ETSI TS 133 536 V16.0.0 (2020-07)

LTE;
5G;
Security aspects of 3GPP support
for advanced Vehicle-to-Everything (V2X) services
(3GPP TS 33.536 version 16.0.0 Release 16)

Reference
DTS/TSGS-0333536vg00

Keywords
5G,LTE,SECURITY

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, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

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

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

The constructions "can" and "cannot" are not 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

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document provides the security aspects for the 5G system to facilitate vehicular communications for Vehicle-to-Everything (V2X) services. The architecture for these V2X services is described in TS 23.287 [2], which is based on the service requirements defined in TS 22.185 [3] and TS 22.186 [4].

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

[3] 3GPP TS 22.185: "Service requirements for V2X services; Stage 1".

[4] 3GPP TS 22.186: "Service requirements for enhanced V2X scenarios".

[5] 3GPP TS 33.185: "Security aspect for LTE support of Vehicle-to-Everything (V2X) services".

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[7] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[8] 3GPP TS 24.587: "Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3".

[9] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

Void

3.2 Symbols

Void

3.3 Abbreviations

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

5GC 5G Core

NR	New Radio (5G)
NRPEK	NR PC5 Encryption Key
NRPIK	NR PC5 Integrity Key
V2X	Vehicle-to-Everything

4 Overview of advanced V2X security architecture

4.1 General

The V2X architecture is described in TS 23.287 [2] which describes V2X communication over both the Uu reference point supported by E-UTRA connected to 5GC and/or NR connected to 5GC and PC5 reference point supported by E-UTRA and/or NR. The NR based PC5 reference point supports unicast, groupcast and broadcast modes (see TS 23.287 [2]).

The security for PC5 reference point supported by E-UTRA is given in TS 33.185 [5]. The security for the other cases is given in the present document.

5 Security for V2X over NR based PC5 reference point

5.1 General

This clause contains the security and privacy requirements and specifies procedures that can achieve the requirements for V2X over NR based PC5 reference point except those for PC5 over E-UTRA which are given in TS 33.185 [5].

5.2 Common security

5.2.1 General

This clause describes the security requirements and the procedures that are commonly applied for the all kinds of communication modes, i.e. unicast mode, groupcast mode and broadcast mode, which the NR based PC5 reference point supports.

5.2.2 Requirements

5.2.2.1 Requirements for Cross-RAT control authorization indication

The 5G System shall provide means to manage the cross-RAT PC5 control authorization.

5.2.3 Procedures

5.2.3.1 Cross-RAT PC5 control authorization indication

The procedures for the cross-RAT PC5 control authorization indication are specified in TS 23.287 [2] clause 6.5.

5.3 Security for unicast mode

5.3.1 General

This clause describes the security requirements and the procedures that can be specifically applied for the NR based PC5 unicast mode.

5.3.2 Requirements

5.3.2.1 Requirements for securing the PC5 unicast link

The initiating UE shall establish a different security context for each receiving UE during the PC5 unicast link establishment if the security is activated.

PC5 unicast link security establishment between the initiating UE and each receiving UE shall be protected from man-in-the-middle attacks.

The system shall support confidentiality protection, integrity protection and replay protection of the user plane data of PC5 unicast.

The system shall support confidentiality protection, integrity protection and replay protection of signalling for PC5 unicast link.

The system shall support means of configuring the signalling and user plane security policies to UEs for a particular PC5 unicast link.

Signalling plane protection of the PC5 unicast link for a V2X service shall align with the PC5 signalling security policies of the communicating UEs.

User plane protection of the PC5 unicast link for a V2X service shall align with the PC5 user plane security policies of the communicating UEs.

5.3.2.2 Identity privacy requirements for the PC5 unicast link

The 5G System should provide means for mitigating trackability attacks on a UE during PC5 unicast communications.

The 5G System should provide means for mitigating link ability attacks on a UE during PC5 unicast communications.

NOTE: The 5G system provides means for mitigating trackability and link ability if security of the connection is activated.

5.3.3 Procedures

5.3.3.1 Securing the PC5 unicast link

5.3.3.1.1 General

The NR based PC5 unicast communication procedures are described in TS 23.287 [2]. Clause 5.3.3.1 details how the security for this communication is established and used.

5.3.3.1.2 Overview

5.3.3.1.2.1 Key hierarchy

PC5 unicast link uses 4 different layers of keying material as shown in figure 5.3.3.1.2.1-1.

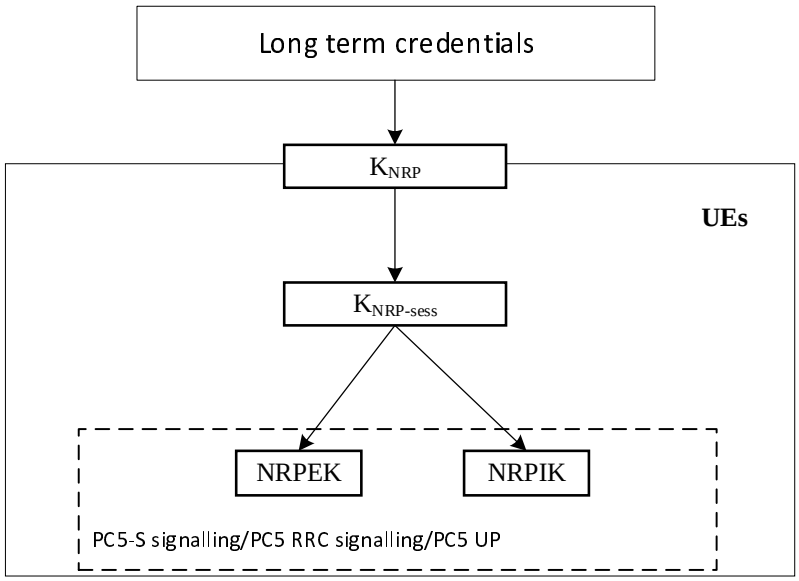

Figure 5.3.3.1.2.1-1: Key Hierarchy for PC5 unicast link

The different layers of keys are the following:

- Long term credentials: These are the credentials that are provisioned into the UE(s) and form the root of the security of the PC5 unicast link. The credentials may include symmetric key(s) or public/private key pair depending on the particular use case. Authentication signalling (see clause 5.3.3.1.3.2) is exchanged between the UEs to derive the K_{NRP}.

