3GPP TS 33.536 V0.3.0 (2020-03)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

**Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services**

 (Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP..
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

Security, V2X, 5G

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Overview of advanced V2X security architecture 8

4.1 General 8

5 Security for V2X over NR based PC5 reference point 8

5.1 General 8

5.2 Common security 8

5.2.1 General 8

5.2.2 Requirements 8

5.2.3 Procedures 8

5.3 Security for unicast mode 8

5.3.1 General 8

5.3.2 Requirements 9

5.3.2.1 Requirements for securing the PC5 unicast bearer 9

5.3.2.2 Identity privacy requirements for the PC5 unicast bearer 9

5.3.3 Procedures 9

5.3.3.1 Securing the PC5 unicast bearer 9

5.3.3.1.1 General 9

5.3.3.1.2 Overview 9

5.3.3.1.2.1 Key hierarchy 9

5.3.3.1.2.2 Security states 10

5.3.3.1.2.3 High level flows for security establishment 10

5.3.3.1.3 Key establishment procedures 11

5.3.3.1.3.1 General 11

5.3.3.1.3.2 Key establishment 12

5.3.3.1.4 Security establishment procedures 13

5.3.3.1.4.1 General 13

5.3.3.1.4.2 Security policy 13

5.3.3.1.4.2.1 General 13

5.3.3.1.4.2.2 Procedure for security policy provisioning for NR PC5 link 13

5.3.3.1.4.2.3 Security policy handling 13

5.3.3.1.4.3 Security establishment during connection set-up 14

5.3.3.1.4.4 Security establishment during re-keying 15

5.3.3.1.4.5 Security establishment for user plane bearers 16

5.3.3.1.5 Protection of the NR PC5 unicast traffic 16

5.3.3.1.5.1 General 16

5.3.3.1.5.2 Integrity protection 16

5.3.3.1.5.3 Confidentiality protection 17

5.3.3.1.4.4 Content of the PDCP packet 17

5.3.3.2 Identity privacy for the PC5 unicast bearer 17

5.3.3.2.1 General 17

5.3.3.2.2 Procedures 17

5.4 Security for groupcast mode 18

5.4.1 General 18

5.4.2 Requirements 18

5.4.2.1 Requirements for securing the PC5 groupcast bearer 18

5.4.2.2 Identity privacy requirements for the PC5 groupcast bearer 18

5.4.3 Procedures 19

5.4.3.1 Securing the PC5 groupcast bearer 19

5.4.3.2 Identity privacy procedures for the PC5 groupcast bearer 19

5.5 Security for broadcast mode 19

5.5.1 General 19

5.5.2 Requirements 19

5.5.2.1 Requirements for securing the PC5 broadcast bearer 19

5.5.2.2 Identity privacy requirements for the PC5 broadcast bearer 19

5.5.3 Procedures 19

5.5.3.1 Securing the PC5 broadcast bearer 19

5.5.3.2 Identity privacy procedures for the PC5 broadcast bearer 19

6 Security for V2X over Uu reference point 19

6.1 General 19

6.2 Requirements 20

6.3 Procedures 20

Annex A (normative): Key derivation functions 20

A.1 KDF interface and input parameter construction 20

A.1.1 General 20

A.1.2 FC value allocations 20

A.2 Calculation of NRPEK and NRPIK 20

A.3 Calculation of KNRP-sess from KNRP 20

Annex B (informative): Change history 21

# 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: "Enhancement of 3GPP support for V2X scenarios; Stage 1".

[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)".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

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

5GC 5G Core

L2 ID Layer 2 Identity

NR New Radio (5G)

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 PC5 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 are 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, groupcast and broadcast, the NR PC5 supports.

### 5.2.2 Requirements

Editor's Note: This clause lists up the requirements that can commonly apply for all the modes over NR based PC5 reference point

### 5.2.3 Procedures

Editor's Note: This clause specifies mechanisms that can meet the requirements captured in 5.2.2

## 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 unicast communication mode over the NR PC5 interface.

### 5.3.2 Requirements

#### 5.3.2.1 Requirements for securing the PC5 unicast bearer

The initiating UE shall establish a different security context for each peer UEs during the V2X unicast link establishment.

