|  |  |
| --- | --- |
| 3GPP TR 33.893 V1.0.0 (2023-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of Ranging Based Services and Sidelink Positioning  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| 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.  © 2022, 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 7

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Symbols 10

3.3 Abbreviations 10

4 Architecture assumptions 10

4.1 Reference architecture 10

4.2 Reference points 11

5 Key issues 11

5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services 11

5.1.1 Key issue details 11

5.1.2 Security threats 12

5.1.3 Potential security requirements 12

5.2 Key Issue #2: Authorization for Ranging/Sidelink Positioning Service 12

5.2.1 Key issue details 12

5.2.2 Security threats 13

5.2.3 Potential security requirements 13

5.3 Key issue #3: Protection of discovery procedure 13

5.3.1 Key issue details 13

5.3.2 Security threats 13

5.3.3 Potential security requirements 14

5.4 Key issue #4: Protection of unicast direct communication 14

5.4.1 Key issue details 14

5.4.2 Security threats 14

5.4.3 Potential security requirements 14

5.5 Key issue #5: Protection of groupcast/broadcast 15

5.5.1 Key issue details 15

5.5.2 Security threats 15

5.5.3 Potential security requirements 15

6 Solutions 16

6.0 Mapping of solutions to key issues 16

6.1 Solution #1: Privacy protection for UEs in Ranging 17

6.1.1 Introduction 17

6.1.2 Solution details 17

6.1.3 Evaluation 18

6.2 Solution #2: Authorization of 5GC NF for Ranging/SL positioning service exposure 18

6.2.1 Introduction 18

6.2.2 Solution details 18

6.2.3 Evaluation 20

6.3 Solution #3: Authorization of Application Server for Ranging/SL positioning service exposure 20

6.3.1 Introduction 20

6.3.2 Solution details 21

6.3.3 Evaluation 22

6.4 Solution #4: Subscription-based authorization of the role of the UE during discovery 23

6.4.1 Introduction 23

6.4.2 Solution details 23

6.4.3 Evaluation 27

6.5 Solution #5: Use of authorization tokens at PC5 security establishment 28

6.5.1 Introduction 28

6.5.2 Solution details 28

6.5.2.1 Token based authorization for scenario of SL positioning services 28

6.5.2.1.1 Security for network assisted Sidelink Positioning with full network coverage 28

6.5.2.1.2 Security for network assisted Sidelink Positioning with partial network coverage 29

6.5.2.2 Token based authorization for scenario of Ranging services 30

6.5.2.2.1 Security for Ranging procedure between Reference UE and Target UE 30

6.5.2.2.2 Security for Ranging procedure between Reference UE/Target UE and Assistant UE 31

6.5.3 Evaluation 33

6.6 Solution #6: Protection of direct communication for Sidelink Positioning service 33

6.6.1 Introduction 33

6.6.2 Solution details 33

6.6.3 Evaluation 35

6.7 Solution #7: Security policy based protection for Ranging/SL positioning service operation 35

6.7.1 Introduction 35

6.7.2 Solution details 35

6.7.3 Evaluation 36

6.8 Solution #8: Security policy based protection for ranging result sent to SL Positioning Client UE 37

6.8.1 Introduction 37

6.8.2 Solution details 37

6.8.2.1 Security policy configuration for ranging result sent via PC5 37

6.8.2.2 Security policy configuration for ranging result sent via 5GC 38

6.8.3 Evaluation 38

6.9 Solution #9: Ranging/SL Positioning discovery and link establishment procedure for V2X capable UEs 39

6.9.1 Introduction 39

6.9.2 Solution details 40

6.9.2.1 Security for direct discovery and communication for V2X capable UEs 40

6.9.2.2 Security for Assistant UE discovery and communication for V2X capable UEs 42

6.9.3 Evaluation 44

6.10 Solution #10: Use of authorization tokens after PC5 security establishment 44

6.10.1 Introduction 44

6.10.2 Solution details 45

6.10.3 Evaluation 46

6.11 Solution #11: Client UE authorization for service exposure through sidelink 46

6.11.1 Introduction 46

6.11.2 Solution details 46

6.11.2.1 Authorization of SL Positioning Client UE during direct link establishment 46

6.11.2.2 Authorization of SL Positioning Client UE after direct link establishment 48

6.11.2.3 Authorization of SL Positioning Client UE during direct discovery 49

6.11.3 Evaluation 51

6.12 Solution #12: Ranging/SL Positioning discovery security for 5G ProSe capable UEs 52

6.12.1 Introduction 52

6.12.2 Solution details 52

6.12.3 Evaluation 52

6.13 Solution #13: Security of Ranging unicast communication 52

6.13.1 Introduction 52

6.13.2 Solution details 52

6.13.3 Evaluation 53

6.14 Solution #14: Direct communication security for Ranging-based services 53

6.14.1 Introduction 53

6.14.2 Solution details 53

6.14.3 Evaluation 53

6.15 Solution #15: Protection of information over group communication for Ranging/SL Positioning service 54

6.15.1 Introduction 54

6.15.2 Solution details 54

6.15.2.1 Security flows 54

6.15.2.2 Protection of messages between UEs 56

6.15.2.2.1 Message processing in the sending UE 56

6.15.2.2.2 Protected message processing in the receiving UE 57

6.15.3 Evaluation 57

6.16 Solution #16: Privacy protection of Located UE during its discovery and selection 57

6.16.1 Introduction 57

6.16.2 Solution details 57

6.16.3 Evaluation 60

6.17 Solution #17: Client UE authorization for service exposure through 5GC network 60

6.17.1 Introduction 60

6.17.2 Solution details 60

6.17.3 Evaluation 62

6.18 Solution #18: Client UE authorization by 5GC for service exposure through PC5 62

6.18.1 Introduction 62

6.18.2 Solution details 62

6.18.2.1 General 62

6.18.2.1 Authorization of SL Positioning Client UE during direct link establishment 63

6.18.2.2 Authorization of SL Positioning Client UE during Ranging/SL positioning procedure 64

6.18.3 Evaluation 65

6.19 Solution #19: Protecting Ranging/SL Positioning discovery out of network coverage 65

6.19.1 Introduction 65

6.19.2 Solution details 66

6.19.3 Evaluation 67

6.20 Solution #20: Secure groupcast/broadcast of SL positioning data 68

6.20.1 Introduction 68

6.20.2 Solution details 68

6.20.3 Evaluation 69

6.21 Solution #21: Security of ranging/SL positioning groupcast communication 69

6.21.1 Introduction 69

6.21.2 Solution details 69

6.21.3 Evaluation 70

6.22 Solution #22: Protection of broadcast Sidelink Positioning data in coverage scenario 70

6.22.1 Introduction 70

6.22.2 Solution details 70

6.22.3 Evaluation 72

6.23 Solution #23: Provisioning groupcast/broadcast protection key out of coverage 72

6.23.1 Introduction 72

6.23.2 Solution details 72

6.23.3 Evaluation 75

6.24 Solution #24: Protecting groupcast/broadcast messages 75

6.24.1 Introduction 75

6.24.2 Solution details 76

6.24.2.1 Protecting groupcast message 76

6.24.2.1.1 Groupcast security key hierarchy 76

6.24.2.1.2 Groupcast security 76

6.24.2.2 Protecting broadcast message 77

6.24.2.2.1 Broadcast security key hierarchy 77

6.24.2.2.2 Broadcast security 77

6.24.3 Evaluation 77

6.25 Solution #25: Protection for groupcast of SLPP signalling 78

6.25.1 Introduction 78

6.25.2 Solution details 78

6.25.2.1 General 78

6.25.2.2 Key provisioning for SLPP signalling groupcast 79

6.25.2.3 SLPP signaling protection and verification 80

6.25.3 Evaluation 81

6.26 Solution #26: Protection of SLPP broadcast based on central key management function 81

6.26.1 Introduction 81

6.26.2 Solution details 81

6.26.2.1 General 81

6.26.2.2 Key provisioning via the PCF 82

6.26.2.3 Key provisioning via the LMF 83

6.26.3 Evaluation 85

6.27 Solution #27: Protection of broadcast communication 85

6.27.1 Introduction 85

6.27.2 Solution details 86

6.27.3 Solution Evaluation 88

6.28 Solution #28: Protection of broadcast communication 88

6.28.1 Introduction 88

6.28.2 Solution details 88

6.28.3 Evaluation 90

6.29 Solution #29: Discovery security material and SL session root key provisioning for Ranging/SL positioning UE discovery 91

6.29.1 Introduction 91

6.29.2 Solution details 91

6.29.3 Evaluation 93

7 Conclusions 93

7.1 Conclusions on Key Issue #1 93

7.2 Conclusions on Key Issue #2 94

7.3 Conclusions on Key Issue #3 94

7.4 Conclusions on Key Issue #4 94

Annex X: Change history 96

# 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 present document investigates the security and privacy aspects of Ranging based services and sidelink positioning in 5G system. The study is based on the architectural and functional requirements on Ranging based services and sidelink positioning services, so as to ensure that the proposed solutions address the security and privacy implications on the architecture enhancