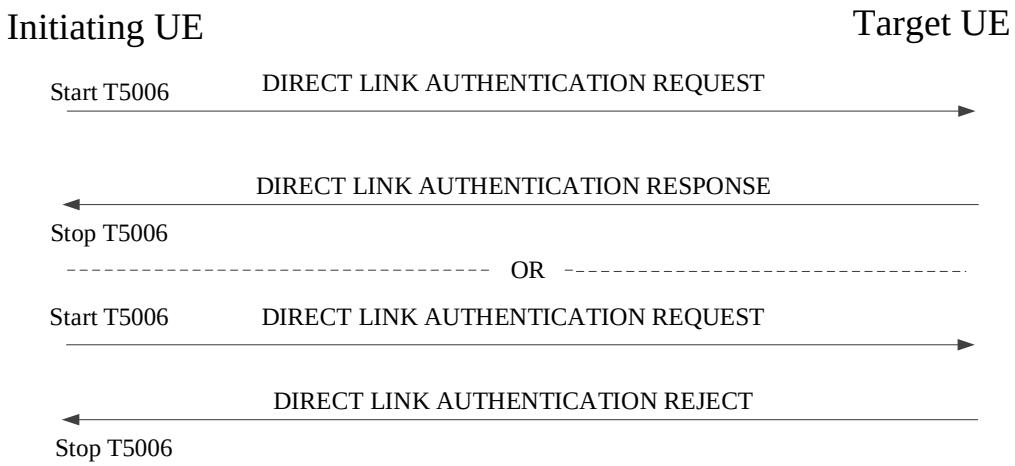

Figure 6.1.2.6.2: PC5 unicast link authentication procedure

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 IE.

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 T5006.

NOTE: When the initiating UE derives the new K_{NRP} during the PC5 unicast link authentication procedure depends on the authentication method in use.

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 T5006 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 T5006 expires.

   The initiating UE shall retransmit the DIRECT LINK AUTHENTICATION REQUEST message and restart timer T5006. 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. Security is not established if the UE PC5 signalling integrity protection is not activated. 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 over this PC5 unicast link between the UEs and the security context can be used to protect all PC5 user plane data exchanged over this PC5 unicast link 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".

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:

      i) has either identified an existing K_{NRP} based on the K_{NRP} ID included in the DIRECT LINK ESTABLISHMENT REQUEST message or derived a new K_{NRP}; or

      ii) has decided not to activate security protection based on its UE PC5 unicast signalling security policy and the target UE's PC5 unicast signalling security policy; 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 K_{NRP}.

If a new K_{NRP} has been derived by the initiating UE, the initiating UE shall generate the 16 MSBs of K_{NRP} ID to ensure that the resultant K_{NRP} 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:

a) 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;

b) shall not select the null ciphering protection algorithm if the ciphering protection algorithm currently in use for the PC5 unicast link is different from the null ciphering protection algorithm;

c) shall select the null integrity protection algorithm if the integrity protection algorithm currently in use is the null integrity protection algorithm; and

d) shall select the null ciphering protection algorithm if the ciphering protection algorithm currently in use is the null ciphering protection algorithm.

Then the initiating UE shall:

a) generate a 128-bit Nonce_2 value;

b) derive $K_{NRP\text{-}sess}$ from K_{NRP}, Nonce_2 and Nonce_1 received in the DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.536 [20];

c) derive the NR PC5 encryption key NRPEK and the NR PC5 integrity key NRPIK from $K_{NRP\text{-}sess}$ and the selected security algorithms as specified in 3GPP TS 33.536 [20], and

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

   1) shall include the key establishment information container IE if a new K_{NRP} has been derived at the initiating UE and the authentication method used to generate K_{NRP} requires sending information to complete the authentication procedure;

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

   2) shall include the MSBs of K_{NRP} ID IE if a new K_{NRP} has been derived at the initiating UE;

3) shall include a Nonce_2 IE set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this PC5 unicast link if the selected integrity protection algorithms is not the null integrity protection algorithm;

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 UE PC5 unicast signalling security policy received from the target UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message; and

7) shall include the 8 LSBs of $K_{NRP-sess}$ ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the selected integrity protection algorithms is not the null integrity protection algorithm.

If the security protection of this PC5 unicast link is activated, the initiating UE shall form the $K_{NRP-sess}$ ID from the 8 MSBs of $K_{NRP-sess}$ ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of $K_{NRP-sess}$ ID included in the DIRECT LINK SECURITY MODE COMMAND message.

If the security protection of this PC5 unicast link is activated, 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 T5007. The UE shall not send a new DIRECT LINK SECURITY MODE COMMAND message to the same target UE while timer T5007 is running.

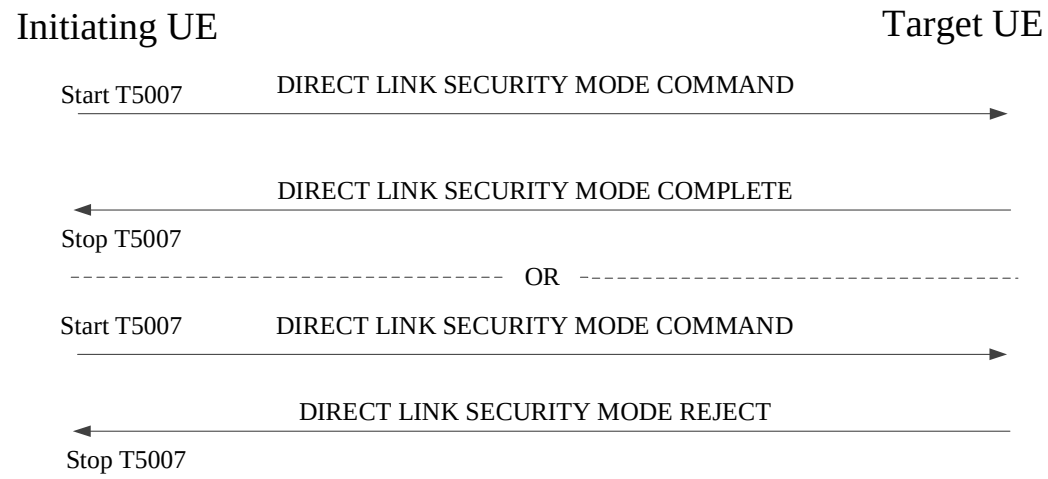

Figure 6.1.2.7.2: PC5 unicast link security mode control procedure

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, the target UE shall first check the selected security algorithms IE included in the DIRECT LINK SECURITY MODE COMMAND message. If "null integrity algorithm" is included in the selected security algorithms IE, the security of this PC5 unicast link is not activated. If "null ciphering algorithm" and an integrity algorithm other than "null integrity algorithm" are included in the selected algorithms IE, the signalling ciphering protection is not activated. If the target UE's PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required", the target UE shall check the selected security algorithms IE in the DIRECT LINK SECURITY MODE COMMAND message does not include the null integrity protection algorithm. If the an integrity algorithm other than "null integrity algorithm" is included in the selected security algorithms IE.If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall:

a) derive $K_{NRP-sess}$ from K_{NRP}, Nonce_1 and Nonce_2 received in the DIRECT LINK SECURITY MODE COMMAND message as specified in 3GPP TS 33.536 [20]; and

b) derive NRPIK from $K_{NRP-sess}$ and the selected integrity algorithm as specified in 3GPP TS 33.536 [20].

If the $K_{NRP-sess}$ is derived and the selected ciphering protection algorithm is not the null integrityciphering protection algorithm, then the target UE shall derive NRPEK from $K_{NRP-sess}$ and the selected ciphering algorithm as specified in 3GPP TS 33.536 [20].

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

a) checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message only include the null integrity protection algorithm if the target UE's PC5 unicast signalling integrity protection policy is set to "signalling integrity protection not needed" or "signalling integrity protection notor preferred"; and

b) checking the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK, if the selected integrity protection algorithm is not the null integrity protection algorithm;

c) 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;

d) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure,

   1) 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; and

   2) checking that the 8 LSBs of $K_{NRP-sess}$ 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; 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 K_{NRP} 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 K_{NRP}, the target UE shall derive K_{NRP} as specified in 3GPP TS 33.536 [20]. The target UE shall choose the 16 LSBs of K_{NRP} ID to ensure that the resultant K_{NRP} ID will be unique in the target UE. The target UE shall form K_{NRP} ID from the received MSBs of K_{NRP} ID and its chosen LSBs of K_{NRP} ID and shall store the complete K_{NRP} ID with K_{NRP}.

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 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];

d) if a new K_{NRP} was derived, shall include the 16 LSBs of K_{NRP} 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. In the case where the different V2X services are mapped to the different PC5 unicast user plane security policies, when more than one V2X service identifier is included in the DIRECT LINK ESTABLISHMENT REQUEST message, each of

the user plane security polices of those V2X services shall be compatible, e.g. "user plane integrity protection not needed" and " user plane integrity protection required" are not compatible.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall form the $K_{NRP-sess}$ ID from the 8 MSBs of $K_{NRP-sess}$ ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of $K_{NRP-sess}$ ID received in the DIRECT LINK SECURITY MODE COMMAND message.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall integrity protect the DIRECT LINK SECURITY MODE COMPLETE message with the new security context. If the selected ciphering protection algorithm is not the null ciphering protection algorithm, the target UE shall cipher 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, NRPIK, NRPEK if applicable, $K_{NRP-sess}$ ID, and the selected security algorithm as specified in TS 33.536 [20].

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 T5007. If the selected integrity protection algorithm is not the null integrity protection algorithm, the UE checks 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. If the selected integrity protection algorithm is the null integrity protection algorithm, the UE continues the procedure without checking the integrity protection.

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: LSBs of $K_{NRP-sess}$ ID conflict;

#e: UE PC5 unicast signalling security policy mismatch; 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 #e "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 #e "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 T5007 and:

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

6.1.2.7.6 Abnormal cases

6.1.2.7.6.1 Abnormal cases at the initiating UE

a) Timer T5007 expires.

The initiating UE shall retransmit the DIRECT LINK SECURITY MODE COMMAND message and restart timer T5007. 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.

6.1.2.8 PC5 unicast link keep-alive procedure

6.1.2.8.1 General

The PC5 unicast link keep-alive procedure is used to maintain a PC5 unicast link between two UEs, i.e., check that the link between the two UEs is still viable. The UE sending the DIRECT LINK KEEPALIVE REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

The PC5 unicast link keep-alive procedure can be initiated by only one UE or both UEs in the established PC5 unicast link.

NOTE: Whether the PC5 unicast link keep-alive procedure is initiated by only one UE or both UEs in the established PC5 unicast link is UE implementation specific.

6.1.2.8.2 PC5 unicast link keep-alive procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the PC5 unicast link keep-alive procedure:

a) there is a PC5 unicast link between the initiating UE and the target UE.

The initiating UE shall manage a keep-alive timer T5003 and a keep-alive counter for the PC5 unicast link keep-alive procedure. Timer T5003 is used to trigger the periodic initiation of the PC5 unicast link keep-alive procedure. The UE shall start or restart timer T5003 whenever the UE receives a PC5 signalling message or PC5 user plane data from the target UE over this PC5 unicast link. The UE shall set the keep-alive counter to an initial value of zero after PC5 unicast link establishment.

Editor's note: Other conditions to restart the keep-alive timer T5003 are FFS.

Editor's note: Whether the keep-alive timer T5003 value needs to be included or negotiated as part of the PC5 unicast link establishment procedure is FFS.

The initiating UE shall initiate the PC5 unicast link keep-alive procedure when:

a) timer T5003 for this link expires;

b) optionally, a request from the lower layers to check the viability of the PC5 unicast link is received; or

NOTE 1: Whether the lower layers can request the initiation of the PC5 unicast link keep-alive procedure, and what the triggers for the lower layers are to request the initiation of the PC5 unicast link keep-alive procedure, are UE implementation specific.

c) optionally, a request from the upper layers to check the viability of the PC5 unicast link is received.

NOTE 2: Whether the upper layers can request the initiation of the PC5 unicast link keep-alive procedure, and what the triggers for the upper layers are to request the initiation of the PC5 unicast link keep-alive procedure, are UE implementation specific.

In order to initiate the PC5 unicast link keep-alive procedure, the initiating UE shall stop timer T5003, if running, and shall create a DIRECT LINK KEEPALIVE REQUEST message. In this message, the initiating UE:

a) shall include the keep-alive counter for the PC5 unicast link; and

b) may include a maximum inactivity period to indicate the maximum inactivity period of the initiating UE over this PC5 unicast link.

NOTE 3: The value chosen for the maximum inactivity period of the initiating UE is UE implementation specific with the objective to minimize the number of keep-alive procedures as much as possible. It is desirable to have the maximum inactivity period value to be slightly higher than the value of keep-alive timer T5003.

After the DIRECT LINK KEEPALIVE 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, and start timer T5004. The UE shall not send a new DIRECT LINK KEEPALIVE REQUEST message to the same target UE while timer T5004 is running.

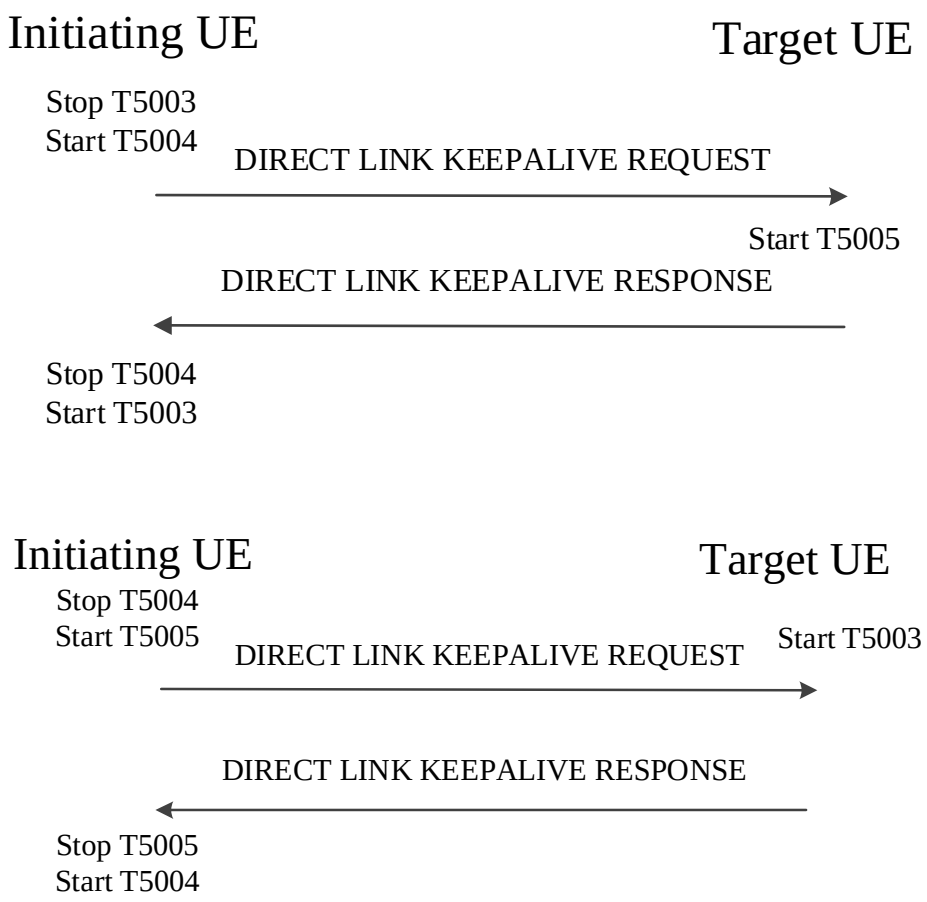

Figure 6.1.2.8.2: PC5 unicast link keep-alive procedure

6.1.2.8.3 PC5 unicast link keep-alive procedure accepted by the target UE

Upon receipt of a DIRECT LINK KEEPALIVE REQUEST message, the target UE shall create a DIRECT LINK KEEPALIVE RESPONSE message. In this message, the target UE:

a) shall include the keep-alive counter set to the same value as that received in the DIRECT LINK KEEPALIVE REQUEST message.

After the DIRECT LINK KEEPALIVE 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.

If a maximum inactivity period is included in the DIRECT LINK KEEPALIVE REQUEST message, the target UE shall stop T5005, if running, and start T5005 with its value set to the maximum inactivity period. The target UE shall restart T5005 whenever the target UE receives a PC5 signalling message or PC5 user plane data from the initiating UE over this PC5 unicast link.

6.1.2.8.4 PC5 unicast link keep-alive procedure completion by the initiating UE

Upon receipt of a DIRECT LINK KEEPALIVE RESPONSE message, the initiating UE shall stop timer T5004, start timer T5003 and increment the keep-alive counter for the PC5 unicast link.