V2X unicast link security establishment between the initiating UE and each peer UE shall be protected from man-in-the-middle attacks.

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

The system shall support confidentiality protection, integrity protection and replay protection of PC5 signalling for V2X unicast.

The system shall support a means of configuring the UEs on whether to use confidentiality and/or integrity protection for a particular unicast connection.

All PC5 unicast UP data of V2X service type shall be protected according to the PC5 UP security policies of the initiating UE and the receiving UE.

#### 5.3.2.2 Identity privacy requirements for the PC5 unicast bearer

The 5G System shall provide means for mitigating trackability attacks on a UE during eV2X unicast communications.

The 5G System shall provide means for mitigating linkability attacks on a UE during eV2X unicast communications.

### 5.3.3 Procedures

#### 5.3.3.1 Securing the PC5 unicast bearer

##### 5.3.3.1.1 General

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

##### 5.3.3.1.2 Overview

###### 5.3.3.1.2.1 Key hierarchy

NR PC5 unicast communication 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: PC5 Key Hierarchy

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 unicast communications. The credentials may include asymmetric key 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 KNRP. The credentials also include identifiers for the keys.

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

KNRP-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 a communication between the UEs, the KNRP-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 KNRP-sess. The 16 bit KNRP-sess ID identifies the KNRP-sess.

NOTE: A KNRP-sess ID with a zero value indicates no security is used and hence the UEs do not assign an all zero value of KNRP-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 UP traffic. They are derived from KNRP-sess and are refreshed automatically every time KNRP-sess is changed.

###### 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 KNRP 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 KNRP, KNRP-sess, NRPEK and NRPIK, the chosen confidentiality and integrity algorithms and PDCP counters used with each bearer.

Once a UE ends its communication session with another UE, it shall delete KNRP-sess, NRPEK and NRPIK, the choice of algorithms and the counters. It may also delete KNRP.

###### 5.3.3.1.2.3 High level flows for 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 send a Direct Communication Request. This message may be received by multiple UEs.

2a/3a/4a. UE\_2a choose to respond to the message and initiates the Direct Auth and Key Establishment procedure (if needed based on the credentials used to establish security – see clause 5.3.3.1.3) to generate the key that will be used to protect the connection. UE\_2a then runs the Direct Security Mode Command procedure with UE\_1 to establish the security based on that key. 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.

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 include in the Direct Security Mode Complete message (sent as part of the Direct Security Mode procedure) from UE\_1 as this message is both confidentiality and integrity protected (see TS 23.287 [2]).

##### 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 KNRP. The long term credentials and associated authentication method that are used to establish the keys used to protect the NR PC5 unicast traffic 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 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 PC5 interface. This allows, for example, an application to change authentication method without affecting the 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. In both cases the Direct Communication Request message shall include the Key\_Est\_Info.

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) KNRP. UE\_2 shall send a Direct Security Mode Command messages to UE\_1. The message may include Key\_Est\_Info if need by the authentication method being used and shall contain MSB of KNRP ID. The MSB of KNRP ID are chosen so that they uniquely identify KNRP at UE\_2.

4. On receiving the Direct Security Mode Command, UE\_1 shall calculate (if not already done) KNRP based from Key\_Est\_Info (if provided). UE\_1 shall choose the LSB of KNRP ID are chosen so that they uniquely identify KNRP at UE\_1. UE\_1 shall form KNRP ID from the received MSB of KNRP ID and its chosen LSB of KNRP ID and shall store the complete KNRP ID with KNRP.

 UE\_1 shall send a Direct Security Mode Complete message to UE\_2 which shall contain the LSB of KNRP ID. UE\_1 shall form KNRP ID from its chosen MSB of KNRP ID and the received LSB of KNRP ID and shall store the complete KNRP ID with KNRP.

##### 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 NR PC5 link shall support activation or deactivation of security based on the network security policy similar to Uu, as defined in TS 33.501[6]. Security policy for PC5 link shall be provisioned for NR PC5 V2X communication as well, as detailed in clause 5.3.3.1.4.2.2 of this document and handled as detailed in clasue 5.3.3.1.4.2.3 of this document.