- K_{NRP}: This is a 256-bit root key that is shared between the two entities that communicating using NR PC5 unicast link. It may be refreshed by re-running the authentication signalling using the long-term credentials. In order to generate a $K_{NRP-sess}$ (the next layer of keys), nonces are exchanged between the UEs. K_{NRP} may be kept even when the UEs have no active unicast communication session between them. The K_{NRP} ID is used to identify $K_{NRP.}$

- $K_{NRP-sess}$: This is the 256-bit key that is the root of the actual security context that is being used (or at least in the process of being established) to protect the transfer of data between the UEs. During activated unicast communication session between the UEs, the $K_{NRP-sess}$ may be refreshed by running the rekeying procedure. The actual keys (see next bullet) that are used in the confidentiality and integrity algorithms are derived directly from $K_{NRP-sess}$. The 16-bit $K_{NRP-sess}$ ID identifies the $K_{NRP-sess}$.

NOTE 1: A $K_{NRP-sess}$ ID with a zero value indicates no security is used and hence the UEs do not assign an all zero value of $K_{NRP-sess}$ ID when creating a security context.

- NRPEK and NRPIK: The NR PC5 Encryption Key (NRPEK) and NR PC5 Integrity Key (NRPIK) are used in the chosen confidentiality and integrity algorithms respectively for protecting PC5-S signalling, PC5 RRC signalling, and PC5 user plane data. They are derived from $K_{NRP-sess}$ and are refreshed automatically every time $K_{NRP-sess}$ is changed.

NOTE 2: Whether the above keys (i.e. KNRP, KNRP-sess, NRPEK and NRPIK) are derived is based on the security activation result of the signalling and user plane security.

5.3.3.1.2.2 Security states

A UE may be in one of the three different security states with respect to another UE as follows:

- Provisioned-security: This is where a UE just has its own long term keys.

- Partial-security: This is where a UE has recently communicated with another UE and still has the K_{NRP} that it used with the other UE, but no other derived keys.

- Full-security: This is where a UE is actually communicating with another UE and has K_{NRP}, $K_{NRP-sess}$, NRPEK (if applicable) and NRPIK, the chosen confidentiality (if applicable) and integrity algorithms and PDCP counters used with each bearer. The NRPEK and the chosen confidentiality algorithm may not exist if both signalling and user plane confidentiality are inactivated.

Once a UE ends its unicast communication session with another UE in Full-security state, it shall delete $K_{NRP-sess}$, NRPEK, and NRPIK, the choice of algorithms and the counters. It may also delete K_{NRP}.

5.3.3.1.2.3 High level flows for the security establishment

Figure 5.3.3.1.2.3-1 provides a high-level flow of a UE establishing a connection with other UE(s).

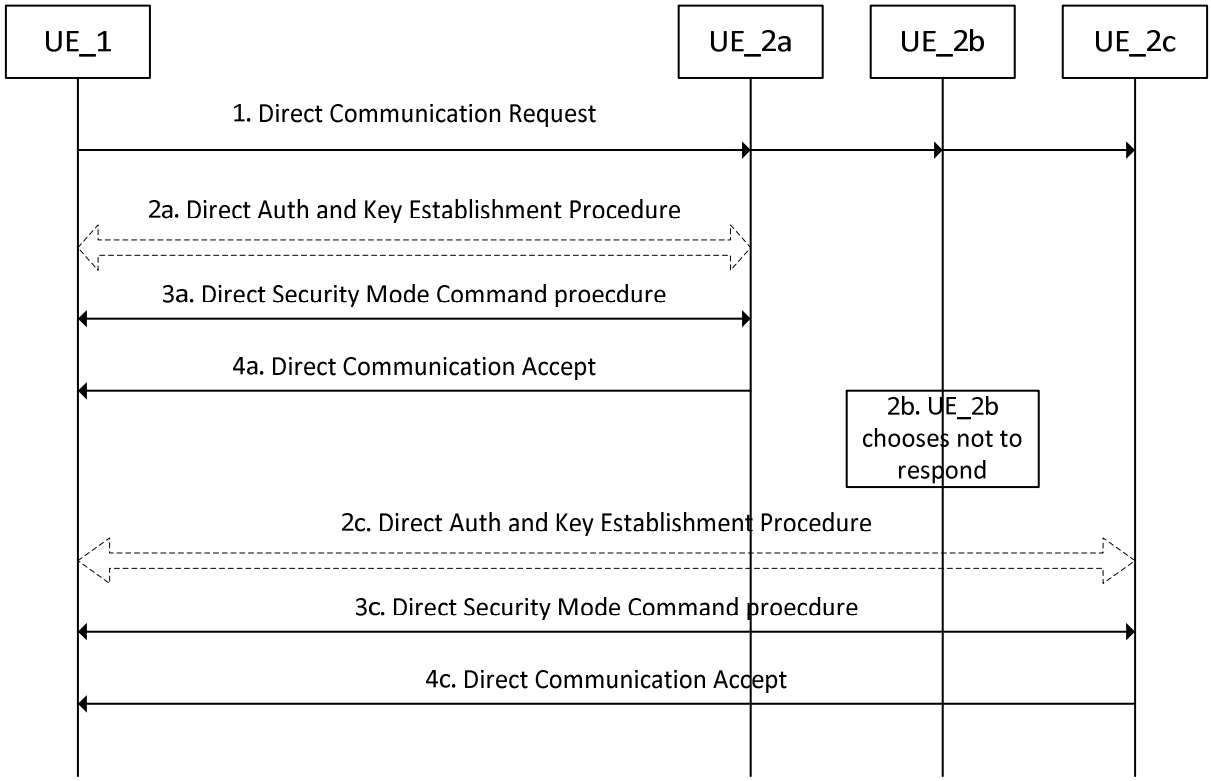

Figure 5.3.3.1.2.3-1: High-level flow of connection establishment

The flow proceeds as follow:

1. UE_1 sends a Direct Communication Request. This message may be received by multiple UEs.

2a/3a/4a. UE_2a choose to respond to the message and may initiate the Direct Auth and Key Establishment procedure (if needed based clause 5.3.3.1.3) to generate the key K_{NRP}. UE_2a then runs the Direct Security Mode Command procedure with UE_1 to continue the connection establishment procedures. If this is successful, UE_2a sends the Direct Communication Accept message.

2b. UE_2b chooses not to respond the UE_1

2c/3c/4c. UE_2c responds to UE_1 using the same sequence of messages as UE_2a.

When each responder decides to activate signalling integrity protection and/or signalling confidentiality protection, each responder establishes a different security context with UE_1 that is not known to the other UEs, i.e. the security context used between UE_1 and UE_2a is not known to UE_2b and UE_2c.

The Direct Communication Request is always sent unprotected and only contains enough information for a secure connection to be established with the other UE. Any information UE_1 needs to send to the other UEs in order to establish the connection is included in the Direct Security Mode Complete message (sent as part of the Direct Security Mode procedure, see TS 23.287 [2]) from UE_1 as this message is both confidentiality and integrity protected under the condition of activated non-NULL signalling confidentiality protection of the link.

