ETSI TS 133 536 V18.0.0 (2024-04)

LTE;
5G;
Security aspects of 3GPP support
for advanced Vehicle-to-Everything (V2X) services
(3GPP TS 33.536 version 18.0.0 Release 18)

Reference
RTS/TSGS-0333536vi00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 https://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

5.3.3.1.2.0 Security Context

The UE establishes a security context for each unicast link. The security context includes $K_{NRP\text{-}sess}$, NRPEK (if applicable), NRPIK, the chosen confidentiality (if applicable) and integrity algorithms, and PDCP counters used with each bearer. The UE updates the security context associated to the unicast link when the unicast link is rekeyed. The UE deletes the security context associated to a unicast link once the unicast link is released.

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.