5.3.3.1.4.2.2 Procedure for security policy provisioning for NR PC5 link

For handling the security policy for the NR PC5 link, the PCF shall also provision the UP security policy per V2X application, 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 NR PC5 Unicast the UE shall be provisioned with the following security policy:

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/OFF

• Signalling confidentiality protection: REQUIRED/PREFERRED/OFF

• User plane integrity protection: REQUIRED/PREFERRED/OFF

• User plane confidentiality protection: REQUIRED/PREFERRED/OFF

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

Editor’s note: Whether policy is OFF or NOT NEEDED is FFS

The signalling integrity protection security policy being OFF means that the UE shall only establish a connection with no security. The signalling integrity protection security policy being PREFFERED means that the UE may try to establish security but will accept the connection with no security.. With the integrity protection security policy set to REQUIRED, the UE may only accept the connection if a non-NULL integrity algorithm is used for protection of the signalling traffic.

For the other cases, a setting of OFF means that the UE shall only use NULL confidentiality algorithm for that traffic or apply no integrity protection, while a REQUIRED setting means that the UE shall use a non-NULL algorithm. If the security policy is PREFERRED, then the UE may accept any algorithm for that particular protection. One use of PREFERRED is to enable a security policy to be changed without updating all UEs at once.

At initial connection, the UE include its signalling security policy in the Direct Communication Request message. The UE(s) responding to this take account of this when choosing the algorithms 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.

When adding a V2X service to an existing connection, the UE responding to the request shall reject the request if signalling security in use does not match the policy for the new application.

The combination of security policies for UP Integrity Protection will result in the following activation of integrity protection:

Case 1: Both UP security policies indicate UP Integrity Protection "required", or one UP security policy indicates “required” and the other indicates “preferred”:

Activation of UP integrity protection for each user plane bearer individually of the service type when the PC5 unicast is established.

Case 2: Both UP security policies indicate UP Integrity Protection "preferred":

Activate or deactivate of UP integrity protection for each user plane bearer individually of the service type when the PC5 unicast is established based on local policy.

Case 3: For the other scenarios besides Case 1 and Case 2:

Deactivation of UP integrity protection for each user plane bearer individually of the service type when the PC5 unicast is established.

For UP Ciphering Protection, the resulting activation is the same as the UP integrity protection activation.

Editor’s note: The security policy handling related part needs to be clearly defined. It is FFS that how the initiating UE and the receiving UE deal with the security policy, e.g., whether to accept the communication or not with their security policy and local policy

###### 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 Nonce\_1 (for session key KNRP-sess generation), UE\_1 security capabilities (the list of algorithms that UE\_1 will accept for this connection), UE\_1’s signalling security policy and the most significant 8-bits of the KNRP-sess ID. These bits 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 KNRP ID if the UE\_1 has an exisiting KNRP for the UE that it trying to communicate with. The absence of the KNRP ID parameter indicates that UE\_1 does not have a KNRP for UE\_2. The message also contains Key\_Est\_Info (see subclause 5.3.3.1.3.2).

2. 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 KNRP and KNRP 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 optionally Key\_Est\_Info of KNRP ID and optionally Key\_Est\_Info if a fresh KNRP is to be generated (see clause 5.3.3.1.3). UE\_2 shall include Nonce\_2 to allow a session key to be calculated and 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 security policy has integrity as OFF or PREFERRED. UE\_2 shall also return the UE\_1 security capabilities and UE\_1’s signalling security policy to provide protection against bidding down attacks. UE\_2 shall also includes the least significant 8-bits of KNRP-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 KNRP-Sess from KNRP and both Nonce\_1 and Nonce\_2 (see Annex X.Y) and then derive the confidentiality and integrity keys based on the chosen algorithms (Annex X.Y). 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 KNRP-sess ID from the most significant bits it received in message 1 and least significant bits it sent in message 3.