5.3.3.1.3 Key establishment procedures

5.3.3.1.3.1 General

Clause 5.3.3.1.3 provides the details on the establishment of K_{NRP}. The key establishment procedures in this clause shall be skipped if signalling integrity protection is not activated based on the decision of receiving UE of this PC5 unicast link. The long-term credentials and associated authentication method that are used to establish the keys used to protect the PC5 unicast link may either be specified in 3GPP specification or be a method described outside of 3GPP specifications. In the latter case, it is not practical for all cases to specify the signalling in individual IEs on the NR PC5 interface for all these applications, hence all the authentication is specified to be carried in a generic container (called Key_Est_Info in the following clause) on the NR PC5 interface. This allows, for example, an application to change the authentication method without affecting the NR PC5 interface.

5.3.3.1.3.2 Key establishment

At each step of the flow (and the possible multiple times that step 2 can be run), the Key_Est_Info contains the different data that is required for key establishment. Such data is transparent to the PC5 layer, i.e. the PC5 layer does not need to understand the content of Key_Est_info.

NOTE: The endpoint in the UEs that understands the contents of Key_Est_Info may be an application on the UEs. Between the PC5 layer and the application layer on the vehicles, the information contained in Key_Est_Info can be passed in an implementation-specific manner, e.g. as one block or several IEs.

Figure 5.3.3.1.3.2-1 shows the message flows for establishing security at PC5 using the key established at the layer above PC5. The need for both steps 2a and 2b (and the number of times both steps 2a and step 2b are run) depends on the authentication method being used.

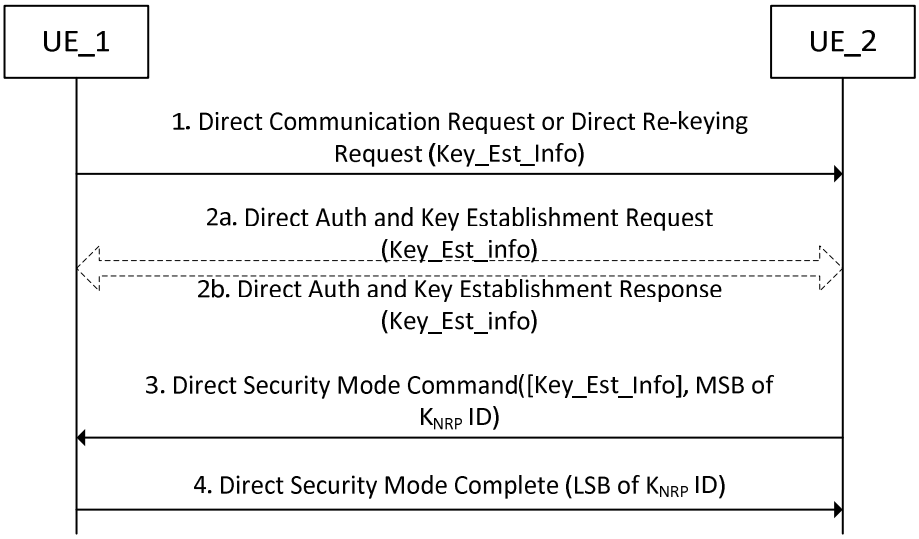

Figure 5.3.3.1.3.2-1: Message flow for the establishment of PC5 security key using a generic container

The steps are as follows and apply to establishment of the initial key or rekeying:

1. In the case, UE_1 determines it needs to establish a PC5 connection with another UE, UE_1 sends the Direct Communication Request message and this message is received by UE_2. In case of rekeying an existing connection with UE_2, UE_1 shall send a Direct Rekeying Request message to UE_2 instead of Direct Communication Request. The Direct Communication Request message shall include the Key_Est_Info unless UE_1's signalling integrity security policy is NOT NEEDED. In the former case, the message may include Key_Est_Info. The Direct Rekeying Request message shall include Key_Est_Info unless the Null integrity algorithm is currently in use.

2. This step is optional and may be run multiple times depending on the authentication method used.

   a. UE_2 shall send a Direct Auth and Key Establish message including the Key_Est_Info to UE_1.

b. UE_1 shall send respond with a Direct Auth and Key Establish Response message including the Key_Est_Info to UE_2.

3. UE_2 shall calculate (if not already done) K_{NRP}. UE_2 shall send a Direct Security Mode Command messages to UE_1. These messages may include Key_Est_Info if need by the authentication method being used and shall contain MSB of K_{NRP} ID. The MSB of K_{NRP} ID are chosen so that they uniquely identify K_{NRP} at UE_2.

4. On receiving the Direct Security Mode Command, UE_1 shall calculate (if not already done) K_{NRP} based on Key_Est_Info (if provided). UE_1 shall choose the LSB of K_{NRP} ID so that they uniquely identify K_{NRP} at UE_1. UE_1 shall form K_{NRP} ID from the received MSB of K_{NRP} ID and its chosen LSB of K_{NRP} ID and shall store the complete K_{NRP} ID with K_{NRP}.

UE_1 shall send a Direct Security Mode Complete message to UE_2 which shall contain the LSB of K_{NRP} ID. UE_2 shall form K_{NRP} ID from its chosen MSB of K_{NRP} ID and the received LSB of K_{NRP} ID and shall store the complete K_{NRP} ID with K_{NRP}.

5.3.3.1.4 Security establishment procedures

5.3.3.1.4.1 General

Clause 5.3.3.1.4.2 describes the security policy and how the UEs handle the policy. There are two different cases when an overall security context may be established; to set up a new connection and to re-key an ongoing connection. These cases are described in clauses 5.3.3.1.4.3 and 5.3.3.1.4.4 respectively. Clause 5.3.3.1.4.5 describes the establishment of security for a user plane bearer.

5.3.3.1.4.2 Security policy

5.3.3.1.4.2.1 General

The PC5 unicast link shall support activation or deactivation of security based on the security policy similar to Uu, as defined in TS 33.501[6]. The security policy shall be provisioned for PC5 unicast link as well, as detailed in clause 5.3.3.1.4.2.2 of the present document and handled as detailed in clause 5.3.3.1.4.2.3 of the present document.

5.3.3.1.4.2.2 Procedure for security policy provisioning for PC5 unicast link

For selectively activating or deactivation the security of the PC5 unicast link, the PCF may provision the security policy per V2X service, during service authorization and information provisioning procedure as defined in TS 23.287 [2].