6.1.2.8.5 Abnormal cases

6.1.2.8.5.1 Abnormal cases at the initiating UE

a) Timer T5004 expires.

The initiating UE shall retransmit the DIRECT LINK KEEPALIVE REQUEST message with the last used value of the keep-alive counter and restart timer T5004. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link keep-alive procedure and locally release the PC5 unicast link.

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 keep-alive procedure is completed.

The initiating UE shall abort the PC5 unicast link keep-alive procedure and initiate a PC5 unicast link release procedure.

c) The initiating UE receives a DIRECT LINK KEEPALIVE RESPONSE message with a keep-alive counter value different from the value which the initiating UE had included in the last sent DIRECT LINK KEEPALIVE REQUEST message.

The initiating UE shall discard the DIRECT LINK KEEPALIVE RESPONSE message.

d) The initiating UE receives a PC5 signalling message other than a DIRECT LINK KEEPALIVE RESPONSE message or PC5 user plane data from the target UE over this PC5 unicast link while timer T5004 is running.

The initiating UE shall stop timer T5004, abort the PC5 unicast link keep-alive procedure, start timer T5003 and increment the keep-alive counter for the PC5 unicast link.

e) The initiating UE receives a DIRECT LINK KEEPALIVE RESPONSE message when T5004 is not running.

The initiating UE shall discard the DIRECT LINK KEEPALIVE RESPONSE message.

6.1.2.8.5.2 Abnormal cases at the target UE

a) Timer T5005 expires.

The target UE may:

1) initiate a PC5 unicast link keep-alive procedure to check the link; or

2) initiate the PC5 unicast link release procedure.

Whether the UE chooses 1) or 2) is left to UE implementation.

b) The target UE receives a DIRECT LINK KEEPALIVE REQUEST message with a keep-alive counter value lower that the value which the target UE had included in the last sent DIRECT LINK KEEPALIVE RESPONSE message.

The target UE shall discard the DIRECT LINK KEEPALIVE REQUEST message.

c) The target UE receives a DIRECT LINK KEEPALIVE REQUEST message while it is generating a PC5 signalling message to be sent to the initiating UE over this PC5 unicast link.

The target UE:

1) shall pass this PC5 signalling 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; and

2) may consider transmission of this PC5 signalling message to be an implicit DIRECT LINK KEEPALIVE RESPONSE message and skip generating a DIRECT LINK KEEPALIVE RESPONSE message. If a maximum inactivity period is included in the DIRECT LINK KEEPALIVE REQUEST message, the target UE shall stop T5005, if running, and start T5005 with its value set to the maximum inactivity period.

6.1.2.9 Data transmission over PC5 unicast link

When receiving user data from upper layers to be sent over PC5 unicast link to a specific UE, the transmitting UE shall determine the PC5 unicast link context corresponding to the application layer ID, and then shall tag each outgoing protocol data unit with the following information before passing it to the lower layers for transmission:

a) a layer-3 protocol data unit type (see 3GPP TS 38.323 [10]) set to:

1) IP packet, if the V2X message contains IP data; or

2) non-IP packet, if the V2X message contains non-IP data;

b) the PC5 link identifier associated with the PC5 unicast link context;

c) optionally, the source layer-2 ID set to the source layer-2 ID associated with the PC5 unicast link context;

d) optionally, the destination layer-2 ID set to the destination layer-2 ID associated with the PC5 unicast link context; and

e) the PQFI set to the value corresponding to the V2X service identifier and the optional V2X application requirements according to the mapping rules specified in clause 5.2.3.

6.1.2.10 PC5 unicast link re-keying procedure

6.1.2.10.1 General

The purpose of the PC5 unicast link re-keying procedure is to derive a new $K_{NRP\text{-}sess}$ and, optionally, a new K_{NRP} for an existing PC5 unicast link. The UE sending the DIRECT LINK REKEYING REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

NOTE: There is no benefit in performing the PC5 unicast link re-keying procedure when using the null integrity protection algorithm, hence it is recommended not to trigger it when using the null integrity protection algorithm.

6.1.2.10.2 PC5 unicast link re-keying procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the PC5 unicast link re-keying procedure:

a) there is a PC5 unicast link between the initiating UE and the target UE; and

1) if the session key $K_{NRP\text{-}sess}$ used to protect PC5 unicast link needs to be refreshed and neither timer T5007 nor T5008 are running; or

2) if the UE wants to refresh K_{NRP} and neither timer T5007 nor T5008 are running.

In order to initiate the PC5 unicast link re-keying procedure, the initiating UE shall create a DIRECT LINK REKEYING REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container IE if the null integrity protection algorithm is not in use;

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

b) shall include a Nonce_1 IE set to the 128-bit nonce value generated by the initiating UE for the purpose of session key refresh over this PC5 unicast link if the null integrity protection algorithm is not in use;

c) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the re-keying of this PC5 unicast link;

d) shall include the 8 MSBs of $K_{NRP-sess}$ ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the null integrity protection algorithm is not in use; and

e) may include a Re-authentication indication if the initiating UE wants to derive a new K_{NRP}.

After the DIRECT LINK REKEYING 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, and start timer T5008. The UE shall not send a new DIRECT LINK REKEYING REQUEST message to the same target UE while timer T5008 is running.

NOTE 2: In order to ensure successful PC5 unicast link re-keying, T5008 should be set to a value larger than the sum of T5006 and T5007.

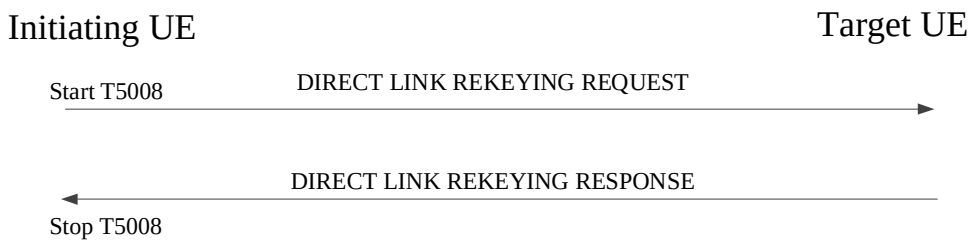

Figure 6.1.2.10.2: PC5 unicast link re-keying procedure

6.1.2.10.3 PC5 unicast link re-keying procedure accepted by the target UE

Upon receipt of a DIRECT LINK REKEYING REQUEST message, if the DIRECT LINK REKEYING REQUEST message includes a Re-authentication indication, the target UE shall derive a new K_{NRP}. This may require performing one or more PC5 unicast link authentication procedures as specified in clause 6.1.2.6.

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

Then the target UE shall initiate a PC5 unicast link security mode control procedure as specified in in clause 6.1.2.7.

Upon successful completion of the PC5 unicast link security mode control procedure, the target UE shall create a DIRECT LINK REKEYING RESPONSE message. The target UE shall cipher and integrity protect the DIRECT LINK REKEYING RESPONSE message with the new security context.

After the DIRECT LINK REKEYING RESPONSE 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.

6.1.2.10.4 PC5 unicast link re-keying procedure completion by the initiating UE

Upon receipt of the DIRECT LINK REKEYING RESPONSE message, the initiating UE shall stop timer T5008 and check the integrity of the DIRECT LINK REKEYING RESPONSE message using the new NRPIK. The initiating UE shall send new NRPIK, NRPEK, $K_{NPR-sess}$ ID, and the selected security algorithm as specified in 3GPP TS 33.536 [20] along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication to the lower layer.

6.1.2.10.5 Abnormal cases at the initiating UE

The following abnormal cases can be identified:

a) Timer T5008 expires.

The initiating UE shall retransmit the DIRECT LINK REKEYING REQUEST message and restart timer T5008. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link re-keying procedure and may initiate the PC5 unicast link release 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 re-keying procedure is completed.

The initiating UE shall abort the procedure.

6.1.2.11 PC5 unicast security

6.1.2.11.1 Overview

This clause describes the principles for the handling of PC5 unicast security contexts in the UE and the procedures used for the security protection of PC5 signalling messages exchanged between UEs over a PC5 unicast link. Based on the security policies of UEs, security protection for a PC5 unicast link involves integrity protection and ciphering of the PC5 signalling messages, and integrity protection and ciphering of PC5 user plane data. The use of integrity protection and ciphering over a PC5 unicast link is optional (see 3GPP TS 33.536 [20]).

The signalling procedures for the control of PC5 unicast security are part of the PC5 signalling protocol and are described in detail in clause 6.1.2.

NOTE: It is recommended to set the UE PC5 unicast signalling integrity protection policy to "signalling integrity protection required" in order to guarantee security protection over PC5. In this clause, for the ease of description, it is assumed that integrity protection and ciphering are used, unless explicitly indicated otherwise. Operation of a PC5 unicast link without integrity protection or ciphering is achieved by configuring the UE so that it always selects the "null integrity protection algorithm", 5G-IA0, or the "null ciphering algorithm", 5G-EA0.

6.1.2.11.2 Handling of PC5 unicast security contexts

6.1.2.11.2.1 General

The security parameters for authentication, integrity protection and ciphering are tied together in a PC5 unicast security context and identified by a $K_{NRP\text{-}sess}$ identifier ($K_{NRP\text{-}sess}$ ID). The relationship between the security parameters is defined in 3GPP TS 33.536 [20]. The $K_{NRP\text{-}sess}$ ID is self-assigned by the UEs.

Before security can be activated, the UEs establishing a PC5 unicast link need to establish a PC5 unicast security context. The PC5 unicast security context is created as the result of a PC5 unicast link authentication procedure and PC5 unicast link security mode control procedure between the UEs.

The PC5 unicast security context is taken into use by the UEs when one of the UEs initiates a PC5 unicast link security mode control procedure.

The creation of a security context also results in the establishment of a key K_{NRP} and its identifier K_{NRP} ID at the UEs.

The PC5 unicast security context can be created using K_{NRP} when a new PC5 unicast link is established without executing a new PC5 unicast link authentication procedure (see clause 6.1.2.11.2.2). For this purpose, the DIRECT LINK ESTABLISHMENT REQUEST message contains a K_{NRP} ID indicating the PC5 unicast security context.

6.1.2.11.2.2 Establishment of secure exchange of PC5 signalling messages

Secure exchange of PC5 signalling messages over a PC5 unicast link is established during the PC5 unicast link establishment procedure by initiating a PC5 unicast link security mode control procedure. After successful completion of the PC5 unicast link security mode control procedure, all PC5 signalling messages exchanged between the UEs are

sent integrity protected using the PC5 unicast security algorithms, and except for the DIRECT LINK SECURITY MODE COMMAND message, all PC5 signalling messages exchanged between the UEs are sent ciphered using the PC5 unicast security algorithms. The security exchange of PC5 signalling messages is maintained for the lifetime of the PC5 unicast link.

6.1.2.11.2.3 Change of security keys

When one of the UEs using the PC5 unicast link initiates a PC5 unicast link re-keying procedure to create a new PC5 unicast security context, the PC5 signalling messages exchanged during the PC5 unicast link authentication procedure, if any, are integrity protected and ciphered using the old PC5 unicast security context, i.e. the PC5 unicast security context that was in use before the start of the PC5 unicast link re-keying procedure.

Both UEs shall continue to use the old PC5 unicast security context until the UE which has received the DIRECT LINK REKEYING REQUEST message initiates a PC5 unicast link security mode control procedure. The UE shall send the DIRECT LINK SECURITY MODE COMMAND message integrity protected with the new PC5 unicast security context, but unciphered. When the peer UE responds with a DIRECT LINK SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the new PC5 unicast security context.

6.1.2.11.3 Checking of PC5 signalling messages in the UE

If the signalling integrity protection is not activated for PC5 unicast link, all PC5 signalling messages are processed by the UE without integrity protection.

If the signalling integrity protection is activated for PC5 unicast link, except the messages listed below, no PC5 signalling messages that is not integrity protected shall be processed by the UE:

a) DIRECT LINK ESTABLISHMENT REQUEST message;

b) DIRECT LINK ESTABLISHMENT REJECT message;

c) DIRECT LINK AUTHENTICATION REQUEST message;

d) DIRECT LINK AUTHENTICATION RESPONSE message;

e) DIRECT LINK AUTHENTICATION REJECT message; and

f) DIRECT LINK SECURITY MODE REJECT message.

NOTE: These messages are accepted by the receiving UE without integrity protection, as in certain situations they are sent by the peer UE before security can be activated.

Once the secure exchange of PC5 signalling messages has been established, the receiving UE shall not process any PC5 signalling message that does not successfully pass the integrity check. The DIRECT LINK SECURITY MODE COMMAND message shall be processed as specified in clause 6.1.2.7.3. If any PC5 signalling message is received as not integrity protected and not ciphered even though the secure exchange of PC5 signalling messages has been established, then the receiving UE shall discard this message.

6.1.2.12 PC5 QoS flow establishment over PC5 unicast link

In order to establish a PC5 QoS flow establishment over PC5 unicast link, the UE shall derive the PC5 QoS parameters based on the V2X application requirements provided by the upper layers (if available) and the V2X service type (e.g. PSID or ITS-AID) according to the PC5 QoS mapping rules defined in clause 5.2.3. The UE shall create the PC5 QoS flow(s) based on the derived PC5 QoS parameters. For each PC5 QoS flow to be created, the UE shall perform the following operations:

a) self-assign a PQFI;

b) create a PC5 QoS flow context, which contains:

   1) the PQFI;

   2) the V2X service indentifier(s); and

   3) the derived PC5 QoS parameters;

c) create a new PC5 QoS rule which contains:

1) a PC5 QoS rule identifier;

2) the PQFI;

3) a set of packet filters; and

4) a precedence value; and

d) pass the following parameters to the lower layers:

1) the PQFI;

2) the PC5 QoS parameters;

3) the PC5 link identifier; and

4) optionally, the source and destination layer-2 IDs.

6.1.2.13 PC5 QoS flow match over PC5 unicast link

When service data or request from the upper layers is received, the UE determines if there is any existing PC5 QoS flow(s) matching the service data or request, i.e. based on the PC5 QoS rules for the existing PC5 QoS flow(s).

If there is no PC5 QoS rules for the existing PC5 QoS flow(s) matching the service data or request, the UE shall derive the PC5 QoS parameters based on the V2X application requirements provided by the upper layers (if available) and the V2X service type (e.g. PSID or ITS-AID) according to the PC5 QoS mapping rules defined in clause 5.2.3 and shall perform the following:

a) if there is no existing PC5 QoS flow that fulfils the derived PC5 QoS parameters, then the UE shall create a new PC5 QoS flow as specified in clause 6.1.2.12;

b) if there is an existing PC5 QoS flow that fulfils the derived PC5 QoS parameters, then the UE shall update the PC5 packet filter set in the PC5 QoS rule of this PC5 QoS flow, e.g. add the new packet filter in the PC5 QoS rule of this existing PC5 QoS flow; and

c) the UE shall use the new PC5 QoS flow created as described in bullet a) or the existing PC5 QoS flow with the updated PC5 QoS rules as described in bullet b) to perform the transmission of V2X communication over PC5 as specified in clause 6.1.2.9.

If there is a PC5 QoS rule for the existing PC5 QoS flow matching the service data or request, the UE shall use this existing PC5 QoS flow to perform transmission of V2X communication over PC5 as specified in clause 6.1.2.9.

6.1.3 Broadcast mode communication over PC5

6.1.3.1 Overview

This clause describes the V2X communication over PC5 reference point in broadcast mode operation. The UE is configured with the related information as described in clause 5.2.3.

6.1.3.2 Transmission of broadcast mode V2X communication over PC5

6.1.3.2.1 Initiation

6.1.3.2.1.1 Requirements for V2X communication over PC5

When the upper layers request the UE to send a V2X message of a V2X service identified by a V2X service identifier using V2X communication over PC5, the request from the upper layers includes:

a) the V2X message;

b) the V2X service identifier of the V2X service for the V2X message;

c) the type of data in the V2X message (i.e. IP or non-IP);

d) if the V2X message contains non-IP data, the V2X message family (see clause 7.1 of 3GPP TS 24.386 [5]) of data in the V2X message;

e) optionally the communication mode which is set to broadcast mode; and

f) optionally the V2X application requirements (e.g. priority requirement, reliability requirement, delay requirement).

Upon a request from upper layers to send a V2X message of a V2X service identified by a V2X service identifier using V2X communication over PC5, if:

a) the UE is configured with V2X service identifier to V2X frequency mapping rules for V2X communication over PC5 as specified in clause 5.2.3; and

b) there is one or more V2X frequencies associated with the V2X service identifier of the V2X service for the V2X message in the current geographical area,

then the UE passes the one or more V2X frequencies associated with the V2X service identifier of the V2X service and the communication mode which is set to broadcast mode for the V2X message to the lower layers.

