|  |  |
| --- | --- |
| 3GPP TR 33.836 V16.1.0 (2020-09) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on 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. | |

|  |
| --- |
|  |
| ***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 [6](#__RefHeading___Toc51254938)

1 Scope [8](#__RefHeading___Toc51254939)

2 References [8](#__RefHeading___Toc51254940)

3 Definitions of terms, symbols and abbreviations [9](#__RefHeading___Toc51254941)

3.1 Terms [9](#__RefHeading___Toc51254942)

3.2 Symbols [9](#__RefHeading___Toc51254943)

3.3 Abbreviations [9](#__RefHeading___Toc51254944)

4 Security Aspects of Advanced V2X Services [9](#__RefHeading___Toc51254945)

5 Key Issues [10](#__RefHeading___Toc51254946)

5.1 Key Issue #1: Privacy protection for unicast messages over PC5 [10](#__RefHeading___Toc51254947)

5.1.1 Key issue details [10](#__RefHeading___Toc51254948)

5.1.2 Security threats [10](#__RefHeading___Toc51254949)

5.1.3 Potential security requirements [10](#__RefHeading___Toc51254950)

5.2 Key Issue #2: Security for eV2X unicast messages over PC5. [10](#__RefHeading___Toc51254951)

5.2.1 Key issue details [10](#__RefHeading___Toc51254952)

5.2.2 Security threats [11](#__RefHeading___Toc51254953)

5.2.3 Potential security requirements [11](#__RefHeading___Toc51254954)

5.3 Key Issue #3: Privacy protection for groupcast messages over PC5 [11](#__RefHeading___Toc51254955)

5.3.1 Key issue details [11](#__RefHeading___Toc51254956)

5.3.2 Security threats [11](#__RefHeading___Toc51254957)

5.3.3 Potential security requirements [12](#__RefHeading___Toc51254958)

5.4 Key Issue #4: Security of identifier conversion in groupcast communication [12](#__RefHeading___Toc51254959)

5.4.1 Key issue details [12](#__RefHeading___Toc51254960)

5.4.2 Security threats [12](#__RefHeading___Toc51254961)

5.4.3 Potential security requirements [12](#__RefHeading___Toc51254962)

5.5 Key Issue #5: Security for setting up groupcast [13](#__RefHeading___Toc51254963)

5.5.1 Key issue details [13](#__RefHeading___Toc51254964)

5.5.2 Security threats [13](#__RefHeading___Toc51254965)

5.5.3 Potential security requirements [13](#__RefHeading___Toc51254966)

5.6 Key Issue #6: Security of the UE service authorization and revocation [13](#__RefHeading___Toc51254967)

5.6.1 Key issue details [13](#__RefHeading___Toc51254968)

5.6.2 Security threats [13](#__RefHeading___Toc51254969)

5.6.3 Potential security requirements [13](#__RefHeading___Toc51254970)

5.7 Key Issue #7: Cross-RAT PC5 control authorization indication [13](#__RefHeading___Toc51254971)

5.7.1 Key issue details [13](#__RefHeading___Toc51254972)

5.7.2 Security threats [14](#__RefHeading___Toc51254973)

5.7.3 Potential security requirements [14](#__RefHeading___Toc51254974)

5.8 Key Issue #8: Privacy protection for broadcast messages over PC5 [14](#__RefHeading___Toc51254975)

5.8.1 Key issue details [14](#__RefHeading___Toc51254976)

5.8.2 Security threats [14](#__RefHeading___Toc51254977)

5.8.3 Potential security requirements [14](#__RefHeading___Toc51254978)

5.9 Key Issue #9: Minimizing the impact of privacy protection mechanism in the application layer communication [15](#__RefHeading___Toc51254979)

5.9.1 Key issue details [15](#__RefHeading___Toc51254980)

5.9.2 Security threats [16](#__RefHeading___Toc51254981)

5.9.3 Potential security requirements [16](#__RefHeading___Toc51254982)

5.10 Key Issue #10: UP security policy handling for PC5 and Uu interface [16](#__RefHeading___Toc51254983)

5.10.1 Key issue details [16](#__RefHeading___Toc51254984)

5.10.2 Security threats [17](#__RefHeading___Toc51254985)

5.10.3 Potential security requirements [17](#__RefHeading___Toc51254986)

5.11 Key Issue #11: Security for eV2X broadcast messages over PC5 [17](#__RefHeading___Toc51254987)

5.11.1 Key issue details [17](#__RefHeading___Toc51254988)

5.11.2 Security threats [17](#__RefHeading___Toc51254989)

5.11.3 Potential security requirements [17](#__RefHeading___Toc51254990)

6 Solutions [17](#__RefHeading___Toc51254991)

6.1 Solution #1: Privacy protection for unicast messages over PC5 [17](#__RefHeading___Toc51254992)

6.1.1 Introduction [17](#__RefHeading___Toc51254993)

6.1.2 Solution details [18](#__RefHeading___Toc51254994)

6.1.3 Evaluation [20](#__RefHeading___Toc51254995)

6.2 Solution #2: Security for eV2X unicast messages over PC5 [20](#__RefHeading___Toc51254996)

6.2.1 Introduction [20](#__RefHeading___Toc51254997)

6.2.2 Solution details [21](#__RefHeading___Toc51254998)

6.2.3 Evaluation [22](#__RefHeading___Toc51254999)

6.3 Solution #3: Security for eV2X unicast messages over PC5 [22](#__RefHeading___Toc51255000)

6.3.1 Introduction [22](#__RefHeading___Toc51255001)

6.3.2 Solution details [23](#__RefHeading___Toc51255002)

6.3.3 Evaluation [25](#__RefHeading___Toc51255003)

6.4 Solution #4: Privacy protection for unicast messages over PC5 [25](#__RefHeading___Toc51255004)

6.4.1 Introduction [25](#__RefHeading___Toc51255005)

6.4.2 Solution details [26](#__RefHeading___Toc51255006)

6.4.3 Evaluation [27](#__RefHeading___Toc51255007)

6.5 Solution #5: Security protection of service authorisation [27](#__RefHeading___Toc51255008)

6.5.1 Introduction [27](#__RefHeading___Toc51255009)

6.5.2 Solution details [27](#__RefHeading___Toc51255010)

6.5.3 Evaluation [28](#__RefHeading___Toc51255011)

6.6 Solution #6: V2X Group Key Provisioning [28](#__RefHeading___Toc51255012)

6.6.1 Introduction [28](#__RefHeading___Toc51255013)

6.6.2 Solution details [28](#__RefHeading___Toc51255014)

6.6.3 Evaluation [29](#__RefHeading___Toc51255015)

6.7 Solution #7: Cross-RAT PC5 control authorization indication [29](#__RefHeading___Toc51255016)

6.7.1 Introduction [29](#__RefHeading___Toc51255017)

6.7.2 Solution details [29](#__RefHeading___Toc51255018)

6.7.3 Evaluation [29](#__RefHeading___Toc51255019)

6.8 Solution #8: Deriving PC5 layer keys based on higher layer keys [29](#__RefHeading___Toc51255020)

6.8.1 Introduction [29](#__RefHeading___Toc51255021)

6.8.2 Solution details [29](#__RefHeading___Toc51255022)

6.8.3 Evaluation [31](#__RefHeading___Toc51255023)

6.9 Solution #9: Security for eV2X unicast messages over PC5 using ECCSI and SAKKE [32](#__RefHeading___Toc51255024)

6.9.1 Introduction [32](#__RefHeading___Toc51255025)

6.9.2 Solution details [32](#__RefHeading___Toc51255026)

6.9.2.1 Initial Security Link Establishment [32](#__RefHeading___Toc51255027)

6.9.2.2 Procedure for privacy protection of unicast communication [34](#__RefHeading___Toc51255028)

6.9.3 Evaluation [35](#__RefHeading___Toc51255029)

6.10 Solution #10: Privacy protection for unicast message over PC5 [35](#__RefHeading___Toc51255030)

6.10.1 Introduction [35](#__RefHeading___Toc51255031)

6.10.2 Solution details [35](#__RefHeading___Toc51255032)

6.10.3 Evaluation [36](#__RefHeading___Toc51255033)

6.11 Solution #11: Solution on minimizing the impact of privacy protection mechanism in the application layer communication [37](#__RefHeading___Toc51255034)

6.11.1 Introduction [37](#__RefHeading___Toc51255035)

6.11.2 Solution details [37](#__RefHeading___Toc51255036)

6.11.3 Evaluation [38](#__RefHeading___Toc51255037)

6.12 Solution #12: Protecting the traffic at the PDCP layer [39](#__RefHeading___Toc51255038)

6.12.1 Introduction [39](#__RefHeading___Toc51255039)

6.12.2 Solution details [39](#__RefHeading___Toc51255040)

6.12.2.1 General [39](#__RefHeading___Toc51255041)

6.12.2.2 Integrity protection [39](#__RefHeading___Toc51255042)

6.12.2.3 Confidentiality protection [39](#__RefHeading___Toc51255043)

6.12.2.4 Security contents in the PCDP header [39](#__RefHeading___Toc51255044)

6.12.3 Evaluation [40](#__RefHeading___Toc51255045)

6.13 Solution #13: Solution against V2X UE tracking based on PC5 identifiers [40](#__RefHeading___Toc51255046)

6.13.1 Introduction [40](#__RefHeading___Toc51255047)

6.13.2 Solution details [40](#__RefHeading___Toc51255048)

6.13.3 Evaluation [40](#__RefHeading___Toc51255049)

6.14 Solution #14: Identifier conversion in groupcast communication [41](#__RefHeading___Toc51255050)

6.14.1 Introduction [41](#__RefHeading___Toc51255051)

6.14.2 Solution details [41](#__RefHeading___Toc51255052)

6.14.3 Evaluation [41](#__RefHeading___Toc51255053)

6.15 Solution #15: Solution on minimizing the impact of privacy protection mechanism in the application layer communication [42](#__RefHeading___Toc51255054)

6.15.1 Introduction [42](#__RefHeading___Toc51255055)

6.15.2 Solution details [42](#__RefHeading___Toc51255056)

6.15.3 Solution Evaluation [43](#__RefHeading___Toc51255057)

6.16 Solution #16: Solution for the activation of user plane security in NR PC5 unicast [43](#__RefHeading___Toc51255058)

6.16.1 Introduction [43](#__RefHeading___Toc51255059)

6.16.2 Solution details [43](#__RefHeading___Toc51255060)

6.16.3 Evaluation [44](#__RefHeading___Toc51255061)

6.17 Solution #17: PC5 layer key derivation using the 5G network keys [44](#__RefHeading___Toc51255062)

6.17.1 Introduction [44](#__RefHeading___Toc51255063)

6.17.2 Solution details [44](#__RefHeading___Toc51255064)

6.17.3 Evaluation [46](#__RefHeading___Toc51255065)

6.18 Solution #18: Solution for the UP security activation policy handling in NR PC5 unicast [46](#__RefHeading___Toc51255066)

6.18.1 Introduction [46](#__RefHeading___Toc51255067)

6.18.2 Solution details [46](#__RefHeading___Toc51255068)

6.18.3 Evaluation [47](#__RefHeading___Toc51255069)

6.19 Solution #19: Protection of IEs in Direct Communication Request message [47](#__RefHeading___Toc51255070)

6.19.1 Introduction [47](#__RefHeading___Toc51255071)

6.19.2 Solution details [47](#__RefHeading___Toc51255072)

6.19.3 Evaluation [47](#__RefHeading___Toc51255073)

6.20 Solution #20: Solution on securely creating destination Layer-2 ID in groupcast communication [48](#__RefHeading___Toc51255074)

6.20.1 Introduction [48](#__RefHeading___Toc51255075)

6.20.2 Solution details [48](#__RefHeading___Toc51255076)

6.20.3 Evaluation [48](#__RefHeading___Toc51255077)

7 Conclusions [49](#__RefHeading___Toc51255078)

7.1 Conclusion on KI #7 [49](#__RefHeading___Toc51255079)

7.2 Conclusion on KI #5 [49](#__RefHeading___Toc51255080)

7.3 Conclusion on KI #11 [49](#__RefHeading___Toc51255081)

7.4 Conclusion on KI #3 and #8 [49](#__RefHeading___Toc51255082)

7.5 Conclusion on KI #6 [49](#__RefHeading___Toc51255083)

7.6 Conclusion on KI #1 [49](#__RefHeading___Toc51255084)

7.7 Conclusion on KI #2 [49](#__RefHeading___Toc51255085)

7.8 Conclusion on KI #10 [49](#__RefHeading___Toc51255086)

7.9 Conclusion on KI#4 [49](#__RefHeading___Toc51255087)

7.10 Conclusion on KI#9 [50](#__RefHeading___Toc51255088)

Annex A: Change History [51](#__RefHeading___Toc51255089)

# Foreword

This Technical Report 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 scope of the present document is to provide security and privacy analysis of eV2X system architecture, derive potential security and privacy requirements, and evaluate security and privacy solutions for protection of it. The security aspects to be considered are as follows:

- Security and privacy for new interfaces in 5G eV2X system architecture, compared to TS 23.285 [2]

- Security and privacy for eV2X unicast over PC5

- Security and privacy for eV2X group communication over PC5

- Other security and privacy issues related to eV2X services, if there is any

# 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 23.285: "Architecture enhancements for V2X services".

[3] 3GPP TS 22.186: "Enhancement of 3GPP support for V2X scenarios; Stage 1".

[4] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[5] 3GPP TR 23.786: "Study on architecture enhancement for EPS and 5G System to support advanced V2X services".

[6] 3GPP TR 33.303: "Proximity-based Services (ProSe); Security aspects".

[7] 3GPP TR 23.303: "Proximity-based services (ProSe); Stage 2".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] 3GPP TR 23.795: "Study on application layer support for V2X services".

[10] IETF RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".

[11] IETF RFC 6508: "Sakai-Kasahara Key Encryption (SAKKE)."

[12] 3GPP TS 33.185: "Security aspect for LTE support of Vehicle-to-Everything (V2X) services".

[13] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[14] IEEE Std 802.11p: "Wireless Access in Vehicular Environments (WAVE)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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].

**Groupcast:** See the definition in TS 23.287 [4].

## 3.2 Symbols

Void.

## 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

AF Application Function

AMF Access and Mobility management Function

AS layer Access Stratum layer

DCA Direct Communication Accept

DCR Direct Communication Request

DSM Direct Security Mode

eV2X enhancement of 3GPP support for V2X

ITS Intelligent Transport Systems

ITS-AID ITS Application Identifier

L2 ID Layer 2 Identity

NG Next Generation

NG-RAN Next Generation RAN

NGAP NG Application Protocol

NR New Radio (5G)

PCF Policy Control Function

PDCP Packet Data Convergence Protocol

PDU Protocol Data Unit

PSID Provider Service Identifier

RAN Radio Access Network

RAT Radio Access Technology

UDM Unified Data Management

V2X Vehicle-to-Everything

# 4 Security Aspects of Advanced V2X Services

Advanced V2X services of 3GPP, in the context of the present document, include several V2X scenarios such as Vehicles Platooning, Advanced Driving, Extended Sensors, Remote Driving, Vehicle quality of service Support, and other general aspects (e.g. interworking), as specified in TS 22.186 [3], with service requirements. To support them, TS 23.287 [4] provides architectural enhancements to the 5G system for V2X communications over the reference points - NR PC5 RAT, LTE PC5 RAT, NR Uu, and E-UTRA Uu (connected to 5GC).

V2X communication over NR based PC5 reference point supports broadcast mode, groupcast, mode and unicast mode, while V2X communication on E-UTRA based PC5 reference point (connected to EPS) is connectionless, i.e. broadcast mode at AS layer. In this release, V2X communication over Uu reference point is only unicast. Architectural reference model is specified in clause 4.2 of TS 23.287 [4], where 5G System architecture applies in general and V3 (PC3) is missing because PCF takes places the role of configuration and provisioning for UE, in addition to external V2X application server.

Potential security impact mostly comes from unicast and groupcast mode of communication over NR PC5, since only broadcast mode is supported over PC5 for V2X communication in previous releases. Unicast mode over PC5 involves signalling over control plane in V2X layer and AS layer, and this might need security protection. Group management for groupcast is handled by application layer, and it still might need consideration of security and privacy aspects. However, security for broadcast mode should still be considered based on changes in the new release. Lastly provisioning of UE configuration for V2X communication and interworking with EPS may require security consideration, whether or not existing 5G security can cover it.

# 5 Key Issues

## 5.1 Key Issue #1: Privacy protection for unicast messages over PC5

### 5.1.1 Key issue details

KI#9 from TR 23.786 [5] is looking at the support of unicast for sensor sharing over PC5, and more specifically, at how to prevent privacy issues related to long duration unicast session, e.g. source L2 ID tracking.

The solution#11 [5], adopted as a baseline for normative work, proposes that a UE updates its peer with its new identifier(s) (e.g. L2 ID) in a Link Identifier Update Request message, e.g., upon an upper layer trigger or upon expiry of a timer. The peer acknowledges the change in a Link Identifier Update Response message. Upon reception of this message both UEs can start using the new identifier(s).

### 5.1.2 Security threats

An adversary that is capable of connecting and linking L2 identities to a real or a long-term Application Layer ID will be able to track and trace the endpoint in space and time. Such trackability and linkability will be an attack on eV2X endpoint privacy.

### 5.1.3 Potential security requirements

The 5G System shall provide means for mitigating trackability attacks on L2 identities during eV2X unicast communications.

The 5G System shall provide means for mitigating linkability attacks on L2 identities during eV2X unicast communications.

## 5.2 Key Issue #2: Security for eV2X unicast messages over PC5.

### 5.2.1 Key issue details

KI#9 from TR 23.786 [5] describes security association establishment for unicast/multicast for sensor sharing over PC5, and the clause 6.3.3 of TS 23.287 [4] specifies the procedures and the messages for unicast control signalling.

The Solution #11 [5], adopted as a baseline for normative work, introduces a new V2X Service oriented L2 link establishment procedure. In this procedure, the initiating UE broadcasts a Direct Communication Request message specifying the V2X Service requesting layer 2 link establishment. All UEs receiving this message and interested in that V2X service reply with a Direct Communication Accept message have to establish a unicast communication and associated security association for that unicast link using their L2 ID as the source L2 ID and the initiating UE L2 ID as the destination L2 ID.

Another "UE Oriented L2 link establishment" procedure is specified in Solution#11. In this procedure, the initiating UE broadcasts a Direct Communication Request message which includes the upper layer identifier of a peer UE and source L2 ID of the initiating UE. If the peer UE decides to respond to the request, it replies with a unicast Direct Communication Accept message using its L2 ID as the source L2 ID and the initiating UE L2 ID as the destination L2 ID.

It is assumed in Solution #11 Clause 6.11.2.4 TR 23.786 [5] that secure L2 link establishment as defined for ProSe one-to-one communications in TS 33.303 [6] is reused.

The protocol for one-to-one link establishment defined for ProSe in TS 23.303 [7] is based on the initiating UE sending the Direct Communication Request over unicast message to a peer UE. An adjustment to the L2 secure link establishment protocol may be needed in order to support the link setup procedure based on an initial broadcast from the initiating UE.

### 5.2.2 Security threats

An adversary that is capable of breaking into signaling exchange between the parties during link establishment as defined in the Solution #11 of TR 23.786 [5] can eavesdrop on signalling or subsequent data traffic, attack integrity of signalling, or usurp the identity of one or more of the participants e.g. initiating UE or one of the peer UEs. The breach of integrity of some information delivered through unicast mode control signalling over PC5 could affect service availability.

### 5.2.3 Potential security requirements

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

NOTE: The potential requirement above is analogous to the corresponding ProSe [6] requirement.

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 and integrity protection of the PC5 user plane.

The system shall support integrity protection of PC5-S Signalling for V2X unicast.

The system shall support confidentiality protection for the update of link identifiers.

## 5.3 Key Issue #3: Privacy protection for groupcast messages over PC5

### 5.3.1 Key issue details

KI#9 from TR 23.786 [5] is looking at the support of groupcast for sensor sharing over PC5, and more specifically, at how to prevent privacy issues related to long duration groupcast session, e.g. source L2 ID tracking.

NOTE: The definition of groupcast is specified in TS 23.287 [4].

### 5.3.2 Security threats

An adversary that is capable of connecting and linking L2 identities to a real or a long-term eV2X endpoint identity will be able to track and trace the endpoint in space and time. Such trackability and linkability will be an attack on eV2X endpoint privacy.

### 5.3.3 Potential security requirements

The 5G System shall provide means for mitigating linkability attacks on L2 identities during eV2X groupcast communications.

The 5G System shall provide means for mitigating trackability attacks on L2 identities during eV2X groupcast communications.

## 5.4 Key Issue #4: Security of identifier conversion in groupcast communication

### 5.4.1 Key issue details

In TR 23.786 [5], Solution #21 "Group communication enhancement for NR PC5" is selected as the baseline for normative work to address KI #1 "Support of eV2X group communication".



Figure 5.4.1-1: End to end groupcast communication

With reference to Figure 5.4.1-1 as in TR 23.786 [5], the group identifier provided by the application layer will be converted into the L2 ID. In addition, it is stated in TR 23.287 [4] that: "When the group identifier information is not provided by the V2X application layer, the UE determines the destination Layer-2 ID based on configuration of the mapping between service type (e.g. PSID/ITS-AID) and Layer-2 ID"

This conversion/mapping procedure should be secured in terms of privacy and traceability. Unless the conversion is carefully performed, the group membership of specific UEs could be disclosed. For example, attackers might be able to make an inquiry whether any member of certain group are exists in some location.

### 5.4.2 Security threats

If the Group ID is not securely converted by the application layer, the intruder can link back to UE groupcast memberships. Similarly if the mapping of L2 ID is not securely performed from the V2X services (e.g. PSID/ITS-AID), the attacker may also link back to the privacy parameters in geographical area(s) that require privacy support.

### 5.4.3 Potential security requirements

5G system shall ensure that the group IDs conversion to L2 IDs are protected from linkability and traceability attacks for eV2X groupcast communications.

## 5.5 Key Issue #5: Security for setting up groupcast

### 5.5.1 Key issue details

In TR 23.786 [5], Solution #11 "Solution for unicast or multicast for eV2X communication over PC5 reference point" is selected as the baseline for normative work to address KI #9 "Support of unicast/multicast for sensor sharing over PC5" in the present document. Solution #11 states that "The unicast or groupcast communication may need protection at link layer as well." Clearly security aspect for setting up a unicast or groupcast communication has not been considered. This key issue is about setting up a multicast communication securely.

NOTE: In the above clause, the directly quoted text from TR 23.786 [5] uses the term "multicast". However, it means "groupcast" as defined in the subsequent normative specification in TS 23.287 [4].

### 5.5.2 Security threats

Since L2 signalling is used to establish eV2X groupcast with eV2X UEs, an adversary may launch a man-in-the-middle attack on the signalling if the L2 link is not protected. The eV2X UEs may not be able to receive groupcast information or may be directed to the wrong groupcast information.

### 5.5.3 Potential security requirements

NOTE: No security requirements are addressed in the present document.

## 5.6 Key Issue #6: Security of the UE service authorization and revocation

### 5.6.1 Key issue details

KI#5 from TR 23.786 [5] is describing Service Authorization and Provisioning to UE for eV2X communications over PC5 reference point. Secure service authorization and revocation is important for the overall security of the eV2X service.

### 5.6.2 Security threats

An adversary that is capable of compromising the eV2X UE service authorization and revocation procedures can compromise the overall integrity of the eV2X system.

### 5.6.3 Potential security requirements

The 5G System shall secure the eV2X UE Service authorization and revocation.

The eV2X UE Service authorization and revocation procedures shall be confidentiality, integrity, and replay protected.

## 5.7 Key Issue #7: Cross-RAT PC5 control authorization indication

### 5.7.1 Key issue details

In TR 23.786 [5], Solution #6 "eV2X impacts to 5GC procedures" is selected as the baseline for normative work to address KI #6 "Service authorization to NG-RAN for eV2X communications over PC5 reference Point". It is mentioned that the AMF obtains the cross-RAT control authorization from UDM and includes it in the NGAP message sent to NG-RAN.

"*The cross-RAT PC5 control authorization indicates whether LTE Uu controls LTE and/or NR sidelink from the cellular network, and whether NR Uu controls LTE and/or NR sidelink from the cellular network.* "

However no IE has been defined for the cross-RAT PC5 control authorization indication.

"*Stage 3 will decide if an explicit cross-RAT PC5 control authorization IE is needed for the signaling over N2, or it can be indicated in an implicit manner.* "

### 5.7.2 Security threats

Lack of proper indication method of cross-RAT control authorization will result in hindrance of service authorization to NG-RAN.

### 5.7.3 Potential security requirements

The 5G system shall have a means to efficiently manage the cross-RAT PC5 control authorization.

## 5.8 Key Issue #8: Privacy protection for broadcast messages over PC5

### 5.8.1 Key issue details

Key issue #3 addresses the needs of privacy protection for groupcast communication over PC5. Similar to groupcast, broadcast is also 1-to-many communication mode where there are multiple recipients of the message, except that the number of recipients in broadcast mode is unknown. If the same L2 ID is used by a UE for a certain period of time, it is possible to track and identify the source of the message.

It should be noted that other V2X technologies (e.g. IEEE 1609 and ETSI ITS) which are based on IEEE 802.11p [14] define communication modes equivalent to "broadcast", "groupcast", and "unicast" mode. In these standards, the use of "pseudonym" for privacy protection purpose is applicable to all communication modes. On the contrary, TS 23.287 [4] clause 6.3.3.2 discusses the periodic L2 ID change in unicast mode only.

According to TS 23.287 [4] clauses 5.1.2.1 and 5.6.1.1, the privacy support requirement is determined based on the type of V2X service (e.g. PSIDs or ITS-AIDs of the V2X applications), and it is independent of the type of communication mode (i.e. broadcast, groupcast, and unicast). Therefore, it means that privacy requirement is applicable to all communication modes.

It should be noted that, in broadcast mode, any entity can receive the messages and who should receive the messages is not managed (i.e. it is not known who is listening). In this respect, the privacy needs in broadcast mode is even more acute than unicast or groupcast modes.

### 5.8.2 Security threats

An adversary that is capable of connecting and linking L2 identities to a real or a long-term eV2X endpoint identity will be able to track and trace the endpoint in space and time. Such trackability and linkability will be a privacy attack on eV2X endpoint that transmits the broadcast messages.

### 5.8.3 Potential security requirements

The 5G System shall provide means for mitigating linkability attacks on L2 identities in eV2X broadcast communications.

The 5G System shall provide means for mitigating trackability attacks on L2 identities in eV2X broadcast communications.

## 5.9 Key Issue #9: Minimizing the impact of privacy protection mechanism in the application layer communication

### 5.9.1 Key issue details

Key issues in KI #1, #3, and #8 describes the need for privacy protection in unicast, groupcast, and broadcast modes. The solution for this requirement is met by introducing a mechanism where the UE periodically changes its L2 ID and communicate it to the peer UE(s). This procedure is also described in the eV2X stage 2 in TS 23.287 [4] clause 6.3.3.2.

It should be noted that the application layer is unaware of such lower layer identity change. This implies that it is a normal course of event where the L2 ID of the communication session changes while the application layer communication continues over a longer period of time. In this scenario, the application layer communication should not be disrupted (i.e. should not be lost or delayed more than a tolerable threshold in low latency V2X communication over PC5 interface). Given that typical V2X communication over PC5 interface require very low latency such as basic safety messages to avoid collision, etc., delay or loss of application communication may potentially results in the difference between accident and no-accident.

The example scenario below illustrates the situation where the L2 ID change event can potentially cause disruption in the application layer communication.



Figure 5.9.1-1: Relative timing of application layer and L2 ID update events (unicast mode)

The event (C) in Figure 5.9.1-1 indicates that the receiving UE is not able to correctly receive the application layer message. It is due to the fact that the application layer event and L2 ID update event occur independently, combined with the relative timing difference of when the new L2 ID becomes effective in both sending and receiving UEs.

Situation such as this needs to be avoided.

In addition, in case of groupcast or broadcast mode where there are multiple peer UEs present in the communication, L2 ID update request message (message #1) may be missed by one or more of the peer UEs. In such case, synchronized L2 ID update by all member UEs is an extra challenge to ensure application layer messages are correctly received by all member UEs.

One possible solution is the sending UE to buffer the application layer messages until the L2 ID change procedure is completed by all UEs involved. However, considering the potential consequence described above, buffering will only lead to delay, thus it is not an acceptable solution in the environment where reliable and low latency communication is mandatory (basic safety messages). Therefore, different solution is needed to ensure all UEs in the communication can receive application layer messages at all time independent of the periodic L2 ID update event.

### 5.9.2 Security threats

NOTE: No security threats are addressed in the present document.

### 5.9.3 Potential security requirements

NOTE: No security requirements are addressed in the present document.

## 5.10 Key Issue #10: UP security policy handling for PC5 and Uu interface

### 5.10.1 Key issue details

This key issue addresses the security aspects of key issue #22: Support for operation modes selection for V2V communications in TR 23.795 [9].

According to the TR 23.795 [9], V2V should be supported via PC5 mode for direct V2V communication and/or Uu mode for indirect V2V communication considering KPI improvement. Solution #27: Switching the mode of operation for V2V communications controlled by network and triggered by V2X Application Enabler (VAE) was proposed, i.e.

- The V2X Application Enabler (VAE) server triggers switching the user plane configuration from direct (PC5) to in-direct (Uu) V2V, when the side-link conditions/QoS are expected to downgrade for single or pre-defined group of V2X-UEs (e.g. based on information from V2X UEs or from V2X application specific server).

- The VAE server triggers switching the user plane configuration from indirect (Uu) to direct (PC5) V2V, when the resource situation or network QoS are expected to downgrade for single or pre-defined group of V2X-UEs (based on the received monitoring events and/or network analytics).



Figure 5.10.1-1: Switching from direct (PC5) to indirect (Uu) V2V communications

For the Uu interface, 5G network already defined the on-demand user plane security mechanism to support the flexibility UP protection according to the DNN, or NSSAI. However, after switching from Uu to PC5, the Uu data will be transferred within the PC5 interface. The 5G network may enforce different activation on user data sent via PC5 and Uu. In this case, the attacker may perform some attacking methods (e.g. jamming) to trigger the communication mode switch for user data attack.

### 5.10.2 Security threats

If the attacker knows that confidentiality protection is enabled on PC5 not on the Uu, the attacker could perform jamming on the PC5 interface, in order to trigger the communication mode switch from PC5 to Uu, and then intercept the data transferred over the Uu interface. For the integrity protection, the attacker can similarly trigger the switching to degrade the data protection, and modify the user data.

### 5.10.3 Potential security requirements

If encryption of user plane data is enabled on the PC5, then encryption shall be enabled for Uu as well after switching from PC5 to Uu, and vice versa.

If integrity protection of user plane data is enabled on the PC5, then integrity protection shall be enabled for Uu as well after switching from PC5 to Uu, and vice versa.

## 5.11 Key Issue #11: Security for eV2X broadcast messages over PC5

### 5.11.1 Key issue details

In TR 23.786 [5] and key issues in previous clauses, the security of the unicast and groupcast communication over PC5 has been mentioned. However, the security of broadcast communication has not been mentioned. Broadcast messages in some cases may be sent by a UE periodically to inform the other vehicles about its driving status or it may be event-driven where information about a specific event is being broadcasted. The attacks on such messages may lead to the receiving UEs being misinformed about the road conditions or may lead them to take wrong decisions. Hence the security of broadcast messages is also to be considered.

### 5.11.2 Security threats

An adversary that can maliciously modify broadcast input may mislead the receiving UEs to make wrong decision/action. Maliciously deleted messages may cause the receiving UE to fail to take action in time. Replayed messages may cause wrong status of the road conditions for the receiving UEs.

### 5.11.3 Potential security requirements

NOTE: No security requirements are addressed in the present document.

# 6 Solutions

## 6.1 Solution #1: Privacy protection for unicast messages over PC5

### 6.1.1 Introduction

This solution addresses key issue #1: Privacy protection for unicast messages over PC5.

The following solution mitigates the trackability and linkability attacks by enabling both UEs to update their L2 ID and the Kd session ID (definition below) simultaneously. It allows the UE to avoid having its previously used L2 identifier being indirectly associated with the Kd session ID and/or with its peer UE's L2 ID. This is to be contrasted with the Link identifier update for a unicast link procedure specified in TS 23.287 [4], which is considering only the initiating UE changing its L2 ID, which is not considering the trackability based on the Kd session ID and the peer's L2 ID.

This solution assumes that a security association identifier for the specific link (called Kd session ID) is used to identify and/or retrieve the corresponding security context as specified in TS 33.303 [6]. Kd session ID is created by concatenating the identifier components from each peer, i.e. the Most Significant Byte (MSB) of Kd session ID is from the initiating UE and the Least Significant Byte (LSB) of Kd session ID is from the peer UE. Kd session ID is transmitted with each packet as part of the PDCP header.

In this solution, UEs involved in a unicast communication update their identifiers simultaneously, i.e., within the same procedure. The identifiers (i.e. L2 IDs and the Kd session ID), included as cleartext within messages sent over the unicast communication, are being changed. Both UEs start using the new identifiers once the procedure is completed.

The initiating UE generates a new L2 ID and its portion of the Kd session ID. The initiating UE sends its new identifiers to a peer UE. The peer UE receiving these new identifiers also generates a new L2 ID and its own portion of the Kd session ID. The peer UE sends its new identifiers to the initiating UE and sends back the received identifiers from the initiating UE to acknowledge them. The initiating UE receiving the new identifiers from its peer UE completes the procedure by acknowledging their reception. A three-way message exchange procedure is required with this solution since both UEs need to change their identifiers during the same procedure and since these new values need to be acknowledged by the peer/initiating UEs prior to start using them.

All messages exchanged during this procedure involve the exchange of new identifiers. These new identifiers, i.e., L2 ID and Kd session ID, need to be confidentiality protected to circumvent linkage between the old L2 IDs and new L2 IDs since the messages exchanged between the peers use the old L2 IDs and old Kd session ID until the procedure is completed and newly assigned identities are accepted. The new identities are being sent as a payload of the previously established (e.g., unicast) communication and are protected as such. Once the procedure is completed, both UEs start using the new identifiers, i.e. new L2 IDs and new Kd session ID.

NOTE: Although this solution focuses on confidentiality protection, integrity and replay protection is also possible using the established security association.

### 6.1.2 Solution details

Figure 6.1.2-1 details procedure for Privacy protection for unicast messages over PC5.



Figure 6.1.2-1 Procedure for Privacy protection for unicast messages over PC5

0) The initiating UE and peer UE have a protected unicast communication established, providing confidentiality, integrity, and replay protection of messages in Steps 2, 4, and 6.

1) The initiating UE generates its new L2 identifier and a new MSB of the Kd session ID. Initiating UE may have received a trigger, e.g. from the upper layer or a timer expiration.

2) The initiating UE sends the newly generated identifiers to the peer UE via the already established unicast communication. The new identifiers are sent as message payload thus are confidentiality, integrity and replay protected. The old identifiers are still used for sending of Message 2, i.e., included within their respective PDUs header(s) (V2X, PDCP), thus sent in cleartext.

3) The peer UE saves locally the received new identifiers from the initiating UE. The peers UE generates new identifiers as well, i.e. a new peer UE's L2 ID and a new LSB of the Kd session ID.

4) The peer UE acknowledges the reception of the initiating UE's new identifiers by sending a response message to the initiating UE and may specify the received initiating UE's new identifiers. Peer UE also sends its own new identifiers as message payload.

5) The initiating UE saves locally the received new identifiers from the peer UE.

6) The initiating UE acknowledges the reception of the peer UE's new identifiers by sending an acknowledgement message to the peer UE and may include the received peer UE's new identifiers as message payload.

7) The initiating UE starts using its new identifiers, i.e. new L2 IDs and new Kd session ID.

8) The peer UE receives the acknowledgement from the initiating UE and starts using the new identifiers, i.e., new L2 IDs and new Kd session ID.

NOTE: It is a part of the Stage 2 work to decide if other PC5 messages besides Link Identifier Update Request/Response may be used to exchange the L2 IDs and Kd session IDs.

### 6.1.3 Evaluation

Solution #1 fully addresses requirements from Key Issue #1: Privacy protection for unicast messages over PC5.

This solution mitigates the trackability and linkability attacks by enabling both participating UEs to update their L2 IDs and the Kd session ID simultaneously. It also allows the participating UEs to avoid the indirect association between the previously used L2 identifier and the Kd session ID with L2 ID of its peer UE.

L2 ID tracking is possible since the source and destination L2 IDs, which identify a PC5 unicast communication, are sent as cleartext with each PC5 message. In addition, the security (i.e., confidentiality and integrity protection) handled at the PDCP layer is using a Kd session ID that is also sent in cleartext in the PDCP header of each PC5 message.

Per clause 6.1.1, a privacy protection mechanism for long duration unicast communication over PC5 is needed to avoid L2 ID tracking.

However, the existing procedure adopted in TS 23.287 [4] (i.e., Link Identifier Update procedure) is enabling only one of the participating UEs to change its L2 ID at a time. Therefore, the existing procedure does not mitigate trackability and linkability attacks from an eavesdropper who can follow the Link Identifier Update procedure and link the old source L2 ID with the new source L2 ID of a participating UE, by passively observing the Kd session ID and/or the destination L2 ID which are left unchanged and exchanged in cleartext before, during, and after the L2 ID update procedure.

## 6.2 Solution #2: Security for eV2X unicast messages over PC5

### 6.2.1 Introduction

This solution addresses key issue #2: Security for eV2X unicast messages over PC5 and more specifically the "V2X Service oriented" method.

During the unicast link establishment, a security association is created between the peer UEs. Each peer UE keeps locally a security context containing confidentiality and integrity keys. Each peer UE uses a portion of the session identifier (i.e., Kd session ID) to identify and retrieve the security context/keys when a message is received (to check its integrity and/or decrypt it) or when a message needs to be sent (to encrypt it and/or protect it for integrity). The session identifier is created by concatenating identifier components from each peer UE, i.e. the Most Significant Byte (MSB) of Kd session ID is from the initiating UE and the Least Significant Byte (LSB) of Kd session ID is from the peer UE. Each UE uses its portion of the Kd session ID (i.e., MSB or LSB) to retrieve the security context associated to the link.

The initiating UE broadcasts a Direct Communication Request (DCR) message announcing a V2X service. This initial message is solely used as an announcement message, i.e., no response is expected to be received. Instead, each peer UE receiving the broadcast message and interested in the announced V2X service initiates a unicast link establishment procedure, i.e., each peer UE generates an MSB of the Kd session ID, creates a security context, and sends a DCR message to the initiating UE specifying the announced V2X service and its generated MSB of Kd session ID. The initiating UE, upon receiving a DCR message, creates a unique security context, saves the received MSB of Kd session ID, generates a LSB of session ID, derives the security keys, and responds to the peer UE by sending a Direct Security Mode (DSM) Command message including the LSB of Kd session ID. The peer UE, upon receiving the DSM Command message from the source UE, updates its local security context, derives the security keys, and sends back a DSM Complete message. The initiating UE completes the unicast link establishment by sending a Direct Communication Accept (DCA) message to the peer UE.