5.3.3.1.4.2.3 Security policy handling

For a NR PC5 unicast link, the UE shall be provisioned with the following:

- The list of V2X services, e.g. PSIDs or ITS-AIDs of the V2X applications, with Geographical Area(s) and their security policy which indicates the following:
  - Signalling integrity protection: REQUIRED/PREFERRED/NOT NEEDED
  - Signalling confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED
  - User plane integrity protection: REQUIRED/PREFERRED/NOT NEEDED
  - User plane confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED

NOTE 1: No integrity protection on signalling traffic enables services that do not require security.

NOTE 2: Ensuring that only a connection with security is used for a V2X service is guaranteed if the signalling integrity security policy of at least one of the UEs for that V2X service is set to REQUIRED. It is recommended to set this security policy to REQUIRED in order to guarantee security protection.

NOTE 3: While some V2X applications are similar to Emergency Services and may require similar security policies handling, such V2X applications are outside of the scope of 3GPP.

REQUIRED means the UE shall only accept the connection if a non-NULL confidentiality or integrity algorithm is used for protection of the traffic.

NOT NEEDED means that the UE shall only establish a connection with no security.

PREFFERED means that the UE may try to establish security but may will accept the connection with no security. One use of PREFERRED is to enable a security policy to be changed without updating all UEs at once.

The handling of signalling security policy proceeds as follows:

- At initial connection, the initiating UE includes its signalling security policy in the Direct Communication Request message. The receiving UE(s) takes this into account when deciding whether to accept or reject the request and when deciding the agreed security policy to be sent back in the Direct Security Mode Command message. The initiating UE can reject the Direct Security Mode Command if the algorithm choice does not match its policy (see clause 5.3.3.1.4.3 for full details of the handling).

All the UP data of PC5 unicast link shall have the same security.

The handling of the user plane security policy proceeds as follows:

- At initial connection, the UE that sent the Direct Communications Request shall include the user plane security policy for the service in the Direct Security Mode Complete message.

- The receiving UE shall reject the Direct Communication Request when the following cases occur: 1) if the received user plane security policy had either confidentiality/integrity set to NOT NEEDED and its own corresponding policy is set to REQUIRED or, 2) if the received user plane security policy had either confidentiality/integrity set to REQUIRED and its own corresponding policy is set to NOT NEEDED.

- Otherwise, the receiving UE may accept the Direct Communication Request and the response message shall include the configuration of user plane confidentiality protection based on the agreed user plane security policy, set as follows:

    1) User plane confidentiality protection set to off if the received user plane security policy had either confidentiality set to NOT NEEDED and/or its own user plane security policy for the service is set to NOT NEEDED; or

    2) User plane confidentiality protection set to on if the received user plane security policy had either confidentiality set to REQUIRED and/or its own user plane security policy for the service its own corresponding policy is set to REQUIRED; or

    3) User plane confidentiality protection set to off or on otherwise (i.e. when both the received user plane security policy and its own user plane security policy for the service had the confidentiality set to PREFERRED).

User plane integrity protection set following the same rules as confidentiality protection but based on the received and its own user plane integrity protection policy for the service.

At link modification for adding a new V2X service to an existing PC5 unicast link, if the signalling and user plane security policies of the new V2X service are satisfied by the security in use for the PC5 unicast link, the initiating UE shall send the Link Modification Request to the receiving UE. The receiving UE shall reject the Link Modification Request if the security in use does not match its signalling and user plane security policies for the new V2X service.

The V2X layer of the UE shall pass the security configurations to its AS layer. The security configurations are mutually agreed by both sides' UEs, including the configuration of confidentiality and integrity protection.

5.3.3.1.4.3 Security establishment during connection set-up

The clause describes how security is established during connection set-up. The signalling flow is shown in figure 5.3.3.1.4.3-1.

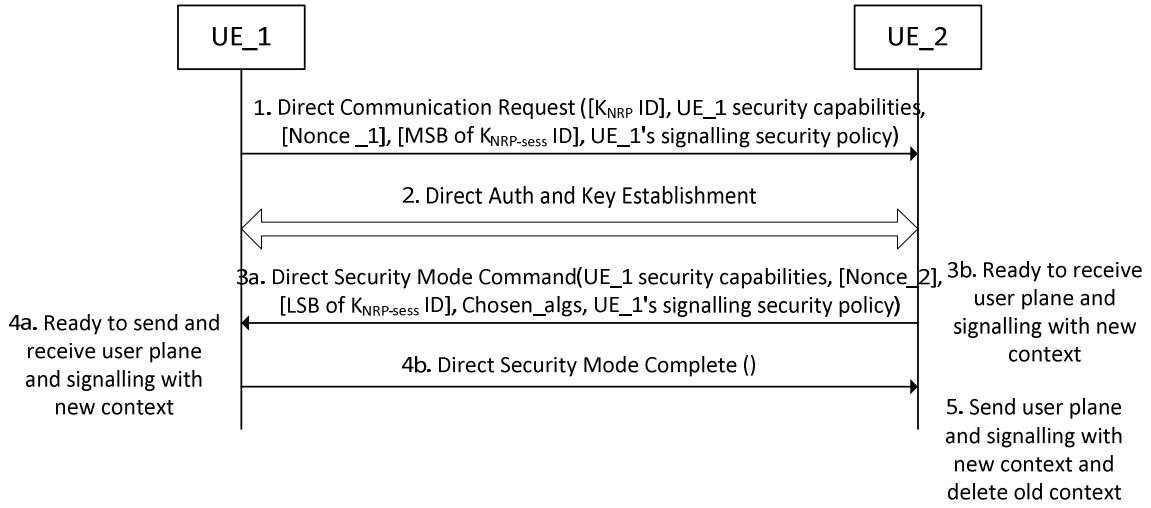

Figure 5.3.3.1.4.3-1: Security establishment at connection set-up

1. UE_1 has sent a Direct Communication Request to UE_2. This message shall include UE_1's security capabilities (the list of algorithms that UE_1 will accept for this connection) and UE_1's signalling security policy. The UE_1 shall also include Nonce_1 (for session key $K_{NRP\text{-}sess}$ generation), and the most significant 8-bits of the $K_{NRP\text{-}sess}$ ID in this message if UE_1's signalling integrity protection policy is either "REQUIRED" or "PREFERRED". The most significant 8-bits of the $K_{NRP\text{-}sess}$ ID shall be chosen such that UE_1 will be able to locally identify a security context that is created by this procedure. The message may also include a K_{NRP} ID if the UE_1 has an existing K_{NRP} for the UE that it is trying to communicate with. The absence of the K_{NRP} ID parameter indicates that UE_1 does not have a K_{NRP} for UE_2. The message also contains Key_Est_Info (see clause 5.3.3.1.3.2).