Then, if any of the following conditions are met:

a) the following conditions are met:

   1) the UE is served by NR or served by E-UTRA for NR-PC5 V2X communication;

   2) the UE intends to use the radio resources (i.e. carrier frequency) provided by a serving cell;

   3) the registered PLMN is in the list of PLMNs in which the UE is authorized to use V2X communication over PC5 when the UE is served by NR or served by E-UTRA for V2X communication over PC5 as specified in clause 5.2.3; and

   4) the V2X service identifier of the V2X service is included in the list of V2X services authorized for V2X communication over PC5 as specified in clause 5.2.3 or the UE is configured with a default destination layer-2 ID for V2X communication over PC5 as specified in clause 5.2.3;

b) the following conditions are met:

   1) the UE is:

      i) not served by NR and not served by E-UTRA for V2X communication over PC5;

      ii) in limited service state as specified in 3GPP TS 23.122 [2], if the reason for the UE being in limited service state is one of the following:

         A) the UE is unable to find a suitable cell in the selected PLMN as specified in 3GPP TS 38.304 [9];

         B) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #11 "PLMN not allowed" as specified in 3GPP TS 24.501 [6]; or

         C) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #7 "5GS services not allowed" as specified in 3GPP TS 24.501 [6]; or

      iii) in limited service state as specified in 3GPP TS 23.122 [2] for reasons other than A), B) or C) above, and located in a geographical area for which the UE is provisioned with "non-operator managed" radio parameters as specified in clause 5.2.3;

   2) the UE is authorized to use V2X communication over PC5 when the UE is not served by NR and not served by E-UTRA for V2X communication as specified in clause 5.2.3; and

   3) the V2X service identifier of the V2X service is included in the list of V2X services authorized for V2X communication over PC5 as specified in clause 5.2.3 or the UE is configured with a default destination layer-2 ID for V2X communication over PC5 as specified in clause 5.2.3;

then the UE shall proceed as specified in clause 6.1.3.2.1.2, else the UE shall not perform transmission of V2X communication over PC5.

6.1.3.2.1.2 PC5 QoS flow match and establishment

When determining if any existing PC5 QoS flow match the request from upper layers, UE shall proceeds as follows:

a) according to the PC5 QoS mapping rules specified in clause 5.2.3, the UE shall use the PC5 QoS parameters corresponding to the V2X service identifier and optionally V2X application requirements;

b) according to the V2X service identifier to destination layer-2 ID for broadcast mapping rules specified in clause 5.2.3, the UE shall use the destination layer-2 ID corresponding to the V2X service identifier;

c) if there is no existing context for the destination layer-2 ID, then:

   1) build a new context for the destination layer-2 ID;

   2) self-assign a new source layer-2 ID; and

   3) pass the source layer-2 ID and the destination layer-2 ID to lower layers.

d) if in the context for the destination layer-2 ID, there is no PC5 QoS rule for the existing PC5 QoS flow(s) matching the service data or request, the UE shall derive the PC5 QoS parameters based on the V2X application requirements provided by the upper layers (if available) and the V2X service type (e.g. PSID or ITS-AID) according to the PC5 QoS mapping rules defined in clause 5.2.3 and shall perform the following::

   1) if there is no existing PC5 QoS flow that fulfils the derived PC5 QoS parameters, then the UE shall create a new PC5 QoS flow by performing the following operations:

      i) self-assign a new PQFI;

      ii) create a new PC5 QoS flow context which contains:

         - the PQFI;

         - the V2X service identifier(s); and;

         - the derived PC5 QoS parameters;

      iii) create a new PC5 QoS rule which contains:

         - a PC5 QoS rule identifier;

         - the PQFI;

         - a set of packet filters; and

         - a precedence value; and

      iv) pass the following parameters to the lower layers:

         - the PQFI;

         - the PC5 QoS parameters; and

         - the source layer-2 ID and the destination layer-2 ID;

   2) if there is an existing PC5 QoS flow that fulfils the derived PC5 QoS parameters, then the UE shall update the PC5 packet filter set in the PC5 QoS rule of this PC5 QoS flow, e.g. add the new packet filter in the PC5 QoS rule of this existing PC5 QoS flow; and

   3) the UE shall use the new PC5 QoS flow created as described in bullet 1) or the existing PC5 QoS flow with the updated PC5 QoS rules as described in bullet 2) to perform the transmission of V2X communication over PC5 as specified in clause 6.1.3.2.2; and

e) if in the context for the destination layer-2 ID, there is a PC5 QoS rule for the existing PC5 QoS flow matching the service data or request, the UE shall use this existing PC5 QoS flow to perform transmission of V2X communication over PC5 as specified in clause 6.1.3.2.2.

Two types of packet filters are supported for V2X communication over PC5, i.e. the IP packet filter set and the V2X packet filter set. A PC5 QoS Rule contains either the IP packet filter set or the V2X packet filter set.

The IP packet filter set is defined as content of the packet filter contents field specified in 3GPP TS 24.501 [6] figure 9.11.4.13.4 and table 9.11.4.13.1.

The V2X packet filter set shall support packet filters based on at least any combination of:

- V2X Service type (e.g. PSID or ITS-AID);
- the source layer-2 ID and the destination layer-2 ID; and
- Application Layer ID (e.g. Station ID);

6.1.3.2.2 Transmission

The UE shall include the V2X message in a protocol data unit with the following parameters:

a) a layer-3 protocol data unit type (see 3GPP TS 38.323 [10]) set to:

   1) IP packet, if the V2X message contains IP data; or

   2) non-IP packet, if the V2X message contains non-IP data;

b) the source layer-2 ID set to the layer-2 ID self-assigned by the UE for V2X communication over PC5;

c) the destination layer-2 ID set to:

   1) the destination layer-2 ID associated with the V2X service identifier of the V2X service in this list of V2X services authorized for V2X communication over PC5 as specified in clause 5.2.3, if the V2X service identifier of the V2X service is included in the list of V2X services authorized for V2X communication over PC5 as specified in clause 5.2.3; or

   2) the default destination layer-2 ID configured to the UE for V2X communication over PC5 as specified in clause 5.2.3, if the V2X service identifier of the V2X service is not included in the list of V2X services authorized for V2X communication over PC5 and the UE is configured with a default destination layer-2 ID for V2X communication over PC5;

d) if the V2X message contains non-IP data, an indication to set the non-IP type field of the non-IP type PDU to the value corresponding to the V2X message family (see clause 7.1 of 3GPP TS 24.386 [5]) used by the V2X service as indicated by upper layers;

e) if the V2X message contains IP data, the source IP address set to the source IP address self-assigned by the UE for V2X communication over PC5;

f) the PQFI set to the value corresponding to the PC5 QoS Rules as specified in clause 6.1.3.2.1;

g) if the UE is configured with V2X service identifier to Tx Profile mapping rules for V2X communication over PC5 as specified in clause 5.2.3, the Tx Profile associated with the V2X service identifier as specified in clause 5.2.3.

then UE shall request radio resources for V2X communication over PC5 as specified in 3GPP TS 38.300 [8], and pass the V2X message on the PC5 QoS Flow identified by the PQFI to lower layers for transmission. The PC5 QoS Rules corresponding to the PQFIs map V2X messages with the same V2X service identifier and with the same PC5 QoS parameters to the same PC5 QoS Flow, and apply PQFI to V2X messages;

If the UE is camped on a serving cell indicating that V2X communication over PC5 is supported by the network, but not broadcasting any carrier frequencies and radio resources for V2X communication over PC5 as specified in 3GPP TS 38.331 [11], the UE shall request radio resources for V2X communication over PC5 as specified in 3GPP TS 24.501 [6].

If the UE has an emergency PDN connection, the UE shall send an indication to the lower layers to prioritize transmission over the emergency PDN connection as compared to transmission of V2X communication over PC5.

6.1.3.2.3 Procedure for UE to use provisioned radio resources for V2X communication over PC5

When the UE is not served by NR and not served by E-UTRA for V2X communication and is authorized to use V2X communication over PC5, the UE shall identify the RAT to be used for V2X communication over PC5 according to the list of RATs in which the UE is authorized to use V2X communication over PC5. If both E-UTRA-PC5 and NR-PC5 for V2X are authorized to the UE for V2X communication over PC5, the UE selects a RAT used for V2X communication over PC5 according to local policy. After identifying E-UTRA-PC5 to be used for V2X communication over PC5, the UE performs the procedure defined in clause 6.1.2.3 of 3GPP TS 24.386 [5]. After identifying NR-PC5 to be used for V2X communication over PC5, the UE shall select the corresponding radio parameters to be used for V2X communication over PC5 as follows:

a) if the UE can determine itself located in a geographical area, and the UE is provisioned with radio parameters for the geographical area, the UE shall select the radio parameters associated with that geographical area; or

b) in all other cases, the UE shall not initiate V2X communication over PC5.

It is out of scope of the present specification to define how the UE can locate itself in a specific geographical area. When the UE is in coverage of a 3GPP RAT it can for example use information derived from the serving PLMN. When the UE is not in coverage of a 3GPP RAT it can use other techniques, e.g. global navigation satellite system (GNSS). The UE shall not consider user provided location as a valid input to locate itself in a specific geographical area.

If the UE intends to use "non-operator managed" radio parameters as specified in clause 5.2.3, the UE shall initiate V2X communication over PC5 with the selected radio parameters.

If the UE intends to use "operator managed" radio parameters as specified in clause 5.2.3, before initiating V2X communication over PC5, the UE shall check with lower layers whether the selected radio parameters can be used in the current location without causing interference to other cells as specified in 3GPP TS 38.331 [11], and:

a) if the lower layers indicate that the usage would not cause any interference, the UE shall initiate V2X communication over PC5; or

NOTE: If the lower layers find that there exists a cell operating the provisioned radio resources (i.e., carrier frequency), and the cell belongs to the registered PLMN or a PLMN equivalent to the registered PLMN, and the UE is authorized for V2X communication over PC5 in this PLMN, the UE can use the radio parameters indicated by the cell as specified in 3GPP TS 38.331 [11].

b) else if the lower layers report that one or more PLMNs operate in the provisioned radio resources (i.e. carrier frequency) then:

   1) if the following conditions are met:

      i) none of the PLMNs reported by the lower layers is the registered PLMN or equivalent to the registered PLMN;

      ii) at least one of the PLMNs reported by the lower layers is in the list of authorized PLMNs for V2X communication over PC5 and provides radio resources for V2X communication over PC5 as specified in 3GPP TS 38.331 [11]; and

      iii) the UE does not have an emergency PDU session;

      then the UE shall:

      i) if in 5GMM-IDLE mode, perform PLMN selection triggered by V2X communication over PC5 as specified in 3GPP TS 23.122 [2]; or

      ii) else if in 5GMM-CONNECTED mode, either:

         A) perform a Registration procedure as specified in 3GPP TS 24.501 [6] and then perform PLMN selection triggered by V2X communication over PC5 as specified in 3GPP TS 23.122 [2]; or

         B) not initiate V2X communication over PC5.

Whether the UE performs i) or ii) above is left up to UE implementation; or

2) else the UE shall not initiate V2X communication over PC5.

If the registration to the selected PLMN is successful, the UE shall proceed with the procedure to initiate V2X communication over PC5 as specified in clause 6.1.3.2.1.

If the UE is performing V2X communication over PC5 using radio parameters associated with a geographical area and moves out of that geographical area, the UE shall stop performing V2X communication over PC5 and then:

a) if the UE is not served by NR and not served by E-UTRA for V2X communication over PC5 or the UE intends to use radio resources for V2X communication over PC5 other than those operated by the serving cell, the UE shall select appropriate radio parameters for the new geographical area as specified above; or

b) if the UE is served by NR or served by E-UTRA for V2X communication over PC5 and intends to use radio resources for V2X communication over PC5 operated by the serving cell, the UE shall proceed with the procedure to initiate V2X communication over PC5 when served by NR or served by E-UTRA for V2X communication over PC5.

6.1.3.2.4 Privacy of V2X transmission over PC5

Upon initiating transmission of V2X communication over PC5, if:

a) the V2X service identifier of a V2X service requesting transmission of V2X communication over PC5 is in the list of of V2X services which require privacy for V2X communication over PC5 as specified in clause 5.2.3; and

b) the UE is located in a geographical area in which this V2X service requires privacy for V2X communication over PC5 as specified in clause 5.2.3, or the UE is not provisioned any geographical areas in which this V2X services requires privacy for V2X communication over PC5,

then the UE shall proceed as follows:

a) if timer T5020 is not running, start timer T5020 and set its timer value as the privacy timer value as specified in clause 5.2.3;

b) upon:

1) getting an indication from upper layers that the application layer identifier has been changed; or

2) timer T5020 expiry,

then:

1) change the value of the source layer-2 ID self-assigned by the UE for the V2X communication over PC5;

2) if the V2X message contains IP data, change the value of the source IP address self-assigned by the UE for V2X communication over PC5;

3) provide an indication to upper layers that the source layer-2 ID and/or the source IP address are changed;

4) pass the changed source layer-2 ID and destination layer-2 ID, along with the corresponding PQFI down to the lower layer;

5) restart timer T5020; and

6) upon stopping transmission of the V2X communication over PC5, stop timer T5020.

6.1.3.3 Reception of broadcast mode V2X communication over PC5

The UE may be configured by upper layers with one or more destination layer-2 ID(s) for reception of V2X messages over PC5. For each received protocol data unit over PC5, the receiving UE shall check if the destination layer-2 ID of the received protocol data unit matches one of the configured destination Layer-2 IDs. If yes, the UE shall then check whether the protocol data unit type as defined 3GPP TS 38.323 [10] provided by the lower layers for the received packet is set to IP packet or non-IP packet, and pass the protocol data unit to the corresponding upper layer entity.

6.1.4 Groupcast mode communication over PC5

6.1.4.1 Overview

This clause describes the V2X communication over PC5 reference point in groupcast mode operation. The UE is configured with the related information as described in clause 5.2.3.

6.1.4.2 Transmission of groupcast mode V2X communication over PC5

6.1.4.2.1 Initiation

6.1.4.2.1.1 Requirements for V2X communication over PC5

The requirements for groupcast mode V2X communication over PC5 is the same as described in clause 6.1.3.2.1.1, with the following additions:

a) When the upper layers request the UE to send a V2X message of a V2X service identified by a V2X service identifier using V2X communication over PC5, then the request from the upper layers may include:

   1) the group identifier information (i.e. an application-layer V2X group identifier);

   2) the group size and the member IDs;

   3) the range requirement; or

   4) the communication mode which is set to groupcast mode.

6.1.4.2.1.2 PC5 QoS flow match and establishment

The PC5 QoS flow match and establishment for groupcast mode V2X communication over PC5 is the same as described in clause 6.1.3.2.1.2, with the following modifications:

a) The UE shall determine the destination layer-2 ID as:

   1) if no group identifier information is provided, then according to the mapping rules specified in clause 5.2.3, the UE shall use the destination layer-2 ID corresponding to the V2X service identifier;

   2) if group identifier information is provided and there is a context for the group identifier information, then UE shall use the destination layer-2 ID in the context for the group identifier information; and

   3) if group identifier information is provided and there is no context for the group identifier information, then the UE shall:

      i) use the group identifier as the input to the SHA-256 hashing algorithm as specified in ISO/IEC 10118-3:2018 [23]; and

      ii) use the 24 least significant bits of the 256 bits of the output as destination layer-2 ID; and

NOTE: SHA-256 hashing algorithm is pre-configured in the ME.

b) If there is no existing context for the destination layer-2 ID and optional group identifier, the UE shall proceed as:

   1) to establish a new context for the destination layer-2 ID and optional group identifier;

   2) self-assign a new source layer-2 ID; and

   3) to pass the source/destination layer-2 IDs, optional group size and optional member IDs to lower layers.

6.1.4.2.2 Transmission

The transmission of groupcast mode V2X communication over PC5 is same as described in clause 6.1.3.2.2, with the following additions:

a) If group identifier is provided, then the destination layer-2 ID shall be set to the destination layer-2 ID in the context for the group identifier as specified in clause 6.1.4.2.1.2.

6.1.4.2.3 Procedure for UE to use provisioned radio resources for groupcast mode V2X communication over PC5

The procedures described in clause 6.1.3.2.3 apply with using the privacy timer T5030 for groupcast.

6.1.4.2.4 Privacy of V2X transmission over PC5

The procedures described in clause 6.1.3.2.4 apply.