This solution ensures that a different security context is established for each peer UE during the V2X unicast link establishment using the V2X Service-oriented method. An issue with existing procedures in [4] TS 23.287 and [6] TS 33.303 stems from the fact that all interested UEs reply to the same broadcast DCR message that includes the MSB of Kd session ID from the initiating UE. When all interested UEs send back a DSM message to create a security association with the initiating UE, they all get associated to the same security context, identified by the MSB of Kd session ID on the initiating UE. To ensure that the initiating UE is able to establish a different security context for each peer UEs during the V2X unicast link establishment, the procedure avoids having the same MSB of Kd session ID being referred to by multiple peer UEs sending a DSM Command message as a response to the broadcast DCR message announcing a V2X service. Instead, each peer UEs allocates its MSB of Kd session ID and includes it in a reply using a DCR message. The initiating UE allocates a unique LSB of Kd session ID per received DCR message (i.e. per peer UE) to identify the corresponding security context and replies by initiating the Direct Security Mode procedure. This solution mitigates man-in-the-middle attacks during V2X unicast link security establishment between the initiating UE and each peer UE by using the protection provided by existing DSM Command/Complete mechanism.

### 6.2.2 Solution details

The solution shown in Figure 6.2.2-1 details a procedure for Security for eV2X unicast messages over PC5.



Figure 6.2.2-1: Procedure for Security for eV2X unicast messages over PC5

1. The initiating UE broadcasts a DCR message to announce a V2X service.

2. The peer UE1 is interested by the announced V2X service. It initiates the unicast communication establishment with initiating UE. The peer UE1 generates the MSB of Kd session ID and sends it via a DCR message to the initiating UE, specifying the V2X service it is interested in. A security context is created.

2a. The peer UE3 is also interested by the announced V2X service so it initiates a unicast link communication with initiating UE. An MSB of Kd session ID is generated and sent to the initiating UE together with the V2X service.

3. The initiating UE receiving a DCR message from the peer UE1 creates a security context and saves the received MSB of Kd session ID. An LSB of Kd session is generated and saved into the security context. The LSB of Kd session is sent to the peer UE1 using DSM Command message.

3a. The initiating UE also receives a DCR message from the peer UE3. It creates another security context and saves the received MSB of Kd session ID. Another LSB of Kd session is generated and saved into this security context. The corresponding LSB of Kd session is sent to the peer UE3 using DSM Command message.

4. The peer UE1 updates its security context with the received LSB of Kd session ID and replies with a DSM Complete message.

4a. The peer UE3 also updates its security context with the received LSB of Kd session ID and replies with a DSM Complete message.

5. The initiating UE completes the unicast link establishment by sending a DCA message to the peer UE1.

5a. Same thing with the peer UE3, i.e. the initiating UE completes the unicast link establishment by sending a DCA message to the peer UE3

### 6.2.3 Evaluation

Solution #2 fully addresses key issue #2: Security for eV2X unicast messages over PC5 requirements.

This solution ensures that a different security context is established for each peer UE during the V2X unicast link establishment using the V2X Service-oriented method.

The V2X Service-oriented method adopted in TS 23.287 [4] combines the Discovery procedure, i.e., advertisement of supported V2X services, with the establishment of a unicast link. Using this method, the DCR message, which is the first message sent during the Unicast Link Establishment procedure, is used by a UE to announce the V2X service it supports and, at the same time, to initiate the establishment of a unicast link. Note that the DCR message is broadcasted instead of being sent to a specific UE.

As described in clause 6.2.1, the DCR message is associated with a unique security context identifier which is allocated in the initiating UE. The UEs interested in the announced V2X service proceed with the Unicast Link Establishment procedure by replying to the received DCR message.

The problem at hand stems from the combination of the Discovery and Unicast Link Establishment procedures. To remedy this problem, the Solution #2 decouples these two procedures by using the existing initial DCR message for initiating the Discovery procedure and using a second DCR "reply" message to proceed with the Unicast Link Establishment procedure for the responding UEs. By using this solution, the initiating UE is able to establish a different security context for each peer UE when receiving a DCR "reply" message.

## 6.3 Solution #3: Security for eV2X unicast messages over PC5

### 6.3.1 Introduction

This solution addresses key issue #2: Security for eV2X unicast messages over PC5 and more specifically the "V2X Service oriented" method.

NOTE: This solution adheres to eV2X architecture (TS 23.287 [4]).

During the unicast link establishment, a security association is created between the peer UEs to be able to secure the link. Each peer UE keeps locally its security context containing keys to encrypt/decrypt messages and to integrity protect them. A portion of the session identifier (i.e., Kd session ID) is used by each peer UE to identify and retrieve the security context/keys when a message is received (to check its integrity and/or decrypt it) or when a message needs to be sent (to encrypt it and/or protect it for integrity). The session identifier is created by concatenating identifier components from each peer, i.e. the Most Significant Byte (MSB) of Kd session ID is from the initiating UE and the Least Significant Byte (LSB) of Kd session ID is from the peer UE. Each UE uses its portion of the Kd session ID (i.e. MSB or LSB) to retrieve the security context associated to the link. The security context is used at the PDCP layer and only the MSB/LSB of Kd session ID are used to retrieve the security context (as opposed to L2 IDs).

In contrast to solution #2, this solution proposes modifications to be handled at the PDCP layer (i.e. local security context retrieval) while solution #2 requires handling at the eV2X layer (i.e. unicast link establishment procedure). Further, compared solution #2, the initiating UE uses the entire session identifier (i.e., Kd session ID) to retrieve the security context associated with the link instead of using a portion of it, i.e. the MSB of Kd session ID.

In case of a second peer UE sending an SMC message containing the same LSB of Kd session ID than a first peer UE, the initiating UE rejects the second peer UE SMC. The second peer UE retries the SMC procedure with a different value for LSB Kd session ID so that initiating UE uses a unique Kd session ID for each peer UE.

The initiating UE generates the MSB of Kd session ID and broadcasts a Direct Communication Request (DCR) message including the announced V2X service and the MSB of Kd session ID. Each peer UE receiving the broadcast message and interested in the announced V2X service generates an LSB of the Kd session ID, creates a security context associated with the Kd session ID and sends a Direct Security Mode (DSM) Command message to the initiating UE specifying the announced V2X service and its generated LSB of Kd session ID. The initiating UE, upon receiving a DSM Command message, forms the session identifier by concatenating the MSB and LSB of the Kd session ID, creates a unique security context to be associated with the Kd session ID, saves the received LSB of Kd session ID with its previously generated MSB of Kd session ID in this context, and derives the security keys. The initiating UE responds to the peer UE by sending a DSM Complete message. The PDCP layers on both UEs use the entire Kd session ID to retrieve the security context (as opposed to only the MSB/LSB of Kd session ID).

This solution ensures that a different security context is established for each peer UE during the V2X unicast link establishment using the V2X Service-oriented method. An issue with existing procedures in [4] TS 23.287 and [6] TS 33.303 stems from the fact that all interested UEs reply to the same broadcast DCR message that includes the MSB of Kd session ID from the initiating UE. When all interested UEs send back DSMs to create a security association with the initiating UE, they get associated to the same security context, identified by the MSB of Kd session ID of the initiating UE. To ensure that the initiating UE establishes a different security context with each peer UE during the V2X unicast link establishment, the procedure avoids having multiple security contexts being associated to the same MSB of Kd session ID when multiple peer UEs send a DSM Command message as a response to the broadcast DCR message announcing a V2X service. To do so, the initiating UE uses the entire Kd session ID to identify the security context for a given peer UE, instead of using only the MSB of Kd session ID. This solution mitigates man-in-the-middle attacks during V2X unicast link security establishment between the initiating UE and each peer UE by using the protection provided by existing DSM Command/Complete mechanism.

### 6.3.2 Solution details

The solution shown in Figure 6.3.2-1 details a procedure for security for eV2X unicast messages over PC5 where the initiating UE uses the entire session identifier (i.e., Kd session ID) to locate the security context.



Figure 6.3.2-1: Procedure for Security for eV2X unicast messages over PC5

1. The initiating UE broadcasts a DCR message to announce a V2X service. An MSB of Kd session ID is specified.

2. The peer UE1 is interested by the announced V2X service so it generates an LSB of Kd session ID and sends it via a DSM Command message to the initiating UE, specifying the V2X service it is interested in. The MSB of Kd session ID received on the DCR message may be specified as well.

2a. The peer UE3 is also interested by the announced V2X service so it generates an LSB of Kd session ID and replies to the initiating UE by sending a DSM Command message which includes the LSB of Kd session ID and the V2X service. The MSB of Kd session ID received on the DCR message may be specified as well.

3. The initiating UE receiving a DSM Command message from the peer UE1 forms the session identifier by concatenating the MSB and LSB of the Kd session ID (i.e. MSB of Kd session ID + LSB of Kd session ID #1). The initiating UE verifies that this session identifier is unique and creates a security context to be associated with this session identifier. The received LSB of Kd session ID and its previously generated MSB of Kd session ID are saved in this context. The initiating UE replies with a DSM Complete message and may specify the received LSB of Kd session ID.

3a.The initiating UE also receives a DSM Command message from the peer UE3. The initiating UE forms a second session identifier by concatenating the MSB of Kd session ID with the LSB of Kd session ID #3, verifies its uniqueness and creates a second security context to be associated with this second session identifier. The initiating UE replies with a DSM Complete message and may specify the received LSB of Kd session ID.

In the case where a LSB of Kd session ID collision (i.e., #3 has the same value as #1) is detected by the initiating UE, the initiating UE rejects the Direct Security Mode Command message (i.e. sends a Direct Security Mode Reject message) with a cause value specifying that the LSB of Kd session ID is not unique. The peer UE3 receiving a Direct Security Mode Reject message looks at the cause value and if the cause is related to the session identifier uniqueness then the peer UE3 generates a new LSB of Kd session ID and replies to the initiating UE again (i.e. sends a DSM Command message). The peer UE3 forgets the former LSB of Kd session ID.

4. The peer UE1 completes the unicast link establishment by sending a Direct Communication Accept (DCA) message.

4a. The peer UE3 completes the unicast link establishment by sending a DCA message.

5. The peer UE1 sends a message (i.e. signaling or data message) to the initiating UE. The message may be confidentiality and/or integrity protected. The session identifier is specified on the message.

5a. The initiating UE when receiving this message uses the entire session identifier (i.e. Kd session ID) to retrieve the corresponding security context and check the integrity and/or decrypt the message.

### 6.3.3 Evaluation

Solution #3 fully addresses key issue #2: Security for eV2X unicast messages over PC5 requirements.

This solution ensures that a different security context is established for each peer UE during the V2X unicast link establishment using the V2X Service-oriented method.

Solution #3 adheres to Rel-16 eV2X architecture.

## 6.4 Solution #4: Privacy protection for unicast messages over PC5

### 6.4.1 Introduction

This solution addresses key issue #1: Privacy protection for unicast messages over PC5.

Note: This solution adheres to eV2X architecture (TS 23.287 [4]).

The following solution mitigates the trackability and linkability attacks by enabling both UEs to update their L2 ID and the Kd session ID simultaneously. It allows the UE to avoid having its previously used L2 identifier being indirectly associated with the Kd session ID and/or with its peer UE's L2 ID.

In this solution, UEs involved in a unicast communication update their identifiers simultaneously, i.e., within the same procedure. The identifiers (i.e. L2 IDs and the Kd session ID), included as cleartext within messages sent over the unicast communication, are being changed. UEs start using the new identifiers once the procedure is completed.

This solution assumes that a security association identifier for the specific link (called Kd session ID) is used to identify and/or retrieve the corresponding security context as specified in [6] TS 33.303. Kd session ID is created by concatenating the identifier components from each peer, i.e., the Most Significant Byte (MSB) of Kd session ID is from the initiating UE and the Least Significant Byte (LSB) of KD-sess ID is from the peer UE. Kd session ID is transmitted with each packet as part of the PDCP header. The existing rekeying procedure updates the security context content including its identifier, Kd session ID. This solution adds the possibility of updating the L2 IDs as well during the rekeying procedure.

The initiating UE generates a new L2 ID and triggers the rekeying procedure to update its own portion of the Kd session ID. The initiating UE sends its new identifiers, (i.e., L2 ID and MSB of Kd session ID), to a peer UE using the rekeying procedure. The peer UE, while receiving these new identifiers, also generates a new L2 ID and its own portion of the Kd session ID. The peer UE additionally generates new keys for the encryption and integrity protection and sends its new identifiers to the initiating UE. The initiating UE receiving the new identifiers from its peer UE generates new encryption and integrity protection keys and sends back a message to the peer UE acknowledging the reception of its new identifiers. The peer UE completes the rekeying procedure by sending a response message. All messages exchanged during this procedure involve the transmission of security protected new identifiers. Once the procedure is completed, both UEs start using the new identifiers, i.e. new L2 IDs and new Kd session ID.

### 6.4.2 Solution details

The solution shown in Figure 6.4.2-1 details a procedure for Privacy protection for unicast messages over PC5. The rekeying procedure is updated with the ability to exchange the new initiating and peer L2 IDs between the communicating UEs, along with the new Kd session ID.



Figure 6.4.2-1: Procedure for Privacy protection for unicast messages over PC5

0) The initiating UE and peer UE have a unicast communication established.