4. On receiving the Direct Security Mode Command, UE\_1 shall first check that the received LSB of KNPR-sess ID is unique, i.e. has not been sent by another UE responding this Direct Commuication Request. If the LSB of KNPR-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 KNPR-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 KNPR-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 KNPR-sess ID). UE-2 shall erase the former LSB of KNPR-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 KNPR-sess ID is unique, UE\_1 shall calculate KNRP-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. UE\_1 shall only accept the NULL integrity algorithm if its security policy for signalling indicates that integrity protection is OFF or PREFERRED. If both these checks pass, then UE\_1 is ready to send and receive signalling and user planetraffic with the new security context. UE\_1 shall send an integrity protected and confidentiality protected (with the chosen algorithm which may be the null algorithm) Direct Security Mode Complete message to UE\_2. UE\_1 shall form the KNRP-sess ID from the most significant bits it sent in message 1 and least significant bits it received in message 3.

5. 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 KNRP-sess are used. Optionally the rekeying can also enforce refresh of KNRP. 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 KNRP-sess and NRPEK and NRPIK, and may refresh KNRP. A rekeying operation follows the flows given in figure 5.3.3.1.4.4-1.

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 Nonce\_1 (for session key generation), UE\_1 security capabilities (the list of algorithms that UE\_1 will accept for this connection) and the most significant 8-bits of the KNRP-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 KNRP. The message also contains Key\_Est\_Info (see subclause 6.5.4).

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 KNRP.

3. This step is the same as step 3 in 5.3.3.1.4.3 except that the chosen integrity algorithm shall only be NULL if the NULL integrity 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 5.3.3.1.4.3 except that UE\_1 shall only accept the NULL integrity algorithm if the NULL integrity algorithm is currently in use and UE\_1 does not check the returned siganlling security policy (as it is not sent in this case).

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

6. When UE\_1 receives a message integrity protected with the new security context, it shall delete any old security context is has still stored for UE\_2.

###### 5.3.3.1.4.5 Security establishment for user plane bearers

At initial connection or adding a V2X service, the initiating UE includes its user plane security policy in the Direct Security Mode Complete or Link Modification request message respectively. The receiving UE shall reject the connection setup or Link Modification Request if the received user plane security policy had either confidentiality/integrity set to OFF and its own corresponding policy is set to REQUIRED or if the received user plane security policy had either confidentiality/integrity set to REQUIRED and its own corresponding policy is set to OFF. Otherwise the receiving UE may accept the connection setup or Link Modification Request.

Editor’s note: If is FFS whether the receiving UE sends its UP security policy or a choice of security back to the initiating when accepting the connection setup or Link Modification Request.

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 5.3.3.1.4.3) before establishing the user plane bearer.

When establishing the user plane bearer the initiating UE shall indicate the configuration of confidentiality and integrity protection in the PC5-RRC message. The confidentiality and integrity protection algorithms are same as those selected for protecting the signalling bearers.

Both UEs shall ensure that 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.

##### 5.3.3.1.5 Protection of the NR PC5 unicast traffic

###### 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, may be sent with no protection. Once security is established all signalling messages are sent integrity protected and confidentiality protected with the chosen algorithms except the Direct Security Mode Command which is sent integrity protected only.

Editor’s note: The exact messages that can be sent without security protection is FFS.

###### 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 relevant bearers. The algorithm identifies 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 used 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 based on the LCID;

Editor’s note: The exact mapping of LCID to Bearer is FFS.

- COUNT[0] to COUNT[31] are filled with counter value.

The receiving UE ensures that received protected signalling messages and user plane traffic 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 one-to-one traffic. The algorithm identifies 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 based on the LCID;

Editor’s note: The exact mapping of LCID to Bearer is FFS.

- COUNT[0] to COUNT[31] are filled with counter value.

###### 5.3.3.1.4.4 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. Key ID is used to signal which security context is being used and shall be set to KNRP-sess ID.

This is illustrated in the Figure 5.3.3.1.4.4-1.