6.1.4.3 Reception of groupcast mode V2X communication over PC5

The reception of groupcast mode V2X communication over PC5 is the same as described in clause 6.1.3.3, with the following additions:

a) Besides the configured destination layer-2 ID(s) for reception of V2X messages over PC5, the UE shall also derive the destination layer-2 ID(s) based on group identifier(s) if provided by upper layers as specified in clause 6.1.4.2.1.

6.2 V2X communication over Uu

6.2.1 General

This clause describes the procedures at the UE and the V2X application server, for V2X communication over Uu.

There are no additional security or privacy procedures of V2X communication over Uu beyond those specified in 3GPP TS 33.501 [21] for Uu connectivity with 5GCN.

Both IP based and non-IP based V2X communication over Uu are supported.

V2X messages carried over Uu are sent or received over unicast only in this release of the specification. Furthermore, V2X messages are carried over Uu using user data over user plane. For this, the UE first performs the UE-requested PDU session establishment procedure to establish user-plane resouces as specified in 3GPP TS 24.501 [6].

Procedures for V2X communication over Uu for V2X services not identified by a V2X service identifier are out of scope of the present version of the present specification.

NOTE: The upper layers are responsible for re-assembly of V2X messages and that is out of scope of 3GPP.

6.2.2 Transmission of V2X communication over Uu from UE to V2X application server

The upper layers can request the UE to send a V2X message of a V2X service identified by a V2X service identifier using V2X communication over Uu. The request from the upper layers includes:

a) the V2X message;

b) the V2X service identifier of the V2X service for the V2X message;

c) the type of data in the V2X message (IP or non-IP); and

d) if the V2X message contains non-IP data, the V2X message family (see clause 7.1 of 3GPP TS 24.386 [5]) of data in the V2X message.

Upon a request from upper layers to send a V2X message of a V2X service identified by a V2X service identifier using V2X communication over Uu:

a) if the registered PLMN of the UE is not in the list of PLMNs in which the UE is configured to use V2X communication over Uu as specified in clause 5.2.4, the UE shall determine that the transmission of V2X communication over Uu from UE to V2X application server is not configured and shall not continue with the rest of the steps; and

b) if the V2X service identifier is included in the list of V2X service identifier to PDU session parameters mapping rules specified in clause 5.2.4;

then:

1) the UE shall determine the mapping rule in the list of V2X service identifier to PDU session parameters mapping rules specified in clause 5.2.4, such that the mapping rule contains the V2X service identifier provided by upper layers;

2) the UE shall consider the PDU session type, the SSC mode (if indicated in determined mapping rule), an S-NSSAI (if indicated in determined mapping rule) and a DNN (if indicated in determined mapping rule) indicated in the determined mapping rule as the UE local configuration and request information of the PDU session via which to send a PDU according to 3GPP TS 24.526 [22]. The UE shall use the transport layer protocol, if indicated in the determined mapping rule, to transport the V2X message;

3) if the PDU session is of "IPv4", "IPv6" or "IPv4v6" PDU session type:

i) if the V2X service identifier is included in the list of V2X service identifier to V2X application server address mapping rules as specified in clause 5.2.4, then:

A) the UE shall discover the V2X application server address for uplink transport as described in clause 6.2.6. If the V2X application server address cannot be discovered, the UE shall determine that the transmission of V2X communication over Uu from UE to V2X application server is not possible and shall not continue with the rest of the steps;

B) if UDP is to be used for the determined V2X application server address, the UE shall generate a UDP message as described in IETF RFC 768 [14]. In the UDP message, the UE shall include the V2X message provided by upper layers in the data octets field. The UE shall send the UDP message to the determined V2X application server address; and

C) if TCP is to be used for the determined V2X application server address:

1) if a TCP connection with the determined V2X application server address is not established yet, the UE shall establish a TCP connection with the determined V2X application server address; and

2) the UE shall generate one or more TCP message(s) as described in IETF RFC 793 [25]. In the one or more TCP message(s), the UE shall include the V2X message provided by upper layers in the

data octets filed. The UE shall send the one or more TCP message(s) to the determined V2X application server address via the TCP connection; and

4) if the PDU session is of "Unstructured" PDU session type and the type of data in the V2X message is non-IP, the UE shall generate a UDP message as described in IETF RFC 768 [14]. In the UDP message, the UE shall encapsulate the V2X message provided by upper layers in the data octets field. The UE shall send the UDP message to the determined V2X application server address.

6.2.3 Reception of V2X communication over Uu from UE to V2X application server

If the V2X application server is configured with one or more UDP ports for uplink transport or one or more TCP ports for bidirectional transport, of V2X message(s) of V2X service(s) identified by V2X service identifier(s) using the V2X communication over Uu as specified in clause 6.2.7:

1) if the V2X application server is configured with a UDP port for uplink transport, the V2X application server shall extract a V2X message of the V2X service from a UDP message received on a local IP address and a UDP port; and

2) if the V2X application server is configured with a TCP port for bidirectional transport, the V2X application server shall listen for incoming TCP connection(s) on a local IP address and the TCP port, shall accept the incoming TCP connection(s), shall receive one or more TCP message(s)via the accepted TCP connection(s) and shall extract a V2X message of the V2X service from the received one or more TCP message(s).

If the V2X application server is configured to handle data of "Unstructured" PDU Session type for transport of V2X message(s) of V2X service(s) identified by V2X service identifier(s) using V2X communication over Uu as specified in clause 6.2.7, the V2X application server shall receive one or more UDP message(s) as data of a point-to-point tunnel established over N6 and shall extract a V2X message and a V2X message family (if the V2X message is non-IP based) from the received UDP message.

6.2.4 Transmission of V2X communication over Uu from V2X application server to UE

The V2X application server shall be configured with UDP port(s), TCP port(s) or any combination of them for transport of the V2X communication over Uu to the UE.

If the V2X application server supports V2X messages of IP type of data and of non-IP type of data, then the V2X application server shall be configured with different UDP ports or TCP ports for V2X messages of different types of data.

If the V2X application server supports V2X messages of several V2X message families, then the V2X application server shall be configured with different UDP ports or TCP ports for V2X messages of different V2X message families.

If the V2X application server determines to use UDP for transmission of the V2X message identified by a V2X service identifier, the V2X application server shall generate a UDP message. If the V2X message is of "Unstructured" PDU Session type, then the V2X application server shall encapsulate the V2X message into IP type data. In the UDP message, the V2X application server:

a) shall set data octets field to the V2X message if the V2X message is of IP type;

a) shall set data octets field to the encapsulated IP type data if the V2X message is of "Unstructured" PDU Session type; and

c) shall set the destination IP address and the destination UDP port to the UE’s IP address and the configured UDP port associated the type of data of the V2X message and the V2X message family of the data of the V2X message (in case of non-IP).

The V2X application server sends the UDP message as the user plane data to the UE.

If the V2X application server determines to use TCP for transmission of the V2X message identified by a V2X service identifier, the V2X application server establishes a TCP connection with the UE if no TCP connection exists, then the V2X application server shall generate a TCP message. In the TCP message, the V2X application server:

a) shall set data octets field to the V2X message; and

b) shall set the destination IP address and the destination TCP port to the UE's IP address and the configured TCP port associated the type of data of the V2X message and the V2X message family of the data of the V2X message (in case of non-IP).

The V2X application server sends the TCP message as the user plane data to the UE.

6.2.5 Reception of V2X communication over Uu from V2X application server to UE

The upper layers can request the UE to receive a V2X message of a V2X service identified by a V2X service identifier using V2X communication over Uu. The request from the upper layers includes:

a) the V2X service identifier of the V2X service for the V2X message to be received;

b) the type of data in the V2X message to be received (IP or non-IP); and

c) if the V2X message to be received contains non-IP data, the V2X message family (see clause 9.2.1) of data in the V2X message to be received.

Upon a request from upper layers to receive a V2X message of a V2X service identified by a V2X service identifier using V2X communication over Uu:

a) if the registered PLMN of the UE is not in the list of PLMNs in which the UE is configured to use V2X communication over Uu as specified in clause 5.2.4, the UE shall determine that the transmission of V2X communication over Uu from V2X application server to UE is not configured and shall not continue with the rest of the steps; and

b) if the V2X service identifier is included in the list of V2X service identifier to PDU session parameters mapping rules specified in clause 5.2.4;

then:

1) the UE shall determine the mapping rule in the list of V2X service identifier to PDU session parameters mapping rules specified in clause 5.2.4, such that the mapping rule contains the V2X service identifier provided by upper layers;

2) the UE shall establish a PDU session with the PDU session type, the SSC mode (if indicated in determined mapping rule), an S-NSSAI (if indicated in determined mapping rule) and a DNN (if indicated in determined mapping rule) indicated in the determined mapping rule, if such PDU session does not exist yet. The UE shall use the transport layer protocol, if indicated in the determined mapping rule, to receive the V2X message;

3) if the PDU session is of "IPv4", "IPv6" or "IPv4v6" PDU session type:

i) if the V2X service identifier is included in the list of V2X service identifier to V2X application server address mapping rules as specified in clause 5.2.4, then:

A) the UE shall discover the V2X application server address for downlink transport as described in clause 6.2.6. If the V2X application server address cannot be discovered, the UE shall determine that the transmission of V2X communication over Uu from V2X application server to UE is not possible and shall not continue with the rest of the steps. If the V2X service identifier is not included in the list of V2X service identifier to V2X application server address mapping rules as specified in clause 5.2.4, the UE shall continue with the rest of the steps; and

B) if UDP is to be used for the determined V2X application server address:

1) the UE shall select the UDP port for downlink transport based on configuration parameters for V2X communication as defined in clause 5.2.4; and

2) the UE shall listen for UDP packets over the determined UDP port, and provide the UDP packets to the upper layers if received; and

C) if TCP is to be used for the determined V2X application server address:

1) if a TCP connection with the determined V2X application server address is not established yet, the UE shall establish a TCP connection with the determined V2X application server address; and

2) the UE shall listen for TCP packets over the established TCP connection, and provide the TCP packets to the upper layers if received; and

4) if the PDU session is of "Unstructured" PDU session type and the type of data in the V2X message is non-IP, the UE shall proceed as UDP is to be used for the determined V2X application server address with the exeption that the V2X message is encapsulated as IP type data packets.

6.2.6 V2X application server discovery

Before initiating V2X communication over Uu, the UE needs to discover the V2X application server to which the V2X messages shall be sent or received.

To discover the V2X application server address for uplink transport, the UE shall proceed as follows, in priority order:

a) if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server IP address and a UDP port for uplink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall use this IP address and the UDP or TCP port for V2X communication over Uu;

b) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

c) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server IP address and a UDP port for uplink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN as specified in clause 5.2.4, the UE shall use this IP address and the UDP or TCP port for V2X communication over Uu;

d) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN as specified inclause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

e) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the IP type of data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

f) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the IP type of data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

g) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN and the IP type of data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

h) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN and the IP type of data

as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

i) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

j) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

k) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

l) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for uplink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

m) else if the V2X service of the V2X message is not identified by a V2X service identifier and the UE is configured with a V2X application server IP address for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall use this IP address for V2X communication over Uu;

n) else if the V2X service of the V2X message is not identified by a V2X service identifier and the UE is configured with a V2X application server FQDN for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address for V2X communication over Uu;

o) else if the V2X service of the V2X message is not identified by a V2X service identifier and the UE is configured with a V2X application server IP address for the serving PLMN as specified in clause 5.2.4, the UE shall use this IP address for V2X communication over Uu; and

p) else if the V2X service of the V2X message is not identified by a V2X service identifier and the UE is configured with a V2X application server FQDN for the serving PLMN as specified in clause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address for V2X communication over Uu.

NOTE: It is out of scope of the present specification to define how the UE can locate itself in a specific geographical area. When the UE is in coverage of a 3GPP RAT it can for example use information derived from the serving PLMN. When the UE is not in coverage of a 3GPP RAT it can use other techniques.

To discover the V2X application server address for downlink transport, the UE shall proceed as follows, in priority order:

a) if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server IP address and a UDP port for downlink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall use this IP address and the UDP or TCP port for V2X communication over Uu;

b) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN and the geographical area in which the UE is located as specified in clause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

c) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server IP address and a UDP port for downlink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN as specified in clause 5.2.4, the UE shall use this IP address and the UDP or TCP port for V2X communication over Uu;

d) else if the V2X service of the V2X message is identified by a V2X service identifier and this V2X service identifier is associated with a V2X application server FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport in the list of V2X service identifier to V2X application server address mapping rules for the serving PLMN as specified in clause 5.2.4, the UE shall perform DNS lookup as specified in IETF RFC 1035 [19], then use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

e) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the IP type of data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

f) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the IP type of data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

g) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the the serving PLMN and the IP type of data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

h) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains IP data, and the default V2X application server address applicable for the serving PLMN and the IP type of data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

i) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu;

j) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN, the geographical area in which the UE is located and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu;

k) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an IP address and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall use the IP address and the UDP or TCP port for V2X communication over Uu; and

l) else if the V2X service of the V2X message is identified by a V2X service identifier, the V2X message contains non-IP data, and the default V2X application server address applicable for the serving PLMN and the V2X message family of the non-IP data as specified in clause 5.2.4 is configured and contains an FQDN and a UDP port for downlink transport or a TCP port for bidirectional transport, then the UE shall perform DNS lookup of the FQDN as specified in IETF RFC 1035 [19], and shall use the resulting IP address and the UDP or TCP port for V2X communication over Uu.

If multiple V2X application servers are discovered, the V2X application server to be used is selected by the V2X application layer.

The UE shall perform V2X application server discovery again when the UE changes its registered PLMN.

If the V2X application server used by the UE is associated with a particular geographical area, the UE shall perform V2X application server discovery again when the UE moves out of that geographical area.

6.2.7 V2X application server configuration

For transport of V2X message(s) of V2X service(s) identified by V2X service identifier(s) using V2X communication over Uu, the V2X application server shall be configured:

a) with one or more UDP ports for uplink transport;

b) with one or more UDP ports for downlink transport;

c) with one or more TCP ports for bidirectional transport;

d) to handle data of "Unstructured" PDU Session type; or

e) any combination of the above.

If the V2X application server is configured with one or more UDP ports for uplink transport of V2X message(s) of a V2X service(s) identified by V2X service identifier(s) using V2X communication over Uu:

1) if the V2X application server supports V2X messages of IP type of data and of non-IP type of data, then the V2X application server shall be configured with different UDP ports for V2X messages of different types of data; and

2) if the V2X application server supports V2X messages of several V2X message families, then the V2X application server shall be configured with different UDP ports for V2X messages of different V2X message families.

7 Message functional definition and contents

7.1 Overview

This clause contains the definition and contents of the messages used in the procedures described in the present document.

7.2 Provisioning of parameters for V2X configuration signalling messages

7.2.1 UE policy provisioning request

7.2.1.1 Message definition

The UE POLICY PROVISIONING REQUEST message is sent by the UE to the PCF to request the PCF to manage V2XP, see table 7.2.1.1.1

Message type: UE POLICY PROVISIONING REQUEST

Significance: dual

Direction: UE to network

Table 7.2.1.1.1: UE POLICY PROVISIONING REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity TS 24 501 [4] clause 9.6	M	V	1
	UE POLICY PROVISIONING REQUEST message identity	UE policy delivery service message type TS 24 501 [4] clause D.6.1	M	V	1
	Requested UE policies	Requested UE policies 8.3.2	M	LV	2-3

7.2.2 UE policy provisioning reject

7.2.2.1 Message definition

The UE POLICY PROVISIONING REJECT message is sent by the PCF to the UE to report that the PCF rejects request to manage V2XP, see table 7.2.2.1.1

Message type: UE POLICY PROVISIONING REJECT

Significance: dual

Direction: network to UE

Table 7.2.2.1.1: UE POLICY PROVISIONING REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity TS 24 501 [4] clause 9.6	M	V	1
	UE POLICY PROVISIONING REJECT message identity	UE policy delivery service message type TS 24 501 [4] clause D.6.1	M	V	1
	UPDS cause	UPDS cause 8.3.1	M	V	1

7.3 V2X communication over PC5 signalling messages

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 identifiers	V2X service identifier 8.4.3	M	LV	5-253
	Source user info	Application layer ID 8.4.4	M	LV	3-253
	UE security capabilities	UE security capabilities 8.4.14	M	LV	3-9
	UE PC5 unicast signalling security policy	UE PC5 unicast signalling security policy 8.4.15	M	V	2
74	Key establishment information container	Key establishment information container 8.4.12	O	TLV-E	4-n
53	Nonce_1	Nonce 8.4.13	O	TV	17
54	MSBs of $K_{NRP\text{-}sess}$ ID	MSBs of $K_{NRP\text{-}sess}$ ID 8.4.16	O	TV	2
28	Target user info	Application layer ID 8.4.4	O	TLV	3-253
52	K_{NRP} ID	K_{NRP} ID 8.4.17	O	TV	5

7.3.1.2 Target user info

The UE shall include this IE if it has received the target UE's application layer ID from upper layers.