1) The initiating UE generates its new L2 ID and a new MSB of the Kd session ID. The initiating UE triggers the rekeying procedure to exchange the new identifiers with the peer UE. The initiating UE may have received a trigger, e.g. from the upper layer or a timer expiration.

2) The initiating UE sends the newly generated identifiers to the peer UE via the already established unicast communication. The new identifiers are confidentiality, integrity and replay protected and sent as message payload. The old identifiers are still used for sending of Message 2, i.e., included within their respective PDU header(s) (V2X/PDCP).

3) The peer UE generates new identifiers as well, i.e., a new L2 ID and a new LSB of the Kd session ID. The peer UE saves locally the received new identifiers from the initiating UE. The peer UE updates the security association with the new Kd session ID and generates new keys.

4) The peer UE acknowledges the reception of the initiating UE's new identifiers by sending its own new identifiers, i.e., its new L2 ID and new LSB of Kd session ID and may also include the initiating UE's new identifiers. Those identifiers are confidentiality, integrity and replay protected and sent as message payload. The rekeying procedure is assumed to be performed with an already established security context. The L2 IDs and MSB/LSB of Kd session ID IEs are ciphered using the available security context while the whole DSM message is integrity protected also using the available security context (this is similar to the partial ciphering functionality on Uu as per [8] TS 33.501, clause 6.4.6).

5) The initiating UE saves locally the received new identifiers from the peer UE. New keys are generated. The security association is updated with the new Kd session ID and the new keys.

6) The initiating UE acknowledges the reception of the peer UE's new identifiers and may send them back to the peer UE to do so. The DSM Complete is confidentiality and integrity protected using the new security context as per existing procedure.

7) The peer UE receives the acknowledgement from the initiating UE and completes the rekeying procedure.

8) From this point on, the UEs use the new identifiers and security keys for their communication, i.e., new L2 IDs, new Kd session ID and new keys for security protection.

NOTE: It is left to Stage 2 work to decide if other PC5 messages besides Direct Rekeying Request/Response may additionally be used to exchange the L2 IDs and Kd session ID.

### 6.4.3 Evaluation

Solution #4 addresses key issue #1: Privacy protection for unicast messages over PC5 requirements.

This solution mitigates trackability and linkability attacks by enabling both UEs to update their L2 ID and the Kd session ID simultaneously. It also enables the UE to avoid having its previously used L2 identifier being indirectly associated with the Kd session ID and/or with its peer UE's L2 ID.

Solution #4 adheres to Rel-16 eV2X architecture.

During a unicast communication, there is a need to periodically run the Rekeying procedure and the Link Identifier Update procedure. In some cases, these procedures, involving exchange of signalling messages between the peer UEs, need to be executed one after another. In these scenarios, adding the Link Identifier Update functionality to the Rekeying procedure considerably reduces the signalling load between two peers and the associated signaling overhead by avoiding the execution of two procedures one after the other (e.g., back to back).

This improvement, while reducing the signalling overhead, comes with the cost of having to partially cipher the DSM Command message since the new IDs have to be exchanged confidentiality protected. For that, the initiating UE sends the DSM Command message with the existing IEs (e.g. Sequence Number, UE Security Capabilities, etc.) in cleartext, as usual. Only the new L2 IDs and new Kd session ID, added to the DSM Command message, are ciphered using the existing security context. The whole DSM Command message is integrity protected.

Hence, the incremental complexity of doing partial ciphering on the UE is minimal and justified due to the savings achieved by the reduction of signalling overhead between the UEs.

## 6.5 Solution #5: Security protection of service authorisation

### 6.5.1 Introduction

This solution addresses key issue #6 'Security of the UE service authorization and revocation' in clause 5.6.

### 6.5.2 Solution details

The procedures of V2X service authorisation is specified in clause 5.1 of TS 23.287 [4], and allow RAT(s) per PLMN basis are provisioned by PCF to UE or by Application server via PCF. The protection of the procedures is provided by security procedures in TS 33.501 [8].

NOTE: Mitigation of misbehaviour of unauthorised UE(s) for V2X communication over PC5 could be supported in the application layer.

### 6.5.3 Evaluation

NOTE: No evaluation is addressed in the present document.

## 6.6 Solution #6: V2X Group Key Provisioning

### 6.6.1 Introduction

This solution addresses Key Issue #5 by secure provisioning of the group key for multicast via NAS signalling. The normal procedures for UDM – 3rd party AS exposure are reused via NEF for the interaction between UDM and V2X Key Management Server (KMF).

### 6.6.2 Solution details

The V2X Key Management Server (KMF) may be co-located with the V2X AS and is responsible for the group key management.



Figure 6.6.2-1: Group Key Provisioning via NAS Transport

1. The UE may send a UE Policy Provisioning Request to the PCF to retrieve keys for one or more V2X Group IDs within a NAS uplink NAS transport message. The UE includes in the NAS message a V2X Security Container that contains the UEs security capabilities and one or more Group IDs (identified by destination layer-2 ID) that the UE is interested to retrieve updated keys.

2. The AMF transparently forwards the message to the PCF within an Npcf\_UEPolicyControl\_Update service message.

3. The PCF extracts the information from the V2X Security Container and retrieves the V2X Security Context(s) (V2X Group Key (VGK), VGK ID, encryption algorithm identifier and expiry time) from the V2X Key Management Function. The PCF then provides the retrieved V2X Security Context(s) to the UE by updating the V2X configuration information. The PCF may use the exposure service via NEF.

4. The PCF sends a UE Configuration Update message for transparent policy delivery (as defined in clause 4.2.4.3 of TS 23.502 [13]) to the UE via AMF in a Namf\_N1N2Communication message. The UE Configuration Update message includes an additional container that includes the V2X Security Context(s) for the group ID(s) according to the UE's request.

5. The AMF forwards the UE Configuration Update message to the UE.

### 6.6.3 Evaluation

NOTE: No evaluation is addressed in the present document.

## 6.7 Solution #7: Cross-RAT PC5 control authorization indication

### 6.7.1 Introduction

This solution address key issue #7 'Cross-RAT PC5 control authorization indication' in clause 5.7. It is applicable for unicast mode as V2X communication over Uu reference point is only unicast.

### 6.7.2 Solution details

A new field 'Cross-RAT PC5 type', is added in the Access and Mobility subscription data type to indicate whether LTE Uu controls LTE and/or NR sidelink from the cellular network, and whether NR Uu controls LTE and/or NR sidelink from the cellular network.

'Cross-RAT PC5 type' is obtained by the AMF from the UDM as a part of the subscription data during the registration procedure and stores it as a part of the UE context. This information is included in the NGAP message from AMF to NG-RAN, which it uses for the resource management of UE's PC5 transmission for V2X services in network scheduled mode.

If cross-RAT PC5 control authorization indication information is to be changed, the AMF notifies NG-RAN via the NGAP UE Context Modification Request message.

The integrity protection of this new field is provided by security procedures in TS 33.501 [8].

### 6.7.3 Evaluation

This solution addresses the requirements of the key issue #7. The protection of the new field 'Cross RAT PC5' type can be addressed by NDS.

## 6.8 Solution #8: Deriving PC5 layer keys based on higher layer keys

### 6.8.1 Introduction

This solution address part of key issue #2 on security for eV2X unicast messages over PC5. In particular, the solution covers the establishment of PC5 security from existing V2X keys that are used to provide security above the PC5 layer.

### 6.8.2 Solution details

This solution assumes that there are keys in the UE that are related to an application that can be used for the purposes of providing security for that application. These keys do not have to belong to a specific application but could be used for several applications (whether these different apps run over the same PC5 bearer or not is outside the scope of this solution).

The UE can be provisioned with information (which may be based on local regulatory requirements) on what security is allowed and/or needed for each of the V2X service.

The solution is to not standardise a particular method of generating KD but rather provide a framework and available IEs in the PC5 signalling in the 3GPP specification to allow multiple methods of establishing KD to work. This is in effect a future proof approach to establishing V2X security at the PC5 layer by taking advantage of the effort of multiple standards fora. It means that any methods for establishing KD could be quickly deployed without the needs for standardisation work in 3GPP.

The below message flows assume the security properties of ProSe one-to-one-link establishment in terms of handling KD ID, establishment of KD-sess etc – see clause 6.5 of TS 33.303 [6]. The interface between the application layer and PC5 layer internal to the UE is not proposed to be standardised. They are shown to clarify the responsibility of each layer.

The Key\_Est\_Info in the below flow carries the necessary information for the application layer to establish the keys. At each step of the flow (and the possible multiple times that step 3 can be run), the Key\_Est\_Info contains different data required for key establishment at the application layer, but such data is transparent to the PC5 layer.

The following figure shows the message flows for establishing security at PC5 using the key established at the layer above PC5.



Figure 6.8.2-1: Message flow for the establishment of PC5 security using app layer keys

The steps are as follows:

1. The application layer in vehicle 1 determines it needs to establish a PC5 connection with vehicle 2.

a. The application layer sends the relevant Key\_Est\_Info to the PC5 layer.

b. The PC5 layer of vehicle 1 sends the Direct Connection Request message including the Key\_Est\_Info received from the application layer to vehicle 2.

c. The PC5 layer in vehicle 2 passes the received Key\_Est\_Info to the application layer in vehicle 2.

2. This step is optional and is omitted if the establishment of KD is completed without needing further information from vehicle 1. In such a case, step 3 is also omitted and the flow proceeds with step 5.

a. The application layer in vehicle 2 sends Key\_Est\_Info to the PC5 layer of vehicle 2. KD is also be sent if available.

b. The PC5 layer in Vehicle 2 sends a Direct Auth and Key Establish message (see clause 6.5.5.2 of TS 33.303 [6]) including the Key\_Est\_Info to vehicle 1.

c. The PC5 layer in vehicle 1 passes the Key\_Est\_Info to the application layer of vehicle 1.

3. This step is optional and is omitted if the establishment of KD is completed without needing further information from vehicle 2. If used, it can be repeated multiple times and is a step 4 (with mandatory Key\_Est\_Info) followed by a Step 2.

4. This step is only used if step 2 is performed.

a. The application layer in vehicle 1 sends Key\_Est\_Info to the PC5 layer in vehicle 1 if further information from vehicle 1 is needed to complete the establishment of KD. KD can also be sent if available.

b. The PC5 layer of vehicle 1 sends the Key\_Est\_Info (if any) to the PC5 layer of vehicle 2.

c. If any Key\_Est\_Info was received, the PC5 layer of vehicle 2 passes the received Key\_Est\_Info to the application layer of vehicle 2.

5. Step 5a is only needed if steps 2 to 4 were omitted or step 4c was performed.

a. The application layer in vehicle 2 sends Key\_Est\_Info if any further information from vehicle 2 is needed to complete the authentication to the PCS layer of vehicle 2. KD can also be sent if available.

b. The PC5 layer of vehicle 2 sends a Direct Security Mode Command to the PC5 layer of vehicle 1 including any Key\_Est\_Info provided if any in step 5a.

c. If the Direct Security Mode Command contained Key\_Est\_Info, then the PC5 layer of vehicle 1 passes this onto the application layer of vehicle 1.

6. Step 6a is only needed if step 5c was performed.

a. The application layer in vehicle 1 sends KD to the PC5 layer in vehicle 1.

b. The PC5 layer in vehicle sends the Direct Security Mode Command to the PC5 layer of vehicle 1. At this point, the PC5-RRC and PC5-S signalling protection are successfully activated.

NOTE: PC5-RRC will use the same algorithms for confidentiality and integrity protection that were chosen for PC5-S. Hence, from this point, both PC5-S and PC5-RRC messages can be confidentiality and integrity protected except further Direct Security Mode Command messages which will only be integrity protected using the new security context.

7. The PC5 layer in vehicle 2 responds with the Direct Communication Accept message

The Key\_Est\_Info is a transparent container as far as the PC5 signalling is concerned, i.e. the PC5 layer does not need to understand the contents. 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.

### 6.8.3 Evaluation

The use of a generic container for carrying the key establishment traffic has the advantage that it allows new key establishment methods to be introduced without 3GPP involvement. This means that a standards organisation other than 3GPP can define a new method of creating the PC5 layer keys without requiring standardisation in 3GPP specification. This is particularly relevant for V2X as this is an industry that has spent much time working on security solution that need to satisfy quite rigorous privacy regulation(s) which are often region specific. Also use of these different authentication methods and their corresponding application specific credentials will be needed as it is not clear that there will be one global solution that can meet all V2X deployment needs.

At the same time, this proposal does not prevent 3GPP from developing a solution, if a need arises at a later date. This could be done by, simply specifying the information elements needed for the authentication method and how they are included in the generic container for each message between the UEs. Hence this approach provides the flexibility to use authentication methods that can be standardised both inside and outside of 3GPP without requiring a change to PC5 layer implementations and the Information Elements carried on the PC5 interface.

The privacy mechanisms given in clauses 5.6.1.1 and 6.3.3.2 of TS 23.287 [4] provide privacy protection of the UEs involved in the unicast session from other UEs and/or attackers tracking them based on the PC5 parameters sent as part of the PC5 transmissions. In order to get privacy protection from the other participant in the unicast session, it is necessary to drop the unicast connection and re-initialise it with a different long term credential. This provides further justification for allowing the unicast session to be based on higher layer keys as it prevents the need to co-ordinate the change of higher layer credentials with PC5 layer credentials in order to preserve the privacy requested by the application.