2. UE_2 shall reject the Direct Communication Request if UE_1's signalling security policy is "NOT NEEDED" while UE_2's security policy is "REQUIRED". UE_2 shall also reject the Direct Communication Request if UE_1's signalling security policy is "REQUIRED" while UE_2's security policy is "NOT NEEDED". UE_2 may initiate a Direct Auth and Key Establish procedure with UE_1. This is mandatory if the UE_2 does not have the K_{NRP} and K_{NRP} ID pair indicated in step 1, and signalling is needed to establish the keys for the particular use case.

3. UE_2 shall send the Direct Security Mode Command message to UE_1. This message shall only contain the MSB and of K_{NRP} ID and optionally Key_Est_Info if a fresh K_{NRP} is to be generated (see clause 5.3.3.1.3). UE_2 shall include the Chosen_algs parameter to indicate which security algorithms the UEs will use to protect the data in the message. The Chosen-algs may only indicate the use of the NULL integrity algorithm if UE_2's signalling integrity security policy is either NOT NEEDED or PREFERRED. UE_2 shall also return the UE_1's security capabilities and UE_1's signalling security policy to provide protection against bidding down attacks. In the case that the NULL integrity algorithm is chosen, the NULL confidentiality algorithm shall also be chosen and UE_2 shall set the $K_{NPR\text{-}sess}$ ID of this security context to the all zero value.

   The following procedures in step 3 shall only be executed if the UE_2 decides to at least activate the integrity security protection for this connection: UE_2 shall also include Nonce_2 to allow a session key to be calculated, as well as the least significant 8-bits of $K_{NRP\text{-}sess}$ ID in the messages. These bits are chosen so that UE_2 will be able to locally identify a security context that is created by this procedure. UE_2 shall calculate $K_{NRP\text{-}Sess}$ from K_{NRP} and both Nonce_1 and Nonce_2 (see clause A.3) and then derive the confidentiality (if applicable) and integrity keys based on the chosen algorithms (clause A.2). UE_2 shall integrity protect the Direct Security Mode Command before sending it to UE_1. UE_2 is then ready to receive both signalling and user plane traffic protected with the new security context. UE_2 shall form the $K_{NRP\text{-}sess}$ ID from the most significant bits it received in step1 and least significant bits it sent in step3.

4. On receiving the Direct Security Mode Command, the UE_1 shall first check the Chosen_algs and shall accept the NULL integrity algorithm only if its security policy for signalling integrity protection is either NOT NEEDED or PREFERRED. Then UE_1 shall check the returned UE_1's security capabilities and UE_1's signalling security to avoid bidding down attacks if NULL integrity algorithm is selected for signalling integrity protection. If the above check passes, UE_1 shall send unprotected Direct Security Mode Complete message to UE_2. UE_1 shall set the $K_{NPR\text{-}sess}$ ID of this security context to the all zero value.

Under the condition of non-NULL integrity algorithm indicated in the Chosen_algs, UE_1 shall first check that the received LSB of $K_{NPR\text{-}sess\ ID}$ is unique, i.e. has not been sent by another UE responding to this Direct Communication Request. If the LSB of $K_{NPR\text{-}sess}$ ID is not unique, then UE_1 shall respond with a Direct Security Mode Reject message including a cause value to specify that the LSB of $K_{NPR\text{-}sess}$ ID is not unique. The peer UE-2 receiving a Direct Security Mode Reject message shall inspect the cause value and, if the cause is related to the session identifier uniqueness then, the UE-2 shall generate a new LSB of $K_{NPR\text{-}sess}$ ID and reply to UE-1 again (i.e., UE-2 shall send a Direct Security Mode Command message with the new LSB of $K_{NPR\text{-}sess}$ ID). UE_2 shall associate the new LSB of $K_{NRP\text{-}sess}$ ID with the security context that is created in step 3. UE-2 shall erase the former LSB of $K_{NPR\text{-}sess}$ ID from its memory. On receiving this new Direct Security Mode Command, UE_1 shall process the message from the start of step 4.

If the LSB of $K_{NPR\text{-}sess}$ ID is unique, UE_1 shall calculate $K_{NRP\text{-}sess}$ and the confidentiality and integrity keys in the same way as UE_2. UE_1 shall check that the returned UE_1 security capabilities and UE_1's signalling security policy are the same as those it sent in step 1. UE_1 shall also check the integrity protection on the message. If both these checks pass, then UE_1 is ready to send and receive signalling and user plane traffic with the new security context. UE_1 shall send integrity protected and confidentiality protected Direct Security Mode Complete message to UE_2. UE_1 shall form the $K_{NRP\text{-}sess}$ ID from the most significant bits it sent in step1 and least significant bits it received in step3.

5. If the Chosen_algs in step 3 includes non-NULL integrity algorithm, UE_2 checks the integrity protection on the received Direct Security Mode Complete. If this passes, UE_2 is now ready to send user plane data and control signalling protected with the new security context. UE_2 deletes any old security context it has for UE_1.

5.3.3.1.4.4 Security establishment during re-keying

By rekeying, the UEs ensure fresh session keys $K_{NRP\text{-}sess}$ are used. Optionally the rekeying can also enforce refresh of K_{NRP}. Either UE may rekey the connection at any time. This shall be done before the counter for a PDCP bearer repeats with the current keys. A rekeying operation shall refresh the $K_{NRP\text{-}sess}$ and NRPEK and NRPIK, and may refresh K_{NRP}. There is no benefit in running the rekeying procedure if the NULL integrity algorithm is in use, hence it is recommended not to trigger it when using the NULL integrity algorithm. A rekeying operation follows the flows given in figure 5.3.3.1.4.4-1.

NOTE: The rekeying procedure is not required from security point of view if the connection is unprotected.