7.3.1.3 Key establishment information container

The UE shall include this IE if the UE PC5 unicast signalling security policy is set to "signalling integrity protection required" or "signalling integrity protection preferred".

7.3.1.4 Nonce_1

The UE shall include this IE if the UE PC5 unicast signalling security policy is set to "signalling integrity protection required" or "signalling integrity protection preferred".

7.3.1.5 MSBs of $K_{NRP\text{-}sess}$ ID

The UE shall include this IE if the UE PC5 unicast signalling security policy is set to "signalling integrity protection required" or "signalling integrity protection preferred".

7.3.1.6 K_{NRP} ID

The UE may include this IE if it has an existing K_{NRP} for the target UE.

7.3.2 Direct link establishment accept

7.3.2.1 Message definition

This message is sent by a UE to another peer UE to accept the received DIRECT LINK ESTABLISHMENT REQUEST message. See table 7.3.2.1.1.

Message type: DIRECT LINK ESTABLISHMENT ACCEPT

Significance: dual

Direction: UE to peer UE

Table 7.3.2.1.1: DIRECT LINK ESTABLISHMENT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK ESTABLISHMENT ACCEPT message identity	PC5 signalling message type 8.4.1.	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	2
	Source user info	Application layer ID 8.4.4	M	LV	3-253
	QoS flow descriptions	PC5 QoS flow descriptions 8.4.5	M	LV-E	5-65537
	Configuration of UE PC5 unicast user plane security protection	Configuration of UE PC5 unicast user plane security protection 8.4.23	M	V	1
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

7.3.4 Direct link modification request

7.3.4.1 Message definition

This message is sent by the UE to another peer UE to initiate the direct link modification procedure. See table 7.3.4.1.1.

Message type: DIRECT LINK MODIFICATION REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.4.1.1: DIRECT LINK MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK MODIFICATION REQUEST message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	Link modification operation code	Link modification operation code 8.4.8	M	V	1
	QoS flow descriptions	PC5 QoS flow descriptions 8.4.5	M	LV-E	5-65537

7.3.5 Direct link modification accept

7.3.5.1 Message definition

This message is sent by the UE to another peer UE to indicate that the link modification request is accepted. See table 7.3.5.1.

Message type: DIRECT LINK MODIFICATION ACCEPT

Significance: dual

Direction: UE to peer UE

Table 7.3.5.1.1: DIRECT LINK MODIFICATION ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK MODIFICATION ACCEPT message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
79	QoS flow descriptions	PC5 QoS flow descriptions 8.4.5	O	TLV-E	6-65538

7.3.6 Direct link release request

7.3.6.1 Message definition

This message is sent by the UE to another peer UE to initiate the direct link release procedure. See table 7.3.6.1.1.

Message type: DIRECT LINK RELEASE REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.6.1.1: DIRECT LINK RELEASE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK RELEASE REQUEST 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
	MSB of K_{NRP} ID	MSB of K_{NRP} ID 8.4.16	M	V	2

7.3.7 Direct link release request accept

7.3.7.1 Message definition

This message is sent by the UE to another peer UE to indicate that the link release request is accepted. See table 7.3.7.1.

Message type: DIRECT LINK RELEASE ACCEPT

Significance: dual

Direction: UE to peer UE

Table 7.3.7.1: DIRECT LINK RELEASE ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT_LINK_RELEASE ACCEPT message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	LSB of K_{NRP} ID	LSB of K_{NRP} ID 8.4.17	M	V	2

7.3.8 Direct link keepalive request

7.3.8.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link keep-alive procedure is initiated. See table 7.3.8.1.1.

Message type: DIRECT LINK KEEPALIVE REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.8.1.1: DIRECT LINK KEEPALIVE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK KEEPALIVE REQUEST message identity	PC5 signalling message type 8.4.1.	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	Keep-alive counter	Keep-alive counter 8.4.10	M	V	4
55	Maximum inactivity period	Maximum inactivity period 8.4.11	O	TV	5

7.3.8.2 Maximum inactivity period

The UE may include this IE to indicate its maximum inactivity period to the peer UE.

7.3.9 Direct link keepalive response

7.3.9.1 Message definition

This message is sent by a UE to another peer UE to respond to a DIRECT LINK KEEPALIVE REQUEST message. See table 7.3.9.1.1.

Message type: DIRECT LINK KEEPALIVE RESPONSE

Significance: dual

Direction: UE to peer UE

Table 7.3.9.1.1: DIRECT LINK KEEPALIVE RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK KEEPALIVE RESPONSE message identity	PC5 signalling message type 8.4.1.	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	Keep-alive counter	Keep-alive counter 8.4.10	M	V	4

7.3.10 Direct link authentication request

7.3.10.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link authentication procedure is initiated. See table 7.3.10.1.1.

Message type: DIRECT LINK AUTHENTICATION REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.10.1.1: 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 8.4.12	M	LV-E	3-n

7.3.11 Direct link authentication response

7.3.11.1 Message definition

This message is sent by a UE to another peer UE to respond to a DIRECT LINK AUTHENTICATION REQUEST message. See table 7.3.11.1.1.

Message type: DIRECT LINK AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to peer UE

Table 7.3.11.1.1: 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 8.4.12	M	LV-E	3-n

7.3.12 Direct link authentication reject

7.3.12.1 Message definition

This message is sent by a UE to another peer UE to reject a DIRECT LINK AUTHENTICATION REQUEST message. See table 7.3.12.1.1.

Message type: DIRECT LINK AUTHENTICATION REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.12.1.1: 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

7.3.13 Direct link security mode command

7.3.13.1 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 7.3.13.1.1.

Message type: DIRECT LINK SECURITY MODE COMMAND

Significance: dual

Direction: UE to peer UE

Table 7.3.13.1.1: 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
	Selected security algorithms	Selected security algorithms 8.4.18	M	V	1
	UE security capabilities	UE security capabilities 8.4.14	M	LV	3-9
	UE PC5 unicast signalling security policy	UE PC5 unicast signalling security policy 8.4.15	M	V	1
55	Nonce_2	Nonce 8.4.13	O	TV	17
52	LSBs of $K_{NRP\text{-}sess}$ ID	LSBs of $K_{NRP\text{-}sess}$ ID 8.4.19	O	TV	2
74	Key establishment information container	Key establishment information container 8.4.12	O	TLV-E	4-n
62	MSBs of K_{NRP} ID	MSBs of K_{NRP} ID 8.4.20	O	TV	3

7.3.13.2 Nonce_2

The UE shall include this IE if the selected integrity protection algorithms is not the null integrity protection algorithm.

7.3.13.3 LSBs of KNRP-sess ID

The UE shall include this IE if the selected integrity protection algorithms is not the null integrity protection algorithm.

7.3.13.4 Key establishment information container

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

7.3.13.5 MSBs of K_{NRP} ID

The UE shall include this IE if the UE has derived a new K_{NRP}.

7.3.14 Direct link security mode complete

7.3.14.1 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 7.3.14.1.1.

Message type: DIRECT LINK SECURITY MODE COMPLETE

Significance: dual

Direction: UE to peer UE

Table 7.3.14.1.1: 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
	UE PC5 unicast user plane security policy	UE PC5 unicast user plane security policy 8.4.22	M	V	1
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
52	LSBs of K_{NRP} ID	LSBs of K_{NRP} ID 8.4.21	O	TV	3

7.3.14.2 IP address configuration

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

7.3.14.3 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".

7.3.14.4 LSBs of K_{NRP} ID

The UE shall include this IE if a new K_{NRP} was derived.

7.3.15 Direct link security mode reject

7.3.15.1 Message definition

This message is sent by a UE to another peer UE to reject a DIRECT LINK SECURITY MODE COMMAND message. See table 7.3.15.1.1.

Message type: DIRECT LINK SECURITY MODE REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.15.1.1: 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

7.3.16 Direct link rekeying request

7.3.16.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link re-keying procedure is initiated. See table 7.3.16.1.1.

Message type: DIRECT LINK REKEYING REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.16.1.1: DIRECT LINK REKEYING REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK REKEYING REQUEST message identity	PC5 signalling message type 8.4.1.	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	UE security capabilities	UE security capabilities 8.4.14	M	LV	3-9
74	Key establishment information container	Key establishment information container 8.4.12	O	TLV-E	4-n
53	Nonce_1	Nonce 8.4.13	O	TV	17
54	MSBs of $K_{NRP-sess}$ ID	MSBs of $K_{NRP-sess}$ ID 8.4.16	O	TV	2
56	Re-authentication indication	Re-authentication indication 8.4.24	O	TV	2

7.3.16.2 Key establishment information container

The UE shall include this IE if the null integrity protection algorithm is not in use.

7.3.16.3 Nonce_1

The UE shall include this IE if the null integrity protection algorithm is not in use.

7.3.16.4 MSBs of KNRP-sess ID

The UE shall include this IE if the null integrity protection algorithm is not in use.

7.3.16.5 Re-authentication indication

The UE shall include this IE if the UE wants to derive a new K_{NRP}.

7.3.17 Direct link rekeying response

7.3.17.1 Message definition

This message is sent by a UE to another peer UE to respond to a DIRECT LINK REKEYING REQUEST message. See table 7.3.17.1.1.

Message type: DIRECT LINK REKEYING RESPONSE

Significance: dual

Direction: UE to peer UE

Table 7.3.17.1.1: DIRECT LINK REKEYING RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK REKEYING RESPONSE message identity	PC5 signalling message type 8.4.1.	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1

7.3.18 Direct link identifier update request

7.3.18.1 Message definition

This message is sent by a UE to another peer UE to initiate the direct link identifier procedure. See table 7.3.18.1.1.

Message type: DIRECT LINK IDENTIFIER UPDATE REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.18.1.1: DIRECT LINK IDENTIFIER UPDATE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK IDENTIFIER UPDATE REQUEST message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	MSB of $K_{NRP-sess}$ ID	MSB of $K_{NRP-sess}$ ID 8.4.16	M	V	1
	Source layer-2 ID	Layer-2 ID 8.4.25	M	V	3
57	Source user info	Application layer ID 8.4.4	O	TLV	4-254
58	Source link local IPv6 address	Link local IPv6 address 8.4.7	O	TV	17

7.3.18.2 Source user info

This IE is included when the initiating UE receives a new application layer ID.

7.3.18.3 Source link local IPv6 address

This IE is included when the link local IPv6 address changes at the initiating UE.

7.3.19 Direct link identifier update accept

7.3.19.1 Message definition

This message is sent by the UE to another peer UE to indicate that the link identifier update request is accepted. See table 7.3.19.1.1.

Message type: DIRECT LINK IDENTIFIER UPDATE ACCEPT

Significance: dual

Direction: UE to peer UE

Table 7.3.19.1.1: DIRECT LINK IDENTIFIER UPDATE ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK IDENTIFIER UPDATE ACCEPT message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	LSB of $K_{NRP-sess}$ ID	LSB of $K_{NRP-sess}$ ID 8.4.17	M	V	1
	MSB of $K_{NRP-sess}$ ID	MSB of $K_{NRP-sess}$ ID 8.4.16	M	V	1
	Source layer-2 ID	Layer-2 ID 8.4.25	M	V	3
	Target layer-2 ID	Layer-2 ID 8.4.25	M	V	3
28	Target user info	Application layer ID 8.4.4	O	TLV	4-254
59	Target link local IPv6 address	Link local IPv6 address 8.4.7	O	TV	17
57	Source user info	Application layer ID 8.4.4	O	TLV	4-254
58	Source link local IPv6 address	Link local IPv6 address 8.4.7	O	TV	17

7.3.19.2 Target user info

This IE is included when the target user info changes at the target UE.

7.3.19.3 Target link local IPv6 address

This IE is included when the link local IPv6 address changes at target UE.

7.3.19.4 Source user info

This IE is included if the target UE receives the source user info in the DIRECT LINK IDENTIFIER UPDATE REQUEST message.

7.3.19.5 Source link local IPv6 address

This IE is included if the target UE receives the source link local IPv6 address in the DIRECT LINK IDENTIFIER UPDATE REQUEST message.

7.3.20 Direct link identifier update ack

7.3.20.1 Message definition

This message is sent by the initiating UE to target UE to indicate that the initiating UE has received target UE's accept message. See table 7.3.20.1.1.

Message type: DIRECT LINK IDENTIFIER UPDATE ACK

Significance: dual

Direction: UE to peer UE

Table 7.3.20.1.1: DIRECT LINK IDENTIFIER UPDATE ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK IDENTIFIER UPDATE ACK message identity	PC5 signalling message type 8.4.1	M	V	1
	Sequence number	Sequence number 8.4.2	M	V	1
	LSB of $K_{NRP-sess}$ ID	LSB of $K_{NRP-sess}$ ID 8.4.z	M	V	1
	Target layer-2 ID	Layer-2 ID 8.4.25	M	V	3
28	Target user info	Application layer ID 8.4.4	O	TLV	4-254
59	Target link local IPv6 address	Link local IPv6 address 8.4.7	O	TV	17

7.3.20.2 Target user info

This IE is included when the initiating UE receives the target user info in the DIRECT LINK IDENTIFIER UPDATE ACCEPT message.

7.3.20.3 Target link local IPv6 address

This IE is included when the initiating UE receives the target link local IPv6 address in the DIRECT LINK IDENTIFIER UPDATE ACCEPT message.

7.3.21 Direct link identifier update reject

7.3.21.1 Message definition

This message is sent by the target UE to initiating UE to indicate that the link identifier update request is not accepted. See table 7.3.21.1.1.

Message type: DIRECT LINK IDENTIFIER UPDATE REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.21.1.1: DIRECT LINK IDENTIFIER UPDATE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK IDENTIFIER UPDATE 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

7.3.22 Direct link modification reject

7.3.22.1 Message definition

This message is sent by the UE to another peer UE to indicate that the link modification request is not accepted. See table 7.3.22.1.1.

Message type: DIRECT LINK MODIFICATION REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.22.1.1: DIRECT LINK MODIFICATION REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK MODIFICATION 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

7.3.23 Direct link establishment reject

7.3.23.1 Message definition

This message is sent by the UE to another peer UE to indicate that the link establishment request is not accepted. See table 7.3.23.1.1.

Message type: DIRECT LINK ESTABLISHMENT REJECT

Significance: dual

Direction: UE to peer UE

Table 7.3.23.1.1: DIRECT LINK ESTABLISHMENT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	DIRECT LINK ESTABLISHMENT 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

8 Information elements coding

8.1 Overview

This clause contains the information elements coding for the messages used in the procedures described in the present document.

8.2 General

The sending entity shall set the value of a spare bit to zero. The receiving entity shall ignore the value of a spare bit.

The sending entity shall not set the value of a field to a reserved value. The receiving entity shall discard a message carrying a field with the value set to a reserved value.

8.3 Provisioning of parameters for V2X configuration signalling information elements

8.3.1 UPDS cause

The purpose of the UPDS cause information element is to indicate the reason why a UPDS request is rejected.

The UPDS cause information element is coded as shown in figure 8.3.2.1 and table 8.3.2.1.

The UPDS cause is a type 3 information element with 2 octets length.

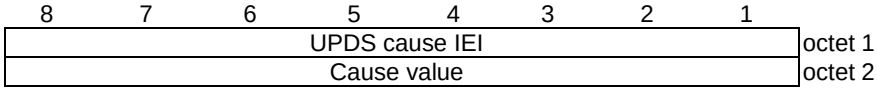

Figure 8.3.2.1: UPDS cause information element

Table 8.3.2.1: UPDS cause information element

Cause value (octet 2)

Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	1	1	1	1	1	Request rejected, unspecified
0	0	1	0	0	0	0	0	Service option not supported
0	0	1	0	0	0	1	0	Service option temporarily out of order
0	0	1	0	0	0	1	1	PTI already in use
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the UE shall be treated as 0010 0010, "service option temporarily out of order". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified".

8.3.2 Requested UE policies

The purpose of the Requested UE policies information element is to enable the UE to request the PCF to provide certain UE policies or certain UE policy subsets.

The Requested UE policies information element is coded as shown in figure 8.3.2.1 and table 8.3.2.1.

The Requested UE policies is a type 4 information element with a minimum length of 3 octets and a maximum length of 4 octets.