## 6.9 Solution #9: Security for eV2X unicast messages over PC5 using ECCSI and SAKKE

### 6.9.1 Introduction

This solution addresses Key issue #1 Privacy Protection for unicast messages over PC5 and key issue #2: Security for eV2X unicast messages over PC5 Procedures in this solution is based on one-to-one bearer level security mechanism which is similar to that of ProSe (specified in TS 33.303[6], clause 6.5.7) Solution proposed does not rely on ProSe Architecture.

The solution uses the "Elliptic Curve-based Certificateless Signatures for Identity-based Encryption" (ECCSI) signature scheme, as defined in IETF RFC 6507 [10]. And, Sakai-Kasahara Key Encryption (SAKKE), as defined in IETF RFC 6508 [11] to generate a shared secret that is used as a KD session ID (root key) for establishing a secure connection between the two UEs.

The UEs are provisioned with the required credentials (as defined in IETF RFC 6507 [10] and IETF RFC 6508 [11]) in advance, when the UEs have secure access to their Key Management Server (KMS). The KMS, common root of trust for the UEs, provisions the UEs with a set of credentials for ECCSI and SAKKE schemes.

Upon successful provisioning for ECCSI, each UE will be configured with the public key of the KMS, and a set of credentials associated with the UE's identity, which are: Secret Signing Key (SSK) and Public Validation Token (PVT). The UE needs to act as "signer" and "verifier." As a signer, the UE uses its SSK to sign a message, and when acting as a verifier, the UE uses the public key of the KMS and the signer's PVT to verify the signature.

Upon successful provisioning for SAKKE, each UE will be configured with the public key of the KMS, and a Receiver Secret Key (RSK) which is associated with the UE's identity. The sender UE uses the receiver's UE identity (receiving entity for SAKKE payload) and the public key of the KMS to create an encrypted SAKKE payload. The receiving UE uses its identity, its Receiver Secret Key and the public key of the KMS to decrypt SAKKE payload.

### 6.9.2 Solution details

#### 6.9.2.1 Initial Security Link Establishment

The solution shown in Figure 6.9.2.1-1 and 6.9.2.1-2 details a procedure for Security for eV2X unicast messages over PC5.



Figure 6.9.2.1-1: Procedure for Security for eV2X unicast messages over PC5 (V2X Service Oriented)



Figure 6.9.2.1-2: Procedure for Security for eV2X unicast messages over PC5 (UE Oriented)

1. UE-1 wishing to engage in one-to-one V2X Direct Communication with UE-2 sends a Direct Communication Request message including the following parameters in addition to parameters described in TS 23.287 [4] clause 6.3.3:

- UE-1 Info = upper-layer information identifying the user of UE-1. This information is used to derive the Signer's identifier (used by ECCSI) as shown in figure 6.9.2.1-1, OR

- V2X Service Info: V2X Service requesting L2 link establishment, e.g., PSID or ITS-AIDs of the V2X application. (Application Layer ID) as shown in figure 6.9.2.1-2

- SIGN – an ECCSI signature (as defined in IETF RFC 6507 [10) of the Direct Communication Request message. The signature is computed over the UE-1 Info parameters or the application based id and the Nonce 1.

2. Upon reception of the Direct Communication Request message, UE-2 verifies the signature payload SIGN. If the verification test is successful, UE-2 presents the authenticated identity ("UE-1 Info") to the UE-2. UE-2 sends a Direct Communication Accept message including the following parameters:

- UE-2 Info = upper-layer information identifying the user of UE-2. This information is used to derive the Signer's identifier (used by ECCSI) as shown in figure 6.9.2.1-1 OR

- Announced V2X Service Info: V2X Service requesting L2 link establishment, e.g. PSID or ITS-AIDs of the V2X application. (Application Layer ID of the UE) as shown in figure 6.9.2.1-2

- SIGN – an ECCSI signature (as defined in IETF RFC 6507 [10]) of the Direct Communication Response message. The signature is computed over the User of UE-2 Info, Nonce 1 and the SAKKE parameters.

SAKKE – UE-2 generates a key Shared Secret Value (SSV), which is used as KD (root key), and encodes SSV value into a SAKKE payload according to the algorithm described in IETF RFC 6508 [11], using the KMS Public Key and the public identity of the of UE-1 o application based id.

Upon receipt of the Direct Communication Accept message, the UE-1 verifies the signature payload SIGN. If the verification test is successful, it decrypts SAKKE payload to extract the SSV which is used as a KD (root key) from which other keys can be derived.

3. Upon successful processing of the Direct Communication Accept message, UE-1 UE completes the unicast link establishment.

Both UEs shall store their own and the other UE's User Info and V2X Service Information with the KD.

This solution protects the unicast message over PC5 by generating the KD session ID, which can be used as anchor keys to generate further keys for the bearer level one-to-one security mechanism. Furthermore, each UE session ID is unique per UE and can be refreshed using the Link update procedure. The solution also provides a mechanism to prevent trackability and linkability attacks by providing a secure mechanism to update the L2 ID and KD Session ID. Link update procedure, as described in clause 6.9.2.2., updates the L2 ID and updates the KD session-id simultaneously.

Credential provisioning services are provided by KMS as per IETF RFC. KMS can reside in the service domain or operator domain. Prose and mission-critical services already have that in the operator domain and controlled by the operator. Similar to prose, provisioning is done after primary authentication in the operator domain. Their credentials are never exposed.

#### 6.9.2.2 Procedure for privacy protection of unicast communication



Figure 6.9.2.2-1: Protection of Link Update Procedure

1. Both UEs have secure PC5 link already established. UE-1 sends a Link Identifier Request to UE-2. This request includes old layer 2 information or UE-1 user information along with other information as described in TS 23.287 [4] clause 6.3.3, i.e. new user information, new upper layer identifiers, new IP address/prefixes, and new L2 IDs, etc.

2. UE-2 responds with a Link Identifier Response including the following parameters:

a) SIGN – an ECCSI signature (as defined in IETF RFC 6507 [10]) of the link update response message. The signature is computed over the User of UE-2 Info or Application ID, Nonce 1 and the SAKKE parameters. In case UE-2 also generates new Layer 2 ID, the signature is computed over the new UE2-layer 2 ID. New UE-2 is also included as payload in the message.

b) SAKKE – UE-2 generates a key Shared Secret Value (SSV), which is used as KD (root key), and encodes SSV value into a SAKKE payload according to the algorithm described in IETF RFC 6508 [11], using the KMS Public Key and the new identity (received in step 1 above) of the user of UE-1.

3. Upon receipt of the Link Update response message, the UE-1 verifies the signature payload SIGN. If the verification test is successful, it decrypts SAKKE payload to extract the SSV which is used as a KD (root key) from which other keys can be derived.

Both UEs shall store their own and the other UE's Info with the KD.

### 6.9.3 Evaluation

Solution #9 addresses key issue #1: Privacy protection for unicast messages over PC5 requirements and key issue #2: Security for eV2X unicast messages over PC5 requirements. Solution #9 adheres to Rel-16 eV2X Architecture.

Confidentiality is achieved by a unique session anchor key per UE.

## 6.10 Solution #10: Privacy protection for unicast message over PC5

### 6.10.1 Introduction

This solution addresses the key issue #1 (Privacy protection for unicast messages over PC5).

The main differences from existing solution #1 and #3 are as follows:

- The procedure verifies the authenticity of the L2 ID update message sent by the UE by introducing a mechanism to include information that allows the receiving UE to verify it. Thus, this procedure allows the peer UE to detect and reject a message injection by malicious UE.

- The procedure aligns with the one defined in TS 23.287 [4] clause 6.3.3.2 (i.e. 2-way message exchange rather than 3-way exchange).

- L2 ID update of one UE does not necessarily mandate the change of L2 ID in the peer UE (i.e. the peer UE can determine by itself when its L2 ID should be updated rather than dictated by the peer UE's action).

### 6.10.2 Solution details

The L2 ID update procedure in unicast communication over PC5 is described in Figure 6.10.2-1.



Figure 6.10.2-1: Procedure for privacy protection for unicast communication over PC5

0. Unicast communication has been established and is in progress.

1. UE1 generates its new L2 ID. At this time, UE1 generates verification information so that the peer UE can verify that this L2 ID change is indeed sent by the legitimate UE that currently uses the L2 ID that the peer UE is aware of in this unicast communication. This verification information may be such as hash result of identities consisting UE1's unique information. For example, input to the hash function may include identities such as currently used L2 ID, newly generated L2 ID, V2X service type (e.g. PSID/ITS-AID), etc.

NOTE: According to TS 23.287 [4], this event is triggered in the UE by, e.g. request from the upper layer or timer expiration as specified in TS 23.287 [4].

2. UE1 sends Link Identifier Update Request message to its peer, UE2, including the UE1's new L2 ID and its verification information.

3. UE2 verifies the received verification information, and checks if the hashed value that UE2 obtained matches the one received in the message in step 2 above. If successful, then UE2 accepts the new L2 ID as the UE1's new L2 ID.

4. UE2 sends Link Identifier Update Response message, including the verification result obtained in step 3.

5. UE1 starts using the new L2 ID in the subsequent messages as the source L2 ID in the unicast communication. UE2 starts accepting the UE1's new L2 ID as the source L2 ID sent from UE1, and starts using UE1's new L2 ID as the destination L2 ID sent from UE2.

### 6.10.3 Evaluation

NOTE: No evaluation is addressed in the present document.

## 6.11 Solution #11: Solution on minimizing the impact of privacy protection mechanism in the application layer communication

### 6.11.1 Introduction

This solution addresses the KI #9, "minimizing the impact of privacy protection mechanism in the application layer communication".

This solution introduces the concept of "time window" in which duplicate application layer messages are sent using 2 different (old and new) L2 IDs (and IP address in case of IP-based communication). This "time window" represents the transition period when the L2 ID is changed from one to another periodically due to the requirement for the privacy protection in communication over PC5 interface.

Duplicate transmission of the application layer message during this transition period ensures that the peer UE to receive the application layer messages successfully independent of the exact timing in which the peer UE switch from the "old" to the "new" L2 ID (and IP address in case of IP-based communication) during the L2 ID update event.

### 6.11.2 Solution details

To ensure the flow of application layer messages is not negatively impacted by the L2 ID update event, the UE that is changing its L2 ID (and its IP address in case of IP-based application) transmit each application layer messages twice within the "timing window" period, using both the old and the new L2 ID (and old and new IP address in case of IP-based application) as the source ID of the application layer messages. This ensures that peer UE is able to receive the application layer messages independent of the relative timing when the peer UE makes transition to start using the new L2 ID (and IP address) and start accepting application layer messages containing the new L2 ID in the source L2 ID field (and IP address in the source IP address field in the IP packet).

The main advantage of this solution is that, it guarantees the peer UE to receive the application layer messages while the L2 ID (or IP address in case of IP-based communication) update of the sender UE takes place independently from the flow of application layer communication.

Figure 6.11.2-1 illustrates this solution.



Figure 6.11.2-1: Procedure for minimizing the impact of privacy protection mechanism in the application communication in groupcast over PC5

0. Unicast communication has been established and is in progress.

1. UE1 determines to update its L2 ID (and its IP address in case of IP-based communication).

NOTE: This event is triggered in the UE by, e.g. request from the upper layer or timer expiration as specified in TS 23.287 [4].

2. UE1 enters the time window to send duplicate application layer messages. It may be triggered by the start of L2 ID update procedure. The L2 ID update messages themselves are not shown to simplify the figure.

3. UE1 sends each application layer message twice, one message using the old L2 ID and another using the new L2 ID (and old and new IP address in case of IP-based communication) as the source address. The dashed line and solid line depict the message that uses the old ID and the new ID, respectively.

The peer UE receives and accepts the application layer message containing either the old or the new L2 ID (or old or new IP address in case of IP-based communication) as the source ID of the message. Which ID the peer UE accepts depends on the timing with respect to the message exchange in the L2 ID update procedure and corresponding switch of ID recognized as UE1.

4. UE1 ends the time window to send duplicate application layer messages as the L2 ID update procedure ends.

5. UE1 sends application layer messages only once using the new L2 ID as the source of the message.

### 6.11.3 Evaluation

NOTE: No evaluation is addressed in the present document.

## 6.12 Solution #12: Protecting the traffic at the PDCP layer

### 6.12.1 Introduction

This solution addresses part of key issue #2 on security for eV2X unicast messages over PC5. In particular, the solution covers the protection at the PDCP layer of signalling and user plane traffic over the PC5 interface and is based on the solution for ProSe in TS 33.303 [6].

### 6.12.2 Solution details

#### 6.12.2.1 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.

All other signalling messages are integrity protected and may be confidentiality protected except the Direct Security Mode Command which is sent integrity protected only.

It is necessary to allocate LCID for bearers that carry signalling messages that are not protected, a bearer to carry Direct Security Mode Command and Direct Security Mode Complete messages, bearers for other signalling messages that are confidentiality and integrity protected and the user plane bearers.

#### 6.12.2.2 Integrity protection

V2X UEs implement NIA0, 128-NIA1 and 128-NIA2 and may implement 128-NIA3 for integrity protection of the relevant bearers

These integrity algorithms are as specified in TS 33.501 [8] and are used with the following modifications;

- The key used is PIK;

- 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 LCID;

- The least significant bits of COUNT[0] to COUNT[31] are filled with Counter and the remaining bits should be filled with some part of KD-sess ID (or equivalent parameter).

The receiving UE ensures that received messages are not replayed.

#### 6.12.2.3 Confidentiality protection

V2X UEs implement NEA0, 128-NEA1 and 128-NEA2 and may implement 128-NEA3 for ciphering of one-to-one traffic.

These ciphering algorithms are as specified in TS 33.501 [8] and are used with the following modifications;

- The key used in PEK;

- Direction is set as for integrity protection (see 6.5.6.2);

- Bearer[0] to Bearer[4] are set to LCID;

- The least significant bits of COUNT[0] to COUNT[31] are filled with Counter and the remaining bits should be filled with some part of KD-sess ID(or equivalent parameter).

#### 6.12.2.4 Security contents in the PCDP header

The Key ID and Counter parameters 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 may be part of KD-sess ID.

This is illustrated in the Figure 6.12.2.4-1.



Figure 6.12.2.4-1: Security contexts of the PDCP header for one-to-one communications

If the configuration is not to use any PDCP protection for one-to-one communication user plane bearers, then the UE sets the values of the security information (Key ID and Counter) to zero in the header of the user plane PDCP packets.

For the signalling messages that are not protected, the Key ID and Counter in PDCP format are set to zeros in the header of the PDCP packet.

### 6.12.3 Evaluation

The solution addressed the requirements of the key issue by introducing a method of protecting the traffic at the PDCP layer. The same security method protects the PC5-S signalling, PC5-RRC signalling and user plane traffic, which avoids the need for deploying more than one security solution.

The solution is similar to the one proposed for ProSe in TS 33.303 [6] and uses the same inputs to the confidentiality and integrity algorithms so that the already deployed algorithms can be re-used without changes.

## 6.13 Solution #13: Solution against V2X UE tracking based on PC5 identifiers

### 6.13.1 Introduction

This solution addresses KI#1:<Privacy protection for unicast messages over>, KI#3:< Privacy protection for groupcast messages over PC5> and KI #8:< Privacy protection for broadcast messages over PC5>.

According to clauses 5.6.1.2 and 5.6.1.3 in TS 23.287 [4], the UE self-selects a source Layer ID for broadcast mode and groupcast mode. It is expected that the UE self-selects a source Layer ID for unicast mode as well.

According to clause 5.6.1.4 in TS 23.287 [4] for unicast mode V2X communication over PC5 reference point, the UE maintains a mapping between the Application Layer IDs and the source Layer-2 IDs used for the PC5 unicast links, as the V2X application layer does not use the Layer-2 IDs. This allows the change of source Layer-2 ID without interrupting the V2X applications. Also, when Application Layer IDs change, the source Layer-2 ID(s) of the PC5 unicast link is changed if the link(s) was used for V2X communication with the changed Application Layer IDs. It is expected that for broadcast mode and groupcast mode V2X communication over PC5 reference point, the UE maintains a similar mapping between the Application Layer IDs and the source Layer-2 IDs used for the PC5 groupcast links and broadcast links.

### 6.13.2 Solution details

The solution is based on the privacy mechanism defined in TS 33.185 [12] for V2X LTE which is intended to mitigate against the threat of tracking the UE by an attacker based on the source Layer 2 ID. This mechanism is described below.

The source Layer-2 ID is randomized and regularly changed in the UE.

The source Layer-2 ID is randomized and changed in the UE when indicated by the V2X application that the application layer identifier has changed.

The UE provides an indication to the V2X application layer whenever the source Layer-2 ID is changed.

### 6.13.3 Evaluation

The randomized self-selection of Layer-2 IDs is adopted as in TS 23.287 [4].

## 6.14 Solution #14: Identifier conversion in groupcast communication

### 6.14.1 Introduction

This solution addresses Key Issue #4 on "Security of identifier conversion in groupcast communication" by updating the L2 ID independently from the application layer group ID, which may never change. The frequency of the update may be depending on the message frequency within the group and is configuration dependent in the V2X AS. In order not to communicate another change of the L2 ID to all group members at the same time, a timer, when all group members change the L2 ID, and a common time basis are signalled to the group member UEs from the V2X AS on application layer signalling. It is assumed that the application layer signalling is security protected.

### 6.14.2 Solution details

The V2X AS creates a virtual time value T as a common time basis that is upon reception at the group member UEs normally increased in the V2X AS and the group member UEs in accordance to their internal clocks in the granularity of seconds, since the virtual time does not rely on the real time received either from the gNB (SIB9) or GPS. The virtual time value is used as an initial secret value and relies on the encrypted application layer signalling to be provisioned in a secure way to the group member UEs. The V2X AS also provides a L2 ID update time interval dT to the group members. Once the group member UEs receive the initial virtual time T and the L2 ID update time interval, they derive the L2 ID using the virtual time value T and the application layer group ID as input to the derivation function. Thus all group member UEs derive the same L2 ID, independently of the transmission delay. The group member UEs then update the virtual time T with the time received either via GPS or SIB9 until the next derivation of the L2 ID according to the L2 ID update time interval a time T+ dT. This update procedure is repeated every L2 ID update time interval in each group member UE until the group member UEs receive a new initial virtual time from the V2X AS.

If a group member does not receive the provisioning message, i.e. the UE is out of coverage of the mobile network, then this UE is also not able to receive the corresponding group messages from the in-coverage group members due to a L2 ID mismatch. This does not matter much since the "out of coverage" UE cannot receive those messages anyway.

Once a "out of coverage" UE recognizes it is back to coverage it is recommended to "re-register" to the V2X AS again to re-sync to the virtual time and update interval.

If one of the UE belonging to the group is still connected to the network, the "out of coverage" UEs belonging the same group ID could receive the provisioning message through an in-coverage UE (i.e., remote UE to NW relay).

Group leader or platoon leader UEs could also provide the provisioning message to the group members locally.

### 6.14.3 Evaluation

The solution fulfils Key Issue #4 on "Security of identifier conversion in groupcast communication" by updating the L2 ID independently from the application layer group ID and has the following characteristics:

- Minimum signalling on application layer to initialize the virtual time for all group members as well as the update interval.

- The frequency of provisioning the virtual time and update interval from the V2X AS can be configured and may not occur frequently at all.

- All group members update the virtual time individually based on their internal clock without dependency of the real time.

- The change to the new destination L2 ID cannot be recognized from outside unless all group members are suddenly sending groupcast messages at the same time.

- Out-of-coverage UEs continue to change their L2 ID based on the previous provisioning message and request an update once returning into coverage.

- The UEs need to have been provisioned at least once.

## 6.15 Solution #15: Solution on minimizing the impact of privacy protection mechanism in the application layer communication

### 6.15.1 Introduction

This solution addresses the KI #9, "minimizing the impact of privacy protection mechanism in the application layer communication".

This solution requires UE to use two different (old and new) identifiers (L2 IDs, Kd Session ID and IP address in case of IP-based communication) for message reception after both UEs updated their identifiers for unicast simultaneously. The feature above allows UE to receive application layer messages even during its peer UE switching identifiers. This solution only proposes additional operations to one.

### 6.15.2 Solution details

To ensure the application layer messages are not interrupted by the identifier switching procedures, the initiating UE and its peer UE exchange messages using established unicast communication. Both UEs are aware of new identifiers (L2 ID, Kd Session ID and IP address in case of IP based application) for this unicast communication by negotiating identifier update messages. The initiating UE listens to messages sent with either the old or the new identifiers after Identifier Update ACK message is sent. During the listening status, the initiating UE maintains two unicast links with old and new identifiers. The listening status keeps until it received any message from peer UE using new identifiers.

The above mechanism assures no application layer messages are discarded caused by switching the message identifiers independently. Advantages of this solution include the unchanged mechanism on peer UE, and no need for additional signalling or application layer messages. The detailed solution is illustrated in Figure 6.15.2-1



Figure 6.15.2-1: Procedure for minimizing the impact of privacy protection mechanism in the application communication in unicast over PC5

0. Unicast communication has been established and is in progress.

1. The initiating UE (UE1) determines to update identifiers (L2 ID, Kd Session ID and its IP address in case of IP-based communication) with peer UE (UE2). This event is triggered in the UE by, e.g. request from the upper layer or timer expiration as specified in TS 23.287 [4]. Both UEs use old identifiers to send and receive application layer messages during the identifier update negotiation.

2. After emitting the acknowledgement message, the initiating UE (UE1) starts to receive and accept the message from the peer UE (UE2) using either the old or the new identifiers of the message. In case of final acknowledgement message of identifier update negotiation is sent by the peer UE (UE2) instead of the initiating UE (UE1), this step is executed by the peer UE (UE2).

The initiating UE (UE1) starts to use new identifiers to send unicast messages to peer UE (UE2).

3. The peer UE (UE2) receives the acknowledgement from the initiating UE and starts using the new identifiers.

4. The initiating UE (UE1) stops to receive and accept the old identifiers from peer UE (UE2) after receiving message from peer UE using new identifiers.

### 6.15.3 Solution Evaluation

NOTE: No evaluation is addressed in the present document.

## 6.16 Solution #16: Solution for the activation of user plane security in NR PC5 unicast

### 6.16.1 Introduction

This solution addresses part of key issue #2 on security for eV2X unicast messages over PC5. In particular, the solution covers the activation of user plane security and provisioning of associated security policy.

In clause 5.1.2.1 of TS 23.287 [4], there is a large list of parameters that need to be provisioned to the UE for PC5 communications. The solution proposes to add some additional parameters to cover the required security policy for V2X services that may use PC5 Unicast. The policy also applies to geographic areas to allow different regulatory policies to be supported. The security policy has the confidentiality and integrity requirements (on or off) for both control and user plane signalling.

### 6.16.2 Solution details

This solution covers the provisioning of PC5 security policy and the activation of user plane security for the V2X NR PC5 unicast.

As part of the provisioning process for PC5 Unicast (see clause 5.1.2.1 of TS 23.287 [4]), the UE is provisioned with the following:

- The list of V2X services, e.g. PSIDs or ITS-AIDs of the V2X applications, with Geographical Area(s) that require and their security policy which indicates whether confidentiality and/or integrity protection are required for signalling and/or user plane traffic.

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

The activation of user plane security follows the model for activation of user plane security when connected to a 5G core and is done based on the security policy provisioned in the UE, namely:

- ciphering is activated or deactivated for each user plane bearer individually when the bearer is established;

- integrity protection is activated or deactivated for each user plane bearer individually when the bearer is established; and

- the same ciphering and integrity algorithms selected for the signalling traffic are used for all user plane bearers (when activated).

### 6.16.3 Evaluation

The solution addresses the requirements of the key issue #2 by showing how the user plane security is activated over PC5 NR unicast.

The activation of the user plane security allows for ciphering and integrity to be activated on a per bearer basis which is the same as for UE connected to a 5G core. This allows the flexibility to apply the appropriate security to each bearer. The security policy to apply for each bearer is provisioned to the UE using the method proposed in TS 23.287 [4].

## 6.17 Solution #17: PC5 layer key derivation using the 5G network keys

### 6.17.1 Introduction

This solution addresses part of key issue #2 on security for eV2X unicast messages over PC5, and proposes a new solution for PC5 layer key derivation using the 5G network keys.

This solution is only applicable in the scenario that the initiating UE is registered into the network, the receiving UE is under the network coverage, and both initiating UE and receiving UE are in the same serving network.

### 6.17.2 Solution details

This solution assumes that the UE1 is already registered into the network, and UE2 is under the 3GPP network coverage, in order that both UEs could negotiate a secured key with the assistance of the core network.

The high level description would be that after receiving the request from the UE1, the UE2 could request the network to generate a shared key for the PC5 layer based on the AMF key, where the AMF key is the secure key established during the registration procedure of UE1.

The PC5 layer key derivation using the 5G network keys is described in Figure 6.17.2-1.



Figure 6.17.2-1: PC5 layer key derivation using the 5G network keys

In this procedure the communicated UEs via PC5 already stores the PC5 data protection status between them, which is negotiated during the PC5 connection establishment. The details solution is as follows.

0. UE1 and AMF1 store the 5G-GUTI1, ngKSI and KAMF, which are established during the UE registration to the network.

1. UE1 sends the NAS Container (5G-GUTI1, ngKSI,…, MAC) to the UE2 via direct communication request message. Other parameters used for direct communication establishment can be referred to TS 23.287[4].

2. UE2 determines whether UE1 and UE2 are in the same serving network based on the serving network ID1 included in the 5G-GUTI1 and serving network ID2, where the serving network ID2 indicates the network that UE2 can register with or currently connected to. If the serving network ID1 and serving network ID2 are the same, the UE2 continues. Otherwise the UE2 could select other ways to negotiate the PC5 layer key, e.g. based on the application layer keys.

3. UE2 forwards the indicator, NAS Container (5G-GUTI1, ngKSI,…, MAC) to the AMF2 via UL NAS message, where the indicator indicates this message is used for PC5 layer key derivation.

NOTE 1: UE1 and UE2 may be connected to the same AMF, i.e. AMF1.