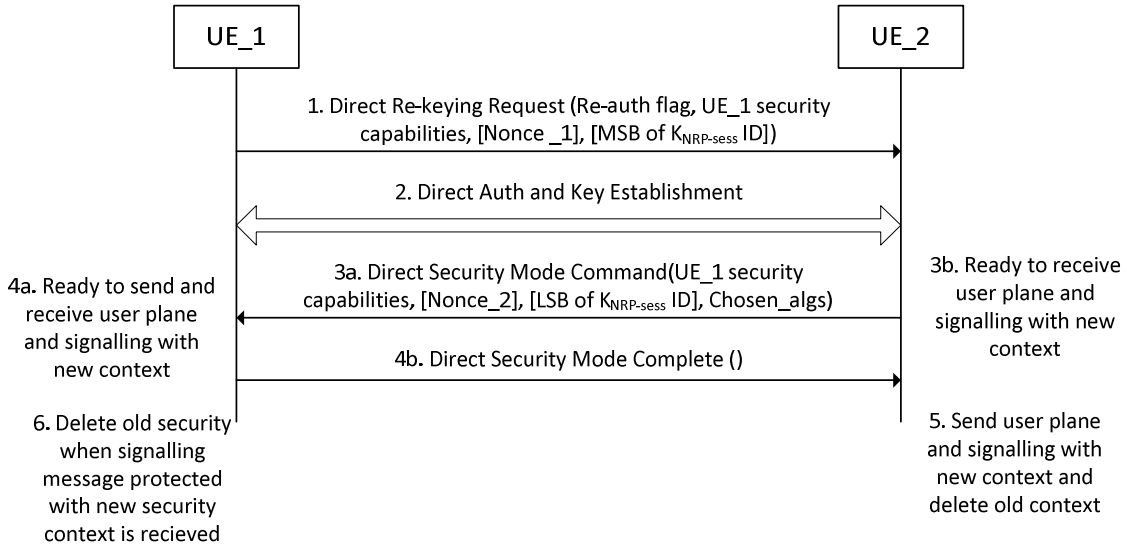

Figure 5.3.3.1.4.4-1: Security establishment during rekeying

1. UE_1 sends a Direct Rekey Request to UE_2. This message shall include UE_1 security capabilities (the list of algorithms that UE_1 will accept for this connection). In addition, if a non-Null integrity algorithm is in use, the message shall include Nonce_1 (for session key generation) and the most significant 8-bits of the $K_{NRP\text{-}sess\ ID}$. These bits are chosen such that UE_1 will be able to locally identify a security context that is created by this procedure. The message may also include a Re-auth Flag if UE_1 wants to rekey K_{NRP}. The message also contains Key_Est_Info (see clause 5.3.3.1.3.2).

2. UE_2 may initiate a Direct Auth Key Establish procedure with UE_1. This is mandatory if UE_1 included the Re-auth Flag and signalling is needed to establish $K_{NRP.}$

3. This step is the same as step 3 in clause 5.3.3.1.4.3 except that the chosen integrity algorithm shall only be NULL if and only if the NULL integrity algorithm is currently in use, the chosen confidentiality algorithm shall only be NULL if and only if the NULL confidentiality algorithm is currently in use and UE_1's signalling security policy is not included in this message.

4. This step is the same as step 4 in clause 5.3.3.1.4.3 except that UE_1 shall only accept the NULL integrity algorithm if and only if the NULL integrity algorithm is currently in use, UE_1 shall only accept the NULL confidentiality algorithm if and only if the NULL confidentiality algorithm is currently in use, and UE_1 does not check the returned signalling security policy (as it is not sent in this case).

5. This step is the same as step 5 in clause 5.3.3.1.4.3.

6. When UE_1 receives message integrity protected with the new security context, it shall delete any old security context it has still stored for UE_2.

5.3.3.1.4.5 Security establishment for user plane bearers

The UEs handle the user plane security policies as described in clauses 5.3.3.1.4.2.3.

The UE initiating the establishment of a user plane bearer shall select an LCID whose associated value of Bearer for input to the security algorithms (see clauses 5.3.3.1.5.2 and 5.3.3.1.5.3) has not been used with the current keys, NRPEK and NRPIK. If this is not possible the UE shall initiate a re-keying (see clause 5.3.3.1.4.4) before establishing the user plane bearer.

When establishing or re-configuring the user plane bearer, the initiating UEs shall ensure the configuration of confidentiality and integrity protection in the PC5-RRC message matches the agreed UP security policies for traffic that will be sent on the bearer. The confidentiality and/or integrity protection algorithms are same as those selected for protecting the signalling bearers if confidentiality and/or integrity protection are required for both signalling and user plane.

Both UEs shall ensure that the user plane for each V2X service is only sent or received (e.g. dropped if received on a bearer with incorrect security) on user plane bearers with the necessary security if security protection of this link is activated.

5.3.3.1.5 Protection of the PC5 unicast link

5.3.3.1.5.1 General

Protection for the signalling and user plane data between the UEs is provided at the PDCP layer. As the security is not preserved through a drop of the connection, all signalling messages that need to be sent before security is established for a connection may be sent with no protection. The PC5-S signalling messages that can be sent and processed unprotected are given in TS 24.587 [8]. Once security is established for a connection all signalling messages for that connection are sent integrity protected and confidentiality protected with the chosen algorithms except the Direct Security Mode Command which is sent integrity protected only.

5.3.3.1.5.2 Integrity protection

UEs shall implement NIA0, 128-NIA1 and 128-NIA2 and may implement 128-NIA3 for integrity protection of the unicast link. The algorithm identifiers from clause 5.11.1.2 of TS 33.501 [6] are reused for PC5-S, PC5-RRC, and PC5-U.

These integrity algorithms are as specified in TS 33.501 [6] and are reused with the following modifications:

- The key used is NRPIK;

- Direction is set to 1 for direct link signalling transmitted by the UE that sent the Direct Security Mode Command for this security context and 0 otherwise;

- Bearer[0] to Bearer[4] are set to 5 LSB of LCID;

- COUNT[0] to COUNT[31] are filled with counter value (see clause 6.3.5 of TS 38.323 [9]).

NOTE: The above input parameters do not apply to NIA0 as specified in Annex D.1 of TS 33.501 [6].

The receiving UE ensures that received protected signalling messages and user plane data that is integrity protected are not replayed.

5.3.3.1.5.3 Confidentiality protection

UEs shall implement NEA0, 128-NEA1 and 128-NEA2 and may implement 128-NEA3 for ciphering of the unicast link. The algorithm identifiers from clause 5.11.1.1 of TS 33.501 [6] are reused for PC5-S, PC5-RRC, and PC5-U.

These ciphering algorithms are as specified in TS 33.501 [6] and are used with the following modifications:

- The key used in NRPEK;
- Direction is set as for integrity protection (see 5.3.3.1.5.2);
- Bearer[0] to Bearer[4] are set to 5 LSB of LCID;
- COUNT[0] to COUNT[31] are filled with counter value.

NOTE: The above input parameters do not apply to NIA0 as specified in Annex D.1 of TS 33.501 [6].

5.3.3.1.5.4 Content of the PDCP packet

The Key ID and least significant bits of the counter are carried in the PDCP header, along with any MAC that is needed for integrity protection. The key ID is used to signal which security context is being used and shall be set to $K_{NRP\text{-}sess}$ ID.

This is illustrated in Figure 5.3.3.1.5.4-1.