8	7	6	5	4	3	2	1	
Requested UE policies IEI								octet 1
Length of Requested UE policies contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	V2XUUI	V2XPC5I	octet 3
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	octet 4*

Figure 8.3.2.1: Requested UE policies information element

Table 8.3.2.1: Requested UE policies information element

UE policies for V2X communication over PC5 indicator (V2XPC5I) (octet 3, bit 1) Bit **1** 0 UE policies for V2X communication over PC5 not requested 1 UE policies for V2X communication over PC5 requested UE policies for V2X communication over Uu indicator (V2XUUI) (octet 3, bit 2) Bit **2** 0 UE policies for V2X communication over Uu not requested 1 UE policies for V2X communication over Uu requested Bit 3 to 8 of octet 3 and bits of octet 4 are spare and shall be coded as zero.

8.4 V2X communication over PC5 signalling information elements

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
0	0	0	0	1	0	1	1	DIRECT LINK AUTHENTICATION REQUEST
0	0	0	0	1	1	0	0	DIRECT LINK AUTHENTICATION RESPONSE
0	0	0	0	1	1	0	1	DIRECT LINK AUTHENTICATION REJECT
0	0	0	0	1	1	1	0	DIRECT LINK SECURITY MODE COMMAND
0	0	0	0	1	1	1	1	DIRECT LINK SECURITY MODE COMPLETE
0	0	0	1	0	0	0	0	DIRECT LINK SECURITY MODE REJECT
0	0	0	1	0	0	0	1	DIRECT LINK REKEYING REQUEST
0	0	0	1	0	0	1	0	DIRECT LINK REKEYING RESPONSE
0	0	0	1	0	0	1	1	DIRECT LINK IDENTIFIER UPDATE REQUEST
0	0	0	1	0	1	0	0	DIRECT LINK IDENTIFIER UPDATE ACCEPT
0	0	0	1	0	1	0	1	DIRECT LINK IDENTIFIER UPDATE ACK
0	0	0	1	0	1	1	0	DIRECT LINK IDENTIFIER UPDATE REJECT

8.4.2 Sequence number

The purpose of the Sequence number information element is to uniquely identify a PC5 signalling message being sent or received. The sending UE will increment the sequence number for each outgoing new PC5 signalling message.

The Sequence number information element is an integer in the 0-255 range.

The Sequence number is a type 3 information element, with a length of 1 octet.

8.4.3 V2X service identifier

The purpose of the V2X service identifier parameter is to carry the identifier of a V2X service.

The V2X service identifier information element is coded as shown in figure 8.4.3.1 and table 8.4.3.1.

The V2X service identifier is a type 4 information element with a minimum length of 6 octets.

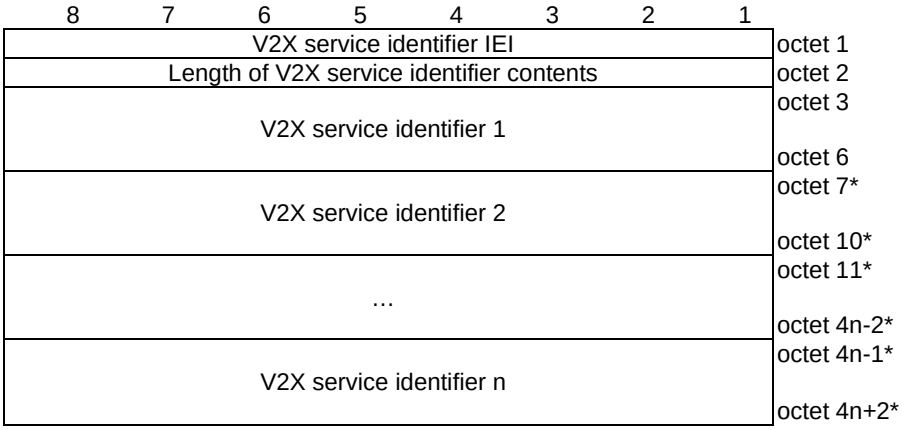

Figure 8.4.3.1: V2X service identifier information element

Table 8.4.3.1: V2X service identifier information element

V2X service identifier: The V2X service identifier field contains a binary coded V2X service identifier as specified in ISO TS 17419 ITS-AID AssignedNumbers [18].

8.4.4 Application layer ID

The purpose of the Application layer ID parameter information element carries an application layer ID as specified in 3GPP TS 23.287 [3].

The Application layer ID information element is coded as shown in figure 8.4.4.1 and table 8.4.4.1.

The Application layer ID is a type 4 information element.

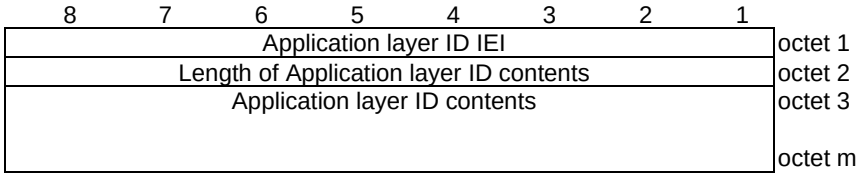

Figure 8.4.4.1: Application layer ID information element

Table 8.4.4.1: Application layer ID information element

The length of Application layer ID contents field contains the binary coded representation of the length of the Application layer ID contents field. The Application layer ID contents field contains the octets indicating the Application layer ID. The format of the Application layer ID parameter is out of scope of this specification.

8.4.5 PC5 QoS flow descriptions

The purpose of the PC5 QoS flow descriptions information element is to indicate a set of PC5 QoS flow descriptions to be used by the UE over the direct link, where each PC5 QoS flow description is a set of parameters as described in clause 5.4.2 of 3GPP TS 23.287 [3].

The PC5 QoS flow descriptions is a type 6 information element with a minimum length of 6 octets. The maximum length for the information element is 65538 octets.

The PC5 QoS flow descriptions information element is coded as shown in figure 8.4.5.1, figure 8.4.5.2, figure 8.4.5.3, figure 8.4.5.4, and table 8.4.5.1.

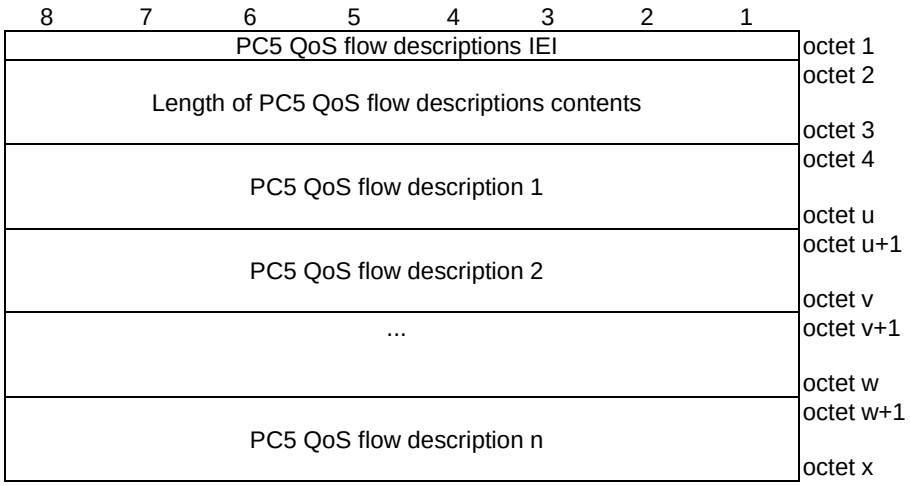

Figure 8.4.5.1: PC5 QoS flow descriptions information element

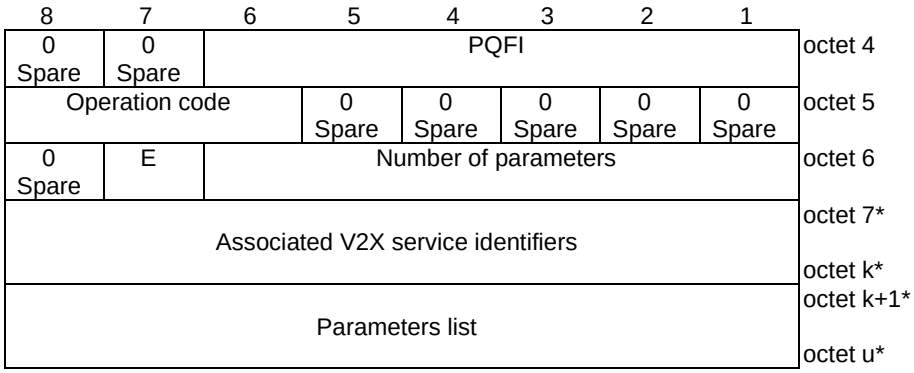

Figure 8.4.5.2: PC5 QoS flow description

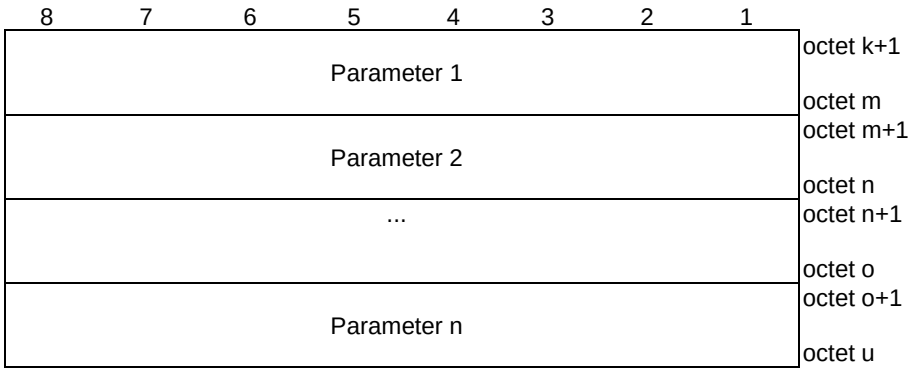

Figure 8.4.5.3: Parameters list

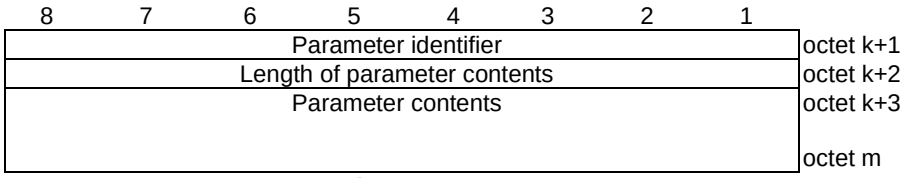

Figure 8.4.5.4: Parameter

Table 8.4.4.1: PC5 QoS flow descriptions information element

PC5 QoS flow identifier (PQFI) (bits 6 to 1 of octet 4)
PQFI field contains the PC5 QoS flow identifier.
Bits
6 5 4 3 2 1
0 0 0 0 0 1PQFI 1
to
1 1 1 1 1 1PQFI 63
The UE shall not set the PQFI value to 0.

Operation code (bits 8 to 6 of octet 5)
Bits
8 7 6
0 0 1 Create new PC5 QoS flow description
0 1 0 Delete existing PC5 QoS flow description
0 1 1 Modify existing PC5 QoS flow description
All other values are reserved.

E bit (bit 7 of octet 6)
For the "create new PC5 QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 reserved
1 parameters list is included

For the "Delete existing PC5 QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 parameters list is not included
1 reserved

For the "modify existing PC5 QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 extension of previously provided parameters
1 replacement of all previously provided parameters

If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" or "replacement of all previously provided parameters", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" and one of the parameters in the new parameters list already exists in the previously provided parameters, the parameter shall be set to the new value.

Number of parameters (bits 6 to 1 of octet 6)
The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet 6 where bit 6 is the most significant and bit 1 is the least significant bit.

Associated V2X service identifiers (octet 7 to k)
The associated V2X service identifiers field contains a variable number of V2X service identifiers associated with the PC5 QoS flow. Associated V2X service identifiers field is coded as the length and value part of V2X service identifier information element as specified in clause 8.4.3 starting with the second octet.

Parameters list (octets k+1 to u)
The parameters list contains a variable number of parameters.

Each parameter included in the parameters list is of variable length and consists of:
- a parameter identifier (1 octet);
- the length of the parameter contents (1 octet); and
- the parameter contents itself (variable amount of octets).

The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:
- 01H (PQI);
- 02H (GFBR); (see NOTE)
- 03H (MFBR); (see NOTE)
- 04H (Averaging window) ;
- 05H (Resource type);
- 06H (Default priority level);
- 07H (Packet delay budget);
- 08H (Packet error rate);
- 09H (Default maximum data burst volume).

If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.
The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.

When the parameter identifier indicates PQI, the parameter contents field contains the binary representation of PQI that is one octet in length.

PQI:

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	
to	Spare
0 0 0 1 0 1 0 0	
0 0 0 1 0 1 0 1	PQI 21
0 0 0 1 0 1 1 0	PQI 22
0 0 0 1 0 1 1 1	PQI 23
0 0 0 1 1 0 0 0	
to	Spare
0 0 1 1 0 1 1 0	
0 0 1 1 0 1 1 1	PQI 55
0 0 1 1 1 0 0 0	PQI 56
0 0 1 1 1 0 0 1	PQI 57
0 0 1 1 1 0 1 0	PQI 58
0 0 1 1 1 0 1 1	PQI 59
0 0 1 1 1 1 0 0	
to	Spare
0 1 0 1 1 0 0 1	
0 1 0 1 1 0 1 0	PQI 90
0 1 0 1 1 0 1 1	PQI 91
0 1 0 1 1 1 0 0	
to	Spare
0 1 1 1 1 1 1 1	
1 0 0 0 0 0 0 0	
to	Operator-specific PQIs
1 1 1 1 1 1 1 0	
1 1 1 1 1 1 1 1	Reserved

The UE shall consider all other values not explicitly defined in this version of the protocol as unsupported.

When the parameter identifier indicates "GFBR", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate followed by two octets containing the value of the guaranteed flow bit rate.
Unit of the guaranteed flow bit rate (octet 1)

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	value is not used
0 0 0 0 0 0 0 1	value is incremented in multiples of 1 Kbps
0 0 0 0 0 0 1 0	value is incremented in multiples of 4 Kbps
0 0 0 0 0 0 1 1	value is incremented in multiples of 16 Kbps
0 0 0 0 0 1 0 0	value is incremented in multiples of 64 Kbps
0 0 0 0 0 1 0 1	value is incremented in multiples of 256 Kbps
0 0 0 0 0 1 1 0	value is incremented in multiples of 1 Mbps
0 0 0 0 0 1 1 1	value is incremented in multiples of 4 Mbps
0 0 0 0 1 0 0 0	value is incremented in multiples of 16 Mbps
0 0 0 0 1 0 0 1	value is incremented in multiples of 64 Mbps
0 0 0 0 1 0 1 0	value is incremented in multiples of 256 Mbps
0 0 0 0 1 0 1 1	value is incremented in multiples of 1 Gbps
0 0 0 0 1 1 0 0	value is incremented in multiples of 4 Gbps
0 0 0 0 1 1 0 1	value is incremented in multiples of 16 Gbps
0 0 0 0 1 1 1 0	value is incremented in multiples of 64 Gbps
0 0 0 0 1 1 1 1	value is incremented in multiples of 256 Gbps
0 0 0 1 0 0 0 0	value is incremented in multiples of 1 Tbps
0 0 0 1 0 0 0 1	value is incremented in multiples of 4 Tbps
0 0 0 1 0 0 1 0	value is incremented in multiples of 16 Tbps

0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps
0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps
0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps
0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps
0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps
0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps
0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps
Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.

Value of the guaranteed flow bit rate (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate in units defined by the unit of the guaranteed flow bit rate.

When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.

When the parameter identifier indicates "MFBR ", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate followed by two octets containing the value of maximum flow bit rate.

Unit of the maximum flow bit rate (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate.

Value of the maximum flow bit rate (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate in units defined by the unit of the maximum flow bit rate.

When the parameter identifier indicates "averaging window", the parameter contents field contains the binary representation of the averaging window for both uplink and downlink in milliseconds and the parameter contents field is two octets in length.

When the parameter identifier indicates "resource type", the parameter contents field contains the binary representation of the resource type that is one octet in length.

Resource type:

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	Non-GBR
0 0 0 0 0 0 1 0	GBR
0 0 0 0 0 0 1 1	Delay critical GBR
0 0 0 0 0 1 0 0	
to	Spare
1 1 1 1 1 1 1 1	

When the parameter identifier indicates "default priority level", the parameter contents field contains the binary representation of the default priority level that is one octet in length.