4. AMF2 sends the indicator and NAS Container (5G-GUTI1, ngKSI,…, MAC) to the AMF1.

5. After receiving the indicator and NAS Container (5G-GUTI1, ngKSI,…, MAC), the AMF1 firstly verifies the MAC based on the NAS key shared with UE1. If the verification successes, the AMF1 generates the PC5 key based on the KAMF.

6-7. AMF1 sends the PC5 key to the UE2 via AMF2.

8. UE2 generates the session key KD based on the PC5 key.

9-11. UE2 initiates the Direct security mode command procedure with UE1. UE1 generates the PC5 key and KD with the same way as AMF1 and UE2.

NOTE 2: This solution focuses on how to establish the PC5 key. Direct security mode command procedure is out of scope of this solution.

12. UE2 sends the direct communication response to the UE1.

### 6.17.3 Evaluation

The solution meets the first potential requirement "The initiating UE shall establish a different security context for each peer UEs during the V2X unicast link establishment". Since the PC5 key is generated based on the AMF key shared between UE1 and AMF1, a different security context for each peer UEs during the V2X unicast link establishment will be established. Furthermore, man-in-the-middle attacks will not be initiated by the attacker without the AMF key. The second potential requirement "V2X unicast link security establishment between the initiating UE and each peer UE shall be protected from man-in-the-middle attacks" is also satisfied.

The operator network is involved in the PC5 key generation in this concrete scenario. 5G key hierarchy (i.e. KAMF) is reused here to assure the security of the newly generated PC5 key. All the security context of PC5 is within 3GPP scope in this case. The solution is only suitable to the applications where operators know the key.

The disadvantage of the solution is its limited applicable scenario, which is only applied when the initiating UE is registered into the network, the receiving UE is under the network coverage, and both initiating UE and receiving UE are registered.

5G-GUTI broadcasting may have privacy implications.

## 6.18 Solution #18: Solution for the UP security activation policy handling in NR PC5 unicast

### 6.18.1 Introduction

This solution addresses the requirement of key issue #2 regarding the confidentiality and integrity protection of the PC5 user plane. In particular, the solution covers the UP security activation policy handling in NR PC5 unicast.

### 6.18.2 Solution details

This solution proposes that the user plane security policy handling is based on the security policy of the eV2X service (e.g. PSID(s) or ITS-AID(s)), preconfigured in the UE.

Assume that the initiating UE is preconfigured with UP security policy 1 for service 1, the receiving UE is preconfigured with UP security policy 2 for the same service. During the PC5 unicast link establishment procedure, the receiving UE determines the final UP security activation policy after receiving the UP security policy 1 from the initiating UE. The UP security activation policy is defined as follow:

- Ciphering: "Required, Preferred, Not needed";

- Integrity protection: "Required, Preferred, Not needed".

The UP security activation handling is defined as follows:

- If any of the UP security policy1 and UP security policy2 is "Required", ciphering/ integrity protection is activated each user plane bearer individually for the service when the bearer is established.

- If both of the UP security policy1 and UP security policy2 is "Preferred", ciphering/ integrity protection is activated or deactivated each user plane bearer individually for the service when the bearer is established depending on the decision of the receiving UE.

- If both of the UP security policy1 and UP security policy2 is "not needed", ciphering/ integrity protection is deactivated each user plane bearer individually for the service when the bearer is established.

Detailed procedures are as follows: After receiving the UP security policy1 and eV2X service ID from the initiating UE, the receiving UE determines the final UP activation policy based on the UP security policy1 and UP security policy2 identified by eV2X service ID as described in the above. Then the receiving UE sends the protection indication to the receiving UE, where the protection indication is the same as the protection indication specified in TS 33.501 [8] clause 6.6.2 UP security activation.

### 6.18.3 Evaluation

This solution addresses the part of key issue #2 on security for eV2X unicast messages over PC5.

The solution meets the first requirement "*The initiating UE shall establish a different security context for each peer UEs during the V2X unicast link establishment*". The solution gives out the PC5 UP policy handling per eV2X service granularity based on the UP security policy1 of the initiating UE and UP security policy2 of the receiving UE. PC5 UP policy is the principle of the security context establishment.

The advantage of the solution is that on demand security protection for PC5 is supported per eV2X service granularity.

The disadvantage of the solution is only applicable when both UEs are preconfigured with the UP security policy of the eV2X service.

## 6.19 Solution #19: Protection of IEs in Direct Communication Request message

### 6.19.1 Introduction

This solution addresses part of key issue #2 on security for eV2X unicast messages over PC5. In particular, the solution covers the protection of the IEs in the Direct Communications request message that are not needed before security establishment.

### 6.19.2 Solution details

This solution assumes that the PC5 NR Unicast security context handling follows that in ProSe (see TS 33.303 [6]) where a complete security context is not kept when the connection drops. This means it is necessary to run Direct Security Mode procedure between the Direct Communication Request message and the Direct Communication Accept message. The solution is then as follows:

- Only IEs that are needed to establish the security are sent in the Direct Communication Request messages

- The other IEs that are needed before the Direct Communication Accept message are included in the Direct Security Mode Complete message

The exact IEs that will be sent in the Direct Communication Request message will be determined as part of the normative work.

NOTE: It will be left to the stage 3 specification to decide how there IEs are carried in the Direct Security Mode Complete message, e.g. as individual IEs or part of Direct Communication Accept message.

### 6.19.3 Evaluation

The solution provides security for the PC5 signalling by delaying the transmission of IEs from the Direct Communication Accept message until the PC5-S security has been established between the UEs, i.e. using the Direct Security Mode Complete message (or equivalent secured message that is sent once security has been established but before Direct Communication Accept message is sent).

The solution does not add any additional messages between the UE but merely moves the IEs from one message to another. The solution is simpler that the initial NAS security protection accepted for 5G security (see TS 33.501 [8]) as there is no partial ciphering required as the solution follows ProSe (see TS 33.303 [6]) with no protection for the Direct Communication Request message.

## 6.20 Solution #20: Solution on securely creating destination Layer-2 ID in groupcast communication

### 6.20.1 Introduction

This solution addresses the KI #4 "Security of identifier conversion in groupcast communication", and part of KI #3 "Privacy protection for groupcast messages over PC5" and KI #9 "Minimizing the impact of privacy protection mechanism in the application layer communication".

### 6.20.2 Solution details

The detailed solution is illustrated in Figure 6.20.2-1.

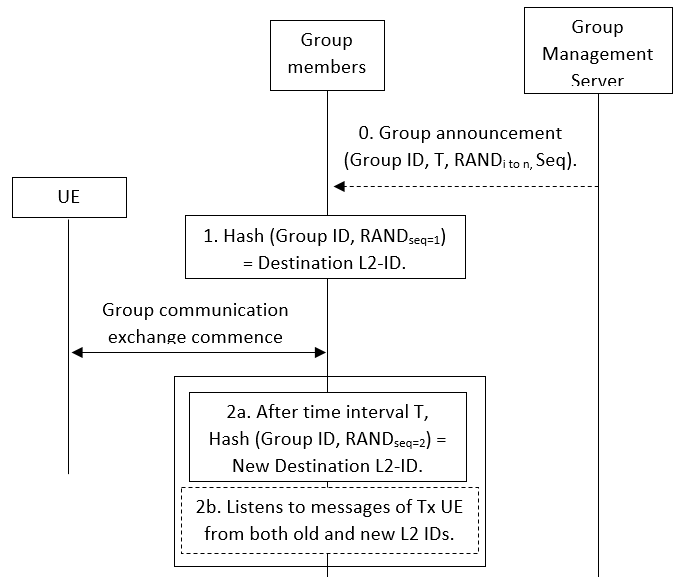


Figure 6.20.2-1: Procedure for secure conversion of application layer group ID to destination Layer-2 ID

0. Group Setup: Once the group is created, the group management server will send the group ID to the associated UEs and a timer T. It will also send a set of random numbers and a specific sequence in which these random number are to be used. It is assumed that the application layer signalling is protected.

1. ID Conversion: All the UEs use the group ID and the first random number according to the sequence as an input to a hash function to generate the destination Layer-2 ID.

2. ID Update: When the timer T expires, a new destination Layer-2 ID is calculated using the next random number according to the sequence. The UEs can listen to both old a new destination Layer-2 IDs, to avoid any time synchronization issues, for a certain period of time or until receives a message with the new ID.

The destination Layer-2 ID is updated until the application layer changes the group ID.

The group management server can also send the corresponding materials to generate random numbers rather than sending the random numbers itself.

### 6.20.3 Evaluation

NOTE: No evaluation is addressed in the present document.

# 7 Conclusions

## 7.1 Conclusion on KI #7

For Key Issue #7 "Cross-RAT PC5 control authorization indication", no normative work is required.

## 7.2 Conclusion on KI #5

For key issue #5 on security for setting up groupcast in Rel-16, it is concluded that there will be no normative work as there is no signalling to establish groupcast bearers and the management of groups is out of scope of 3GPP.

## 7.3 Conclusion on KI #11

For Key Issue #11 on security of PC5 NR broadcast in Rel-16, like LTE V2X broadcast (see [12]), it is concluded that there will be no normative work for security of broadcast bearers.

## 7.4 Conclusion on KI #3 and #8

For key issues #3 and #8 for the layer-2 source ID, solution #13 is chosen as the basis for normative work.

For key issue #8, for the privacy protection of destination Layer-2 ID, no normative work is required.

## 7.5 Conclusion on KI #6

For key issue #6 "Security of the UE service authorization and revocation", it is concluded that no normative work is required.

## 7.6 Conclusion on KI #1

For key issue #1 on privacy protection for unicast messages over PC5, the idea of changing the layer 2 identities and the shared identities (e.g. Key IDs) at the same time as proposed in solution #1 is chosen as the basis for normative work. It is proposed to capture these requirements in the V2X security specification with the actual procedure to perform layer 2 update satisfying these requirement specified in TS 23.287 [4].

## 7.7 Conclusion on KI #2

For Key Issue #2 on security for eV2X unicast messages over PC5, solution #3, solution #8, solution #18, solution #12 and solution#16 are chosen as the basis for normative work. Inconsistencies in the handling of the security policy between solutions #18 and solution #16 will be resolved during the normative phase.

NOTE: Some additional parts of a solution may be needed, e.g. protection of IEs in Direct Communication Request. These additional decisions can be part of the normative work.

## 7.8 Conclusion on KI #10

For Key Issue #10 on UP security policy handling for PC5 and Uu interface, it is concluded that there will be no normative work for UP security policy handling while switching between PC5 and Uu in this release.

## 7.9 Conclusion on KI#4

For Key Issue #4 on Security of identifier conversion in groupcast communication, it is concluded that no normative work is required in this release.

## 7.10 Conclusion on KI#9

For Key Issue #9 on Minimizing the impact of privacy protection mechanism in the application layer communication, it is concluded that no normative work is required in this release.

Annex A:  
Change History

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-03 | SA3#94 AH |  |  |  |  | TR skeleton and scope: S3-190769, S3-190918 | 0.0.0 |
| 2019-05 | SA3#95 |  |  |  |  | Clause 4: S3-191744, New key issues: S3-191746, S3-191747, S3-191670, S3-191740, S3-191748, S3-191749, S3-191341, References: S3-191117 | 0.1.0 |
| 2019-06 | SA3#95-Bis |  |  |  |  | Solution #1, #2, #3, #4, #5: S3-192415, S3-192417, S3-192418, S3-192419, S3-191958  Key issue update #2: S3-192420 | 0.2.0 |
| 2019-08 | SA3#96 |  |  |  |  | Key issues: S3-193162, S3-193164, S3-193166  Solutions: S3-193163, S3-192727, S3-193154, S3-193155, S3-193157, S3-193158, S3-193161, S3-193160, S3-193159, S3-193165  Editorial corrections: S3-192567, S3-193167 | 0.3.0 |
| 2019-10 | SA3#96 AH |  |  |  |  | Key Issues: S3-193429, S3-193430, S3-193806  Solutions: S3-193304, S3-193795, S3-193307, S3-193796, S3-193797, S3-193798, S3-193306, S3-193315, S3-193347, S3-193348, S3-193349, S3-193522, S3-193804, S3-193321, S3-193323, S3-193327, S3-193799, S3-193853, S3-193800, S3-193801, S3-193803  Editorial correction: S3-193326 | 0.4.0 |
| 2019-11 | SA3#97 |  |  |  |  | Solutions: S3-193961, S3-194095, S3-194148, S3-194303, S3-194305, S3-194306, S3-194619, S3-194620, S3-194616, S3-194623, S3-194646, S3-194647, S3-194648, S3-194649, S3-194651, S3-194653, S3-194654  Conclusions: S3-194039, S3-194044, S3-194618, S3-194650, S3-194657 | 0.5.0 |
| 2020-05 | SA3#99e | S3-201339 |  |  |  | Conclusions: S3-200953, S3-200954 | 0.6.0 |
| 2020-06 | SA#88-e | SP-200380 |  |  |  | EditHelp/MCC review  Presented for approval | 1.0.0 |
| 2020-07 | SA#88-e |  |  |  |  | Upgrade to change control version | 16.0.0 |
| 2020-09 | SA#89e | SP-200711 | 0001 | - | F | Clean up of TR 33.836 | 16.1.0 |