$K_{NPR\text{-}sess}$ ID	LSBs of counter	Ciphered payload	Ciphered MAC (if required)

Figure 5.3.3.1.5.4-1: Security parameters in the PDCP header for NR based PC5 unicast mode

5.3.3.2 Identity privacy for the PC5 unicast link

5.3.3.2.1 General

The link identifier update procedure given in TS 23.287 [2] is used to provide privacy for the identities in the unicast link. This procedure only provides privacy if a non-NULL confidentiality algorithm is selected. This means the messages in this procedure are sent confidentiality protected (i.e. using a non-NULL confidentiality algorithm) and hence the new identities agreed by the UEs are only known to the involved UEs. A three-way message exchange procedure is required with this procedure since both UEs need to change their identifiers during the same procedure and to allow these new values to be acknowledged before them being used. This procedure is used to preserve the privacy for the identities that are seen in the clear for an ongoing unicast connection.

NOTE: From a security point of view, it is assumed that the link identifier update procedure is used with a protected connection.

A separate privacy threat that allows to link two subsequent connections is caused by either the same K_{NRP} ID or same partial K_{NRP} ID value being sent in the Direct Communication Request message for subsequent connections. The Layer-2 link release procedure given in TS 23.287 [2] is used to provide privacy for the K_{NRP} ID. The messages in the Layer-2 link release procedure are always sent protected and hence the new K_{NRP} ID agreed by the UEs is only known to the involved UEs.

5.3.3.2.2 Procedures

5.3.3.2.2.1 Link identifier update

Figure 5.3.3.2.2-1 shows the flows for changing the identities of the UEs involved in PC5 unicast link. The figure only displays the security parameters ($K_{NRP\text{-}sess}$ ID)that are changed and the Layer-2 IDs but not the other parameters described in TS 23.287 [2].

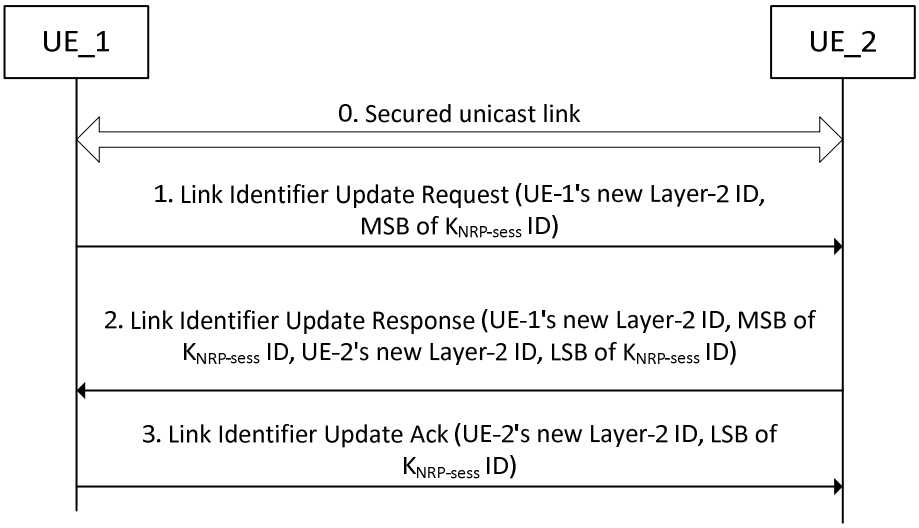

Figure 5.3.3.2.2.1-1: Link identifier update procedure

The procedure proceeds with the following steps and provides additional handling on top of what is provided in TS 23.287 [2].

0. UE_1 and UE_2 are communicating via a unicast link and have established the security for the link.

1. UE_1 decides to change its identifiers and sends a Link Identifier Update Request message to UE_2 (see TS 23.287 [2]). In addition to the changed identifiers, UE_1 shall include the MSB of $K_{NRP-sess}$ ID in the Link Identifier Update Request message. These bits shall be chosen so that they uniquely identify $K_{NRP-sess}$ at UE_1.

2. UE_2 shall choose the LSB of $K_{NRP-sess}$ ID so that they uniquely identify $K_{NRP-sess}$ at UE_2. UE_2 shall form the new $K_{NRP-sess}$ ID from the MSB received from UE_1 and the LSB that UE_2 chose. UE_2 shall associate the new $K_{NRP-sess}$ ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new $K_{NRP-sess}$ ID when it uses the updated Layer-2 IDs. In addition to its updated identifiers, UE_2 shall send the LSB of $K_{NRP-sess}$ ID to UE_1 along with the received MSB of $K_{NRP-sess}$ ID and other identifiers received from UE_1 in the Link Identifier Update Response message. UE_1 shall check that the returned MSB of $K_{NRP-sess}$ ID is identical to the one sent in step 1.

3. UE_1 shall form the new $K_{NRP-sess}$ ID from the LSB received from UE_2 and the MSB chosen by UE_1 (in step 1). UE_1 shall associate the new $K_{NRP-sess}$ ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new $K_{NRP-sess}$ ID when it uses the updated Layer-2 IDs. UE_1 shall send the Link Identifier Update Ack message to UE_2 including the LSB of $K_{NRP-sess}$ ID and other identifiers received from UE_2. UE_2 shall check that the returned LSB of $K_{NRP-sess}$ ID are identical to the one sent in step 2.

5.3.3.2.2.2 Layer-2 link release

Figure 5.3.3.2.2.2-2 shows the message flows for changing the K_{NRP} ID of the UEs involved in PC5 unicast link to remediate the privacy threat for the K_{NRP} ID. This message flow is based on the Layer-2 link release procedure provided in clause 6.3.3.3 of TS 23.287 [2]. The messages in the Layer-2 link release procedure are always sent protected and hence the new K_{NRP} ID agreed by the UEs is only known to the involved UEs. The new K_{NRP} ID is used on a subsequent unicast link establishment procedure (see clause 5.3.3.1.4.3).

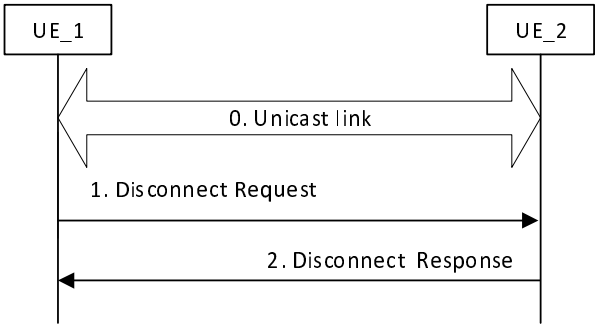

Figure 5.3.3.2.2.2-2: Layer-2 link release procedure

0. UE_1 and UE_2 have a unicast link established as described in TS 23.287 [2].

1. UE_1 sends a Disconnect Request message to UE_2 in order to release the layer-2 link (see TS 23.287 [2]). UE_1 shall include the MSB of K_{NRP} ID in the Disconnect Request message. These bits shall be chosen so that they uniquely identify K_{NRP} at UE_1.

2. UE_2 shall choose the LSB of K_{NRP} ID so that they uniquely identify K_{NRP} at UE_2. UE_2 shall form the new K_{NRP} ID from the MSB received from UE_1 and the LSB that UE_2 chose. UE_2 may use this new K_{NRP} ID when it reconnects with UE_1. UE_2 shall send the LSB of K_{NRP} ID to UE_1 in the Disconnect Response message. Upon reception of the Disconnect Response message, UE_1 shall form the new K_{NRP} ID from the LSB received from UE_2 and the MSB that was chosen by UE_1 (in step 1). UE_1 may use this new K_{NRP} ID when it reconnects with UE_2.

5.4 Security for groupcast mode

5.4.1 General

This clause describes the security requirements and the procedures that can be specifically applied for the groupcast mode over the NR PC5 interface.

5.4.2 Requirements

5.4.2.1 Requirements for securing the NR based PC5 groupcast mode

There are no requirements for securing the NR based PC5 reference point for groupcast mode.

5.4.2.2 Identity privacy requirements for the NR based PC5 groupcast mode

The 5G System shall protect against link ability attacks on Layer-2 ID and IP address for groupcast mode.

The 5G System shall protect against trackability attacks on Layer-2 ID and IP address for groupcast mode.

5.4.3 Procedures

5.4.3.1 Securing the NR based PC5 groupcast mode

There are no particular procedures defined for securing the NR based PC5 groupcast mode.

5.4.3.2 Identity privacy procedures for the PC5 groupcast mode

The below privacy procedures follow the privacy mechanism defined in TS 33.185 [5] for V2X LTE which is intended to mitigate against the threat of tracking the UE by an attacker based on its used source identities.

The UE shall change and randomize its source Layer-2 ID and source IP address including IP prefix (if used) when the V2X application indicates that the Application Layer ID has changed. The UE may change and randomize its source Layer-2 ID and source IP address including IP prefix (if used) at other times (e.g. see clause 5.6.1.1 in TS 23.287 [2]). The UE shall provide an indication to the V2X application layer whenever the source Layer-2 ID and/or source IP address are changed.

NOTE: There are no additional procedures defined for privacy of destination Layer-2 ID in this release.

5.5 Security for broadcast mode

5.5.1 General

This clause describes the security requirements and the procedures that can be specifically applied for the broadcast mode over the NR PC5 interface.

5.5.2 Requirements

5.5.2.1 Requirements for securing the NR based PC5 broadcast mode

There are no requirements for securing the NR based PC5 reference point for broadcast mode.

5.5.2.2 Identity privacy requirements for the NR based PC5 broadcast mode

The 5G System shall protect against link ability attacks on Layer-2 ID and IP address for broadcast mode.

The 5G System shall protect against trackability attacks on Layer-2 ID and IP address for broadcast mode.

5.5.3 Procedures

5.5.3.1 Securing the NR based PC5 broadcast mode

There are no particular procedures defined for securing the NR based PC5 broadcast mode.

5.5.3.2 Identity privacy procedures for the NR based PC5 broadcast mode

These procedures for the privacy of source Layer-2 ID and source IP address are the same as that given in clause 5.4.3.2 for the source identities in the UE.

6 Security for V2X over Uu reference point

6.1 General

This clause contains the security and privacy requirements and procedures that meet the requirements over Uu connectivity with 5G core network.

6.2 Requirements

There are no additional security or privacy requirements for V2X beyond those given in TS 33.501 [6] for Uu connectivity with 5G core network.

6.3 Procedures

There are no additional security or privacy procedures of V2X beyond those given in TS 33.501 [6] for Uu connectivity with 5G core network.

NOTE: The present document does not provide technical solutions to address any privacy concerns specific to V2X service that require privacy for a UE being attached to the network, or that due to the data traversing the network in Uu mode. However, there are general privacy principles applicable outside of 3GPP scope; data minimization and user consent if privacy impacting data collection is unavoidable for providing the V2X service.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

A.1.1 General

This annex specifies the use of the Key Derivation Function (KDF) specified in TS 33.220 [7] for the current specification. This annex specifies how to construct the input string, S, to the KDF (which is input together with the relevant key). For each of the distinct usages of the KDF, the input parameters S are specified below.

A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [7].

A.2 Calculation of NRPEK and NRPIK

When calculating an NRPIK or NRPEK from $K_{NRP-sess}$, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [7]:

- FC = 0x7E
- P0 = 0x00 if NRPEK is being derived or 0x01 if NRPIK is being derived
- L0 = length of P0 (i.e. 0x00 0x01)
- P1 = algorithm identity
- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm identity shall be set as described in TS 33.501 [6].

The input key shall be the 256-bit $K_{NRP-sess}$.

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

A.3 Calculation of $K_{NRP-sess}$ from K_{NRP}

When calculating $K_{NRP-sess}$ from K_{NRP}, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [7]:

- FC = 0x7F
- P0 = Nonce_1
- L0 = length of Nonce_1 (i.e. 0x00 0x10)
- P1 = Nonce_2
- L1 = length of Nonce_2 (i.e. 0x00 0x10)

The input key shall be the 256-bit K_{NRP}.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-11	SA3-97	S3-194526	-	-	-	Skeleton presented for approval at SA3 #97	0.1.0
2019-11	SA3-97	S3-194625	-	-	-	Agreed pCR implemented: S3-194312, S3-194613, S3-194615	0.2.0
2020-03	SA3-98e	S3-200440	-	-	-	Agreed pCR implemented: S3-200087, S3-200088, S3-200108, S3-200468, S3-200241, S3-200496, S3-200501, S3-200506, S3-200507, S3-200508, S3-200509, S3-200350, S3-200510	0.3.0
2020-04	SA3-98-bis-e	S3-200822	-	-	-	Agreed pCR implemented: S3-200824, S3-200605, S3-200612, S3-200806, S3-200653, S3-200823, S3-200682, S3-200825, S3-200828, S3-200685, S3-200690, S3-200819	1.1.0
2020-05	SA3-99e	S3-201338				Agreed pCR implemented: S3-201344, S3-201345, S3-201342, S3-201385, S3-200976, S3-201397, S3-201398, S3-201412, S3-201253, S3-201255, S3-201424, S3-201454	1.2.0
2020-06	SA#88-e	SP-200379				EditHelp review Presented for approval	2.0.0
2020-07	SA#88-e					Upgrade to change control version	16.0.0

History

Document history		
V16.0.0	July 2020	Publication