**Figure 5.3.3.1.4.4-1: Security parameters in the PDCP header for one-to-one communications**

Editor’s Note: It is FFS if the length of counter is 32 bits and if not whether it is the LSB of the counter that is included in PDCP header and if COUNT[0] to COUNT[31] are padded with its of KNPR-sess ID.

#### 5.3.3.2 Identity privacy for the PC5 unicast bearer

##### 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. These messages in this procedure are always sent protected 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 prior to them being used.

##### 5.3.3.2.2 Procedures

Figure 5.3.3.2.2-1 shows the flows for changing the identities of the UEs involved in a unicast communication. The figure and the following steps only show the security parameters (KNRP ID and KNRP-sess ID) that are changed and the Layer-2 ID but not the other parameters described in TS 23.287 [2].



Figure 5.3.3.2.2-1: Link identifier update procedure

The procedures proceeds with the following steps and give the additional processing on top of that given in TS 23.287 [2].

0. UE\_1 and UE\_2 are communicating via a unicast and have established the security for the link.

1. UE\_1 decides to change the identifiers and sends a Link Identifier Update Request message to UE\_2 (see TS 23.287 [2]). UE\_1 shall include the MSB of KNRP-sess ID. These bits shall be chosen so that they uniquely identify KNRP-sess at UE\_1.

2. UE\_2 shall choose the LSB of KNRP-sess ID so that they uniquely identify KNRP-sess at UE\_2. UE\_2 shall form the new KNRP-sess ID from the MSB received from UE\_1 and the LSB that UE\_2 chose. UE\_2 shall associate the new KNRP-sess ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new KNRP-sess ID when it uses the updated Layer-2 IDs. UE\_2 shall send the LSB of KNRP-sess ID to UE\_1 along with the received MSB of KNRP-sess ID in the Link Identifier Update Response message. UE\_1 shall check that the returned MSB of KNRP-sess ID are the same as it sent in step 1.

3. UE\_1 shall form the new KNRP-sess ID from the LSB received from UE\_2 and the MSB chosen by UE\_1 LSB (in step 1). UE\_1 shall associate the new KNRP-sess ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new KNRP-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 KNRP-sess ID. UE\_2 shall check that the returned the LSB of KNRP-sess ID are the same as it sent in step 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 communication mode over the NR PC5 interface.

### 5.4.2 Requirements

#### 5.4.2.1 Requirements for securing the PC5 groupcast bearer

There are no requirements for securing the PC5 bearer for groupcast mode.

#### 5.4.2.2 Identity privacy requirements for the PC5 groupcast bearer

The 5G System shall protect against linkability attacks on Layer-2 ID and IP address during V2X groupcast communications.

The 5G System shall protect against trackability attacks on Layer-2 ID and IP address during V2X groupcast communications.

### 5.4.3 Procedures

#### 5.4.3.1 Securing the PC5 groupcast bearer

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

#### 5.4.3.2 Identity privacy procedures for the PC5 groupcast bearer

The below privacy procedures follows 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 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.

Editor's note: Privacy of destination ID of groupcast if FFS.

## 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 communication mode over the NR PC5 interface.

### 5.5.2 Requirements

#### 5.5.2.1 Requirements for securing the PC5 broadcast bearer

There are no requirements for securing the NR PC5 bearer in broadcast mode.

#### 5.5.2.2 Identity privacy requirements for the PC5 broadcast bearer

The 5G System shall protect against linkability attacks on Layer-2 ID and IP address during V2X broadcast communications.

The 5G System shall protect against trackability attacks on Layer-2 ID and IP address during V2X broadcast communications.

### 5.5.3 Procedures

#### 5.5.3.1 Securing the PC5 broadcast bearer

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

#### 5.5.3.2 Identity privacy procedures for the PC5 broadcast bearer

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.

## 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.

## 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.

NOTE 1: The specification 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 KNRP-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 KNRP-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 KNRP-sess from KNRP

When calculating KNRP-sess from KNRP, 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 KNRP.

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, S3-200211-r2, S3-200241, S3-200342-r4, S3-200345-r6, S3-200346-r2, S3-200347-r10, S3-200348-r3, S3-200349-r1, S3-200350, S3-200352-r3 | 0.3.0 |