Default priority level:

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	1
0 0 0 0 0 0 1 0	2
0 0 0 0 0 0 1 1	3
0 0 0 0 0 1 0 0	4
0 0 0 0 0 1 0 1	5
0 0 0 0 0 1 1 0	6
0 0 0 0 0 1 1 1	7
0 0 0 0 1 0 0 0	8
0 0 0 0 1 0 0 1	
to	Spare
1 1 1 1 1 1 1 1	

When the parameter identifier indicates "packet delay budget", the parameter contents field contains the binary representation of the packet delay budget for both uplink and downlink in milliseconds and the parameter contents field is two octets in length.

When the parameter identifier indicates "packet error rate", the parameter contents field contains the binary representation of the power of 10^{-1} for both uplink and downlink and the parameter contents field is one octet in length.

When the parameter identifier indicates "default maximum data burst volume", the parameter contents field contains the binary representation of the default maximum data burst volume for both uplink and downlink in bytes and the parameter contents field is two octets in length.

NOTE: The GFBR and MFBR apply to both directions of the PC5 unicast link.

8.4.6 IP address configuration

The purpose of the IP address configuration information element is to indicate the configuration options for IP address used by the UE over this direct link.

The IP address configuration is a type 3 information element with the length of 2 octets.

The IP address configuration information element is coded as shown in figure z.3.1.6.1 and table z.3.1.6.1.

8	7	6	5	4	3	2	1	
IP address configuration IEI								octet 1
IP address configuration content								octet 2

Figure 8.4.6.1: IP address configuration information element

Table 8.4.6.1: IP address configuration information element

IP address configuration value (octet 2) Bits **4 3 2 1** 0 0 0 1 IPv6 Router 0 0 1 0 address allocation not supported All other values are reserved. Bit 5 to 8 of octet 2 are spare and shall be coded as zero.

8.4.7 Link local IPv6 address

The purpose of the Link local IPv6 address information element is to indicate the link local IPv6 address.

The Link local IPv6 address is a type 3 information element with the length of 17 octets.

The Link local IPv6 address information element is coded as shown in figure 8.4.7.1 and table 8.4.7.1.

8	7	6	5	4	3	2	1	
Link local IPv6 address IEI								octet 1
Link local IPv6 address content								octet 2
								octet 17

Figure 8.4.7.1: Link local IPv6 address information element

Table 8.4.7.1: Link local IPv6 address information element

Link local IPv6 address value (octet 2 to 17) This contains the 128-bit IPv6 address. This IPv6 address is encoded as a 128-bit address according to IETF RFC 4291 [15].

8.4.8 Link modification operation code

The purpose of the Link modification operation code information element is to indicate what the operation of the PC5 unicast link modification procedure triggered by initiating UE is.

The Link modification operation code is a type 3 information element, with a length of 2 octets.

The Link modification operation code information element is coded as shown in figure 8.4.8.1 and table 8.4.8.1.

8	7	6	5	4	3	2	1	
Link modification operation code IEI								octet 1
Link modification operation code								octet 2

Figure 8.4.8.1: Link modification operation code information element

Table 8.4.8.1: Link modification operation code information element

Link modification operation code (octet 2)				
Bits				
4	**3**	**2**	**1**	
0	0	0	1	void
0	0	1	0	void
0	0	1	1	Add new PC5 QoS flow(s) to the existing PC5 unicast link
0	1	0	0	Modify PC5 QoS parameters of the existing PC5 QoS flow(s)
0	1	0	1	Remove existing PC5 QoS flow(s) from the existing PC5 unicast link
0	1	1	0	Associate new V2X service(s) with existing PC5 QoS flow(s)
0	1	1	1	Remove V2X service(s) from existing PC5 QoS flow(s)
1	0	0	0	
to				Spare
1	1	1	0	
1	1	1	1	Reserved
Bit 5 to 8 of octet 2 are spare and shall be coded as zero.				

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 PC5 unicast link
0	0	0	0	0	1	1	0	Authentication failure
0	0	0	0	0	1	1	1	Integrity failure
0	0	0	0	1	0	0	0	UE security capabilities mismatch
0	0	0	0	1	0	0	1	LBSs of $K_{NRP\text{-}sess}$ ID conflict
0	0	0	0	1	0	1	0	UE PC5 unicast signalling security policy mismatch
0	0	0	0	1	0	1	1	Required service not allowed
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".								

8.4.10 Keep-alive counter

The purpose of the Keep-alive counter information element is to indicate the keep-alive counter which is a 32-bit counter used for the PC5 unicast link keep-alive procedure.

The Keep-alive counter is a type 3 information element with a length of 5 octets.

The Keep-alive counter information element is coded as shown in figure 8.4.10.1 and table 8.4.10.1.

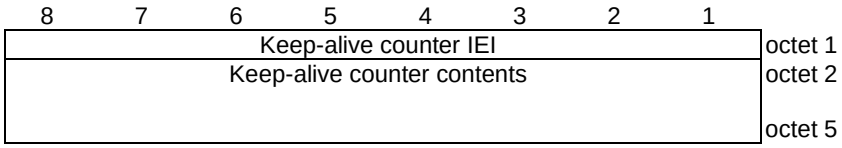

Figure 8.4.10.1: Keep-alive counter information element

Table 8.4.10.1: Keep-alive counter information element

Keep-alive counter contents (octet 2 to 5) This field contains the 32-bit keep-alive counter.

8.4.11 Maximum inactivity period

The purpose of the Maximum inactivity period information element is to indicate the maximum inactivity period of the initiating UE during a PC5 unicast link keep-alive procedure.

The Maximum inactivity period is a type 3 information element, with a length of 5 octets.

The Maximum inactivity period information element is coded as shown in figure 8.4.11.1 and table 8.4.11.1.

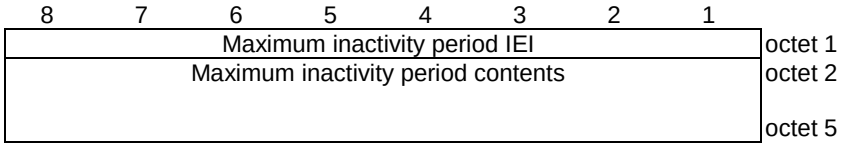

Figure 8.4.11.1: Maximum inactivity period information element

Table 8.4.11.1: Maximum inactivity period information element

Maximum inactivity period contents (octet 2 to 5) This field contains the binary encoding of the maximum inactivity period expressed in units of seconds.

8.4.12 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 8.4.12.1 and table 8.4.12.1.

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.

8.4.13 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 8.4.13.1 and table 8.4.13.1.

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

Figure 8.4.13.1: Nonce information element

Table 8.4.13.1: Nonce information element

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

8.4.14 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 8.4.14.1 and table 8.4.14.1.

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 8.4.14.1: UE security capabilities information element

Table 8.4.14.1: 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

8.4.15 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 8.4.15.1.1 and table 8.4.15.1.

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 8.4.15.1: UE PC5 unicast signalling security policy information element

Table 8.4.15.1: 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.

8.4.16 MSBs of $K_{NRP\text{-}sess}$ ID

The purpose of the MSBs of $K_{NRP\text{-}sess}$ ID information element is to carry the 8 most significant bits of the $K_{NRP\text{-}sess}$ ID.

The MSBs of $K_{NRP\text{-}sess}$ ID information element is a type 3 information element with a length of 2 octets.

The MSBs of $K_{NRP\text{-}sess}$ ID information element is coded as shown in figure 8.4.16.1 and table 8.4.16.1.

8	7	6	5	4	3	2	1	
MSBs of $K_{NRP\text{-}sess}$ ID IEI								octet 1
MSBs of $K_{NRP\text{-}sess}$ ID contents								octet 2

Figure 8.4.16.1: MSBs of $K_{NRP\text{-}sess}$ ID information element

Table 8.4.16.1: MSBs of $K_{NRP-sess}$ ID information element

MSBs of $K_{NRP-sess}$ ID contents (octet 2) This field contains the 8 most significant bits of $K_{NRP-sess}$ ID.

8.4.17 K_{NRP} ID

The purpose of the K_{NRP} ID information element is to carry the identity of the K_{NRP} held by a UE.

The K_{NRP} ID is a type 3 information element with a length of 5 octets.

The K_{NRP} ID information element is coded as shown in figure 8.4.17.1 and table 8.4.17.1

8	7	6	5	4	3	2	1	
K_{NRP} ID IEI								octet 1
K_{NRP} ID contents								octet 2
								octet 5

Figure 8.4.17.1: K_{NRP} ID information element

Table 8.4.17.1: K_{NRP} ID information element

K_{NRP} ID contents (octet 2 to 5) This field contains the 32-bit identifier of a K_{NRP}.

8.4.18 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 8.4.18.1.1 and table 8.4.18.1.

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 8.4.18.1: Selected security algorithms information element

Table 8.4.18.1: 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.	

8.4.19 LSBs of $K_{NRP-sess}$ ID

The purpose of the LSBs of $K_{NRP-sess}$ ID information element is to carry the 8 least significant bits of the $K_{NRP-sess}$ ID.

The LSBs of $K_{NRP-sess}$ ID is a type 3 information element with a length of 2 octets.

The LSBs of $K_{NRP-sess}$ ID information element is coded as shown in figure 8.4.19.1 and table 8.4.19.1.

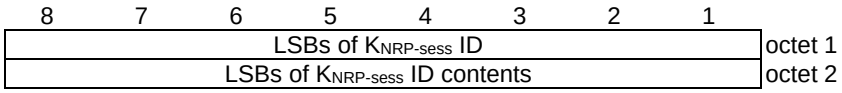

Figure 8.4.19.1: LSBs of $K_{NRP-sess}$ ID information element

Table 8.4.19.1: LSBs of $K_{NRP-sess}$ ID information element

LSBs of $K_{NRP-sess}$ ID contents (octet 2) This field contains the 8 least significant bits of $K_{NRP-sess}$ ID.

8.4.20 MSBs of K_{NRP} ID

The purpose of the MSBs of K_{NRP} ID information element is to carry the 16 most significant bits of the K_{NRP} ID.

The MSBs of K_{NRP} ID is a type 3 information element with a length of 3 octets.

The MSBs of K_{NRP} ID information element is coded as shown in figure 8.4.20.1 and table 8.4.20.1.

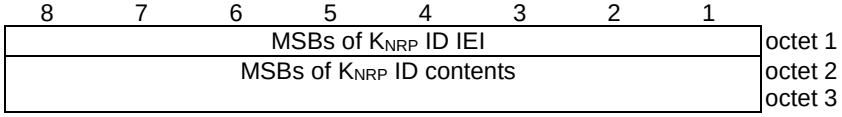

Figure 8.4.20.1: MSBs of K_{NRP} ID information element

Table 8.4.20.1: MSBs of K_{NRP} ID information element

MSBs of K_{NRP} ID contents (octet 2 to 3) This field contains the 16 most significant bits of K_{NRP} ID.

8.4.21 LSBs of K_{NRP} ID

The purpose of the LSBs of K_{NRP} ID information element is to carry the 16 least significant bits of the K_{NRP} ID.

The LSBs of K_{NRP} ID is a type 3 information element with a length of 3 octets.

The LSBs of K_{NRP} ID information element is coded as shown in figure 8.4.21.1 and table 8.4.21.1.

8	7	6	5	4	3	2	1	
LSBs of K_{NRP} ID IEI								octet 1
LSBs of K_{NRP} ID contents								octet 2 octet 3

Figure 8.4.21.1: LSBs of K_{NRP} ID information element

Table 8.4.21.1: LSBs of K_{NRP} ID information element

LSBs of K_{NRP} ID contents (octet 2 to 3) This field contains the 16 least significant bits of K_{NRP} ID.

8.4.22 UE PC5 unicast user plane security policy

The purpose of the UE PC5 unicast user plane security policy information element is to indicate the UE's configuration for integrity protection and ciphering of PC5 user plane data.

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

The UE PC5 unicast user plane security policy information element is coded as shown in figure 8.4.22.1.1 and table 8.4.22.1.

8	7	6	5	4	3	2	1	
UE PC5 unicast user plane security policy IEI								octet 1
0 spare		User plane ciphering policy		0 spare		User plane integrity protection policy		octet 2

Figure 8.4.22.1: UE PC5 unicast user plane security policy information element

Table 8.4.22.1: UE PC5 unicast user plane security policy information element

User plane integrity protection policy (octet 2, bit 1 to 3)
Bits

3	**2**	**1**	
0	0	0	User plane integrity protection not needed
0	0	1	User plane integrity protection preferred
0	1	0	User plane integrity protection required
0	1	1	
to			Spare
1	1	0	
1	1	1	Reserved

If the UE receives a user plane integrity protection policy value that the UE does not understand, the UE shall interpret the value as 010 "user plane integrity protection required".

User plane ciphering policy (octet 2, bit 5 to 7)
Bits

7	**6**	**5**	
0	0	0	User plane ciphering not needed
0	0	1	User plane ciphering preferred
0	1	0	User plane ciphering required
0	1	1	
to			Spare
1	1	0	
1	1	1	Reserved

If the UE receives a user plane ciphering protection policy value that the UE does not understand, the UE shall interpret the value as 010 "user plane ciphering protection required".

Bit 4 and 8 of octet 2 are spare and shall be coded as zero.

8.4.23 Configuration of UE PC5 unicast user plane security protection

The purpose of the configuration of UE PC5 unicast user plane security protection information element is to indicate the agreed configuration for security protection of PC5 user plane data between UEs over the PC5 unicast link.

The configuration of UE PC5 unicast user plane security protection is a type 3 information element with a length of 2 octets.

The configuration of UE PC5 unicast user plane security protection information element is coded as shown in figure 8.4.23.1.1 and table 8.4.23.1.

8	7	6	5	4	3	2	1	
configuration of UE PC5 unicast user plane security protection IEI								octet 1
0 spare	User plane ciphering configuration			0 spare	User plane integrity protection configuration			octet 2

Figure 8.4.23.1: Configuration of UE PC5 unicast user plane security protection information element

Table 8.4.23.1: Configuration of UE PC5 unicast user plane security protection information element

User plane integrity protection configuration (octet 2, bit 1 to 3) Bits **3 2 1** 0 0 0 Off 0 0 1 Off or On 0 1 0 On 0 1 1 to Spare 1 1 0 1 1 1 Reserved User plane ciphering configuration (octet 2, bit 5 to 7) Bits **7 6 5** 0 0 0 Off 0 0 1 Off or On 0 1 0 On 0 1 1 to Spare 1 1 0 1 1 1 Reserved Bit 4 and 8 of octet 2 are spare and shall be coded as zero.

8.4.24 Re-authentication indication

The purpose of the Re-authentication indication information element is to indication that K_{NRP} needs to be refreshed.

The Re-authentication indication information element is a type 3 information element, with a length of 2 octets.

The Re-authentication indication information element is coded as shown in figure 8.4.24.1 and table 8.4.24.1.

8	7	6	5	4	3	2	1	
Re-authentication indication IEI								octet 1
Re-authentication indication contents								octet 2

Figure 8.4.24.1: Re-authentication indication information element

Table 8.4.24.1: Re-authentication indication information element

Re-authentication indication contents (octet 2) Bits **1** 0 Reserved 1 K_{NRP} is requested to be refreshed Bits 2 to 8 of octet 2 are spare and shall be coded as zero.

8.4.25 Layer-2 ID

The purpose of the layer-2 ID information element is to indicate the layer-2 ID that is used by UE.

The layer-2 ID is a type 3 information element with a length of 4 octets.

The layer-2 ID information element is coded as shown in figure 8.4.25.1 and table 8.4.25.1.

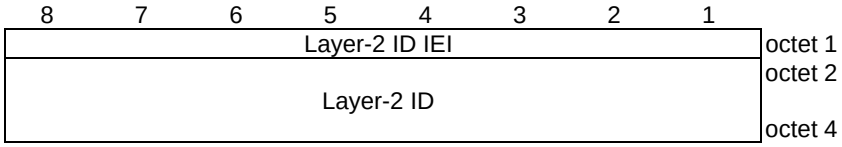

Figure 8.4.25.1: Layer-2 ID information element

Table 8.4.25.1: Layer-2 ID information element

Layer-2 ID (octet 2 to 4) This field contains the 24-bit layer-2 ID.

9 Coding other than information element coding

9.1 Overview

This clause contains the coding of information other than the one provided by the information elements described in clause 8.

10 List of system parameters

10.1 General

The description of timers in the following tables should be considered a brief summary. The complete descriptions of the timers are in the procedures defined in clauses 5 and 6.

10.2 Timers of provisioning of parameters for V2X configuration procedures

Timers of provisioning of parameters for V2X configuration are shown in table 10.2.1.

Table 10.2.1: Timers of provisioning of parameters for V2X configuration – UE side

TIMER NUM.	TIMER VALUE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY
T5010	16s	Transmission of UE POLICY PROVISIONING REQUEST message	MANAGE UE POLICY COMMAND or UE POLICY PROVISIONING REJECT message received	Retransmission of UE POLICY PROVISIONING REQUEST message

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	8s	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	5s	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	5s	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	5s	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	5s	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	Default 10m NOTE 1	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
T5006	2s	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
T5007	2s	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
T5008	8s	Upon sending a DIRECT LINK REKEYING REQUEST message	Upon receiving a DIRECT LINK REKEYING RESPONSE message or DIRECT LINK RELEASE REQUEST message from the target UE	Retransmission of DIRECT LINK REKEYING REQUEST message

TIMER NUM.	TIMER VALUE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T5009	2s	Upon sending a DIRECT LINK IDENTIFIER UPDATE REQUEST message	Upon receiving a DIRECT LINK IDENTIFIER UPDATE ACCEPT or DIRECT LINK IDENTIFIER UPDATE REJECT or DIRECT LINK RELEASE REQUEST message from the target UE	Retransmission of the DIRECT LINK IDENTIFIER UPDATE REQUEST message
T5010	2s	Upon sending a DIRECT LINK IDENTIFIER UPDATE ACCEPT message	Upon receiving a DIRECT LINK IDENTIFIER UPDATE ACK message or DIRECT LINK RELEASE REQUEST message from the initiating UE	Retransmission of the DIRECT LINK IDENTIFIER UPDATE ACCEPT message
T5011		Upon establishing a unicast link configured with privacy	Upon receiving a trigger for link identifier update from the upper layer or upon link release	Transmission of LINK IDENTIFIER UPDATE REQUEST message
NOTE 1 The default value of this timer is used if the DIRECT LINK KEEPALIVE REQUEST message does not provide a timer value in the Maximum inactivity period IE,				

10.4 Timers of PC5 broadcast mode communication

Table 10.4.1: PC5 mode communication timers

TIMER NUM.	TIMER VALUE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T5020	NOTE 1	Upon initiating transmission of broadcast mode V2X communication over PC5, as described in clause 6.1.3.2.4. Upon receiving an indication from upper layers that the application layer identifier has been changed while performing transmission of broadcast mode V2X communication over PC5, as described in clause 6.1.3.2.4. Upon T5020 expiration while performing transmission of broadcast mode V2X communication over PC5, as described in clause 6.1.3.2.4.	Upon stopping transmission of broadcast mode V2X communication over PC5, as described in clause 6.1.3.2.4.	Change the value of the source layer-2 ID self-assigned by the UE for broadcast mode V2X communication over PC5. If the V2X message contains IP data, change the value of the source IP address self-assigned by the UE for broadcast mode V2X communication over PC5.
NOTE 1 The value of this timer is the privacy timer value which is one of the configuration parameters for V2X communication over PC5 (see clause 5.2),				

10.5 Timers of PC5 groupcast mode communication

Table 10.5.1: PC5 groupcast mode communication timers

TIMER NUM.	TIMER VALUE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T5030	NOTE 1	Upon initiating transmission of groupcast mode V2X communication over PC5, as described in clause 6.1.3.2.4. Upon receiving an indication from upper layers that the application layer identifier has been changed while performing transmission of groupcast mode V2X communication over PC5, as described in subclause 6.1.4.2.4. Upon T5030 expiration while performing transmission of groupcast mode V2X communication over PC5, as described in subclause 6.1.3.2.4.	Upon stopping transmission of groupcast mode V2X communication over PC5, as described in subclause 6.1.3.2.4.	Change the value of the source layer-2 ID self-assigned by the UE for groupcast mode V2X communication over PC5. If the V2X message contains IP data, change the value of the source IP address self-assigned by the UE for groupcast mode V2X communication over PC5.

NOTE 1 The value of this timer is the privacy timer value which is one of the configuration parameters for V2X communication over PC5 (see clause 5.2),

Annex A (informative): Change history

Change history							
Date	**Meeting**	**Tdoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-05	CT1#117	C1-193474				Draft skeleton provided by the rapporteur.	0.0.0
2019-05	CT1#117	C1-193475				Implementing the following p-CR agreed by CT1: C1-193475	0.1.0
2019-08						Specification number added	0.1.1
2019-09	CT1#119					Implementing the following p-CRs agreed by CT1: C1-194852, C1-194855, C1-194856, C1-194857, C1-195046, C1-195947, C1-195048	0.2.0
2019-10	CT1#120					Implementing the following p-CRs agreed by CT1: C1-196377, C1-196379, C1-196621, C1-196762, C1-196861, C1-196862, C1-196863, C1-196864	0.3.0
2019-11	CT1#121					Implementing the following p-CRs agreed by CT1: C1-198358, C1-198632, C1-198634, C1-198636, C1-198817, C1-198821, C1-198823 Corrections done by the rapporteur.	0.4.0
2019-12	CT#86	CP-193156				Version 1.0.0 created for presentation to TSG CT#86 for information. Editorials fixed.	1.0.0
2019-12	CT#86	CP-193289				A title corrected	1.0.1
2020-03	CT1#122-e					Implementing the following p-CRs agreed by CT1: C1-200325, C1-200385, C1-200387, C1-200389, C1-200391, C1-200821, C1-200824, C1-200825, C1-200826, C1-200844, C1-200845, C1-200899, C1-200900, C1-200907, C1-200909, C1-200934, C1-200935, C1-201015, C1-201016, C1-201017, C1-201028 Corrections done by the rapporteur.	1.1.0
2020-03	CT-87e	CP-200173				Version 2.0.0 created for presentation to TSG CT#87e for approval	2.0.0
2020-03	CT-87e					Version 16.0.0 created after approval	16.0.0
2020-06	CT-88e	CP-201117	0001		F	Incorrect reference	16.1.0
2020-06	CT-88e	CP-201117	0002	3	B	PC5 unicast link security establishment	16.1.0
2020-06	CT-88e	CP-201117	0003	1	B	NR PC5 unicast security policy provisioning	16.1.0
2020-06	CT-88e	CP-201117	0004	3	B	PC5 unicast link re-keying procedure	16.1.0
2020-06	CT-88e	CP-201117	0005	3	B	Adding general subclause on security of PC5 signalling messages	16.1.0
2020-06	CT-88e	CP-201117	0007	1	F	Add the missing figure for UE-requested V2X policy provisioning procedure	16.1.0
2020-06	CT-88e	CP-201117	0009	1	F	Non-standardized QoS characteristics over PC5-S	16.1.0
2020-06	CT-88e	CP-201117	0010	2	F	Remove FFS on GFBR and MFBR for UL and DL	16.1.0
2020-06	CT-88e	CP-201117	0011	3	F	Group size and member ID from application layer for groupcast	16.1.0
2020-06	CT-88e	CP-201117	0012	1	F	Clarifications on configuration parameters for the PC5 QoS profile	16.1.0
2020-06	CT-88e	CP-201117	0013	2	F	Handling of link establishment accept	16.1.0
2020-06	CT-88e	CP-201117	0014	1	F	Handling of the link modification accept	16.1.0
2020-06	CT-88e	CP-201117	0015	4	F	ENs resolving in modification pocedure	16.1.0
2020-06	CT-88e	CP-201117	0016	1	F	Updates to the link release procedure	16.1.0
2020-06	CT-88e	CP-201117	0017	1	F	Correction of the timers of link identifier update procedure	16.1.0
2020-06	CT-88e	CP-201117	0018	3	F	Encoding of link identifier update messages and parameters	16.1.0
2020-06	CT-88e	CP-201117	0019	1	F	Handling of link identifier update not accept	16.1.0
2020-06	CT-88e	CP-201117	0020	4	F	Handling of PC5 unicast QoS flow match and establishment	16.1.0
2020-06	CT-88e	CP-201117	0021	8	F	Handling of PC5 broadcast QoS flow match and establishment	16.1.0
2020-06	CT-88e	CP-201117	0023	4	F	Timer values for timers of PC5 unicast link management procedures	16.1.0
2020-06	CT-88e	CP-201117	0024	2	F	Correction to the privacy timer	16.1.0
2020-06	CT-88e	CP-201117	0025	3	F	Correction for the target user info in the DIRECT LINK ESTABLISHMENT REQUEST message	16.1.0
2020-06	CT-88e	CP-201117	0026	1	F	Correction for the IP address configuration IE in the DIRECT LINK ESTABLISHMENT ACCEPT message	16.1.0
2020-06	CT-88e	CP-201117	0027	1	F	Correction for the link local IPv6 address IE in the DIRECT LINK ESTABLISHMENT ACCEPT message	16.1.0
2020-06	CT-88e	CP-201117	0028	6	F	Defining new parameters needed for the Link Identifier Update procedure	16.1.0
2020-06	CT-88e	CP-201117	0029	2	C	Maximum number of NR PC5 unicast links for a UE	16.1.0
2020-06	CT-88e	CP-201117	0031		F	Resolution of editor's note under 5.2.3	16.1.0
2020-06	CT-88e	CP-201117	0032		F	Resolution of editor's note under 6.1.2.5.2	16.1.0
2020-06	CT-88e	CP-201118	0033		F	Miscellaneous corrections	16.1.0
2020-06	CT-88e	CP-201118	0034	1	F	Resolution of editor's note under 6.1.2.3.6	16.1.0

2020-06	CT-88e	CP-201118	0035	1	F	Resolution of editor's notes under 6.1.2.5.7.2	16.1.0
2020-06	CT-88e	CP-201118	0036	1	F	Correction on conditions to initiate a PC5 unciast link establishment procedure	16.1.0
2020-06	CT-88e	CP-201118	0037	1	C	Packet filter for PC5 QoS flows	16.1.0
2020-06	CT-88e	CP-201118	0039	1	C	Correction of configuration of PC5 RAT selection and Tx profiles	16.1.0
2020-06	CT-88e	CP-201118	0040	1	F	Correction of configuration of default mode of communication	16.1.0
2020-06	CT-88e	CP-201118	0041	1	F	Correction of PC5 RAT names	16.1.0
2020-06	CT-88e	CP-201118	0042	1	F	Correction of PC5 QoS mapping configuration	16.1.0
2020-06	CT-88e	CP-201118	0043		F	Served by E-UTRAN	16.1.0
2020-06	CT-88e	CP-201118	0044	1	F	Editor's note on security of V2X over Uu	16.1.0
2020-06	CT-88e	CP-201118	0045		F	Editor's note on PDU session establishment for V2X over Uu	16.1.0
2020-06	CT-88e	CP-201118	0047		F	Adding new definitions to 24.587	16.1.0
2020-06	CT-88e	CP-201118	0048	3	F	Modification of the Link Release procedure	16.1.0
2020-06	CT-88e	CP-201118	0050		F	Encoding of link modification reject message	16.1.0
2020-06	CT-88e	CP-201118	0051	1	F	Alignment of the name of cause#5	16.1.0
2020-06	CT-88e	CP-201118	0052	1	F	Handling of link release procedure	16.1.0
2020-06	CT-88e	CP-201118	0053	1	F	Handling of PC5 unicast link ID update accept	16.1.0
2020-06	CT-88e	CP-201118	0054	1	F	Handling of PC5 unicast link ID update accept	16.1.0
2020-06	CT-88e	CP-201118	0060		F	Change the term "service authorisation provisioning"	16.1.0
2020-06	CT-88e	CP-201118	0061	1	F	Abnormal case of link release including Knrp ID	16.1.0
2020-06	CT-88e	CP-201118	0062		C	Huawei, HiSilicon	16.1.0
2020-06	CT-88e	CP-201118	0063	1	C	Addition of function for converting the group identifier to the destination Layer-2 ID	16.1.0
2020-06	CT-88e	CP-201118	0064		C	Updates to link modification procedure	16.1.0
2020-06	CT-88e	CP-201118	0065	1	C	Updates to NR PC5 unicast link release procedure	16.1.0
2020-06	CT-88e	CP-201118	0066	1	B	Mapping between V2X Service ID and PFI for a PC5 unicast link establishment	16.1.0
2020-06	CT-88e	CP-201118	0067	1	B	Updating PC5 unicast link modification procedure	16.1.0
2020-06	CT-88e	CP-201118	0068	1	F	Adding the new V2X message family	16.1.0
2020-07	CT-88e					Editorial corrections and addition of IEI values by rapporteur	16.1.1
2020-09	CT-89e	CP-202199	0069	2	F	PC5 unicast security policy determination based on more than one V2X service	16.2.0
2020-09	CT-89e	CP-202157	0070	1	F	Add a new trigger to link establishment due to V2X service with a conflicting security policy	16.2.0
2020-09	CT-89e	CP-202247	0071	3	F	Change configuration parameters over Uu to meet stage-2 requirements	16.2.0
2020-09	CT-89e	CP-202157	0072	1	F	Remove repeated communication mode in 6.1.1	16.2.0
2020-09	CT-89e	CP-202157	0073	2	F	UE in limited service state for unicast	16.2.0
2020-09	CT-89e	CP-202157	0074		D	Add the missing abbreviation	16.2.0
2020-09	CT-89e	CP-202157	0075		F	UE PC5 unicast signalling security policy	16.2.0
2020-09	CT-89e	CP-202157	0076		F	Knpr ID and Knpr-sess ID	16.2.0
2020-09	CT-89e	CP-202157	0077	1	F	Privacy timer of Layer-2 ID for groupcast and broadcast	16.2.0
2020-09	CT-89e	CP-202157	0078		F	Correction of QoS flow descriptions IE	16.2.0
2020-09	CT-89e	CP-202194	0079	3	F	Addition of “Privacy timer”	16.2.0
2020-09	CT-89e	CP-202157	0080	2	F	Corrections to the Link Identifier Update procedure and messages	16.2.0
2020-09	CT-89e	CP-202157	0081	1	F	Handling of T5003	16.2.0
2020-09	CT-89e	CP-202157	0082		D	Correction to the normal stop of T5009	16.2.0
2020-09	CT-89e	CP-202157	0084		F	Privacy timer for groupcast	16.2.0
2020-09	CT-89e	CP-202157	0085	1	F	Reflect the V2X service id in the accept message	16.2.0
2020-09	CT-89e	CP-202157	0086	1	F	Updates to the handling of broadcast	16.2.0
2020-09	CT-89e	CP-202157	0087	1	F	Updates to the link release	16.2.0
2020-09	CT-89e	CP-202157	0088		F	Correction to PC5 unicast link security mode control procedure	16.2.0
2020-09	CT-89e	CP-202157	0089	1	F	Clarification on integrity protection and ciphering of PC5 signalling and user plane	16.2.0
2020-09	CT-89e	CP-202158	0091		F	Correction to requirements for V2X communication	16.2.0
2020-09	CT-89e	CP-202158	0092	1	D	Correcting editorial errors on Key parameter name	16.2.0
2020-09	CT-89e	CP-202158	0093		B	Inconsistent security policy during PC5 unicast link modification procedure	16.2.0
2020-09	CT-89e	CP-202158	0094	1	C	Removal of Abnormal cases in the target UE	16.2.0
2020-09	CT-89e	CP-202158	0098	2	F	Indication of security protection activation	16.2.0
2020-09	CT-89e	CP-202158	0099	1	F	Miscellaneous corrections	16.2.0
2020-09	CT-89e	CP-202158	0100	2	F	Resolution of editor's notes under clause 6.1.2.2.1	16.2.0

2020-09	CT-89e	CP-202158	0102	1	F	Correction on Timers	16.2.0
2020-09	CT-89e	CP-202158	0105	1	F	PC5 unicast link release due to RLF from lower layer	16.2.0
2020-09	CT-89e	CP-202158	0106	1	F	Removal of resolved ENs for PC5 unicast security	16.2.0
2020-09	CT-89e	CP-202158	0107	1	F	Value of the timers T5009 and T5010	16.2.0
2020-09	CT-89e	CP-202158	0108	1	F	Correction to the values of the timers which control the PC5 unicast link authentication procedure timer and the PC5 unicast link security mode control procedure	16.2.0
2020-09	CT-89e	CP-202158	0109		F	Resolution of the editor's note under clause 8.4.1	16.2.0
2020-09	CT-89e	CP-202158	0110	2	F	Allocation of IEIs	16.2.0
2020-09	CT-89e	CP-202037	0113	2	F	Radio parameters for UE neither served by E-UTRA nor served by NR	16.2.0
2020-09	CT-89e	CP-202158	0114	1	F	Encoding for direct link establishment reject message	16.2.0
2020-09	CT-89e	CP-202238	0115	2	F	Correction to V2X communication over Uu between the UE and the application server	16.2.0
2020-09	CT-89e					Editorial corrections by rapporteur	16.2.1

History

Document history		
V16.1.1	August 2020	Publication
V16.2.1	October 2020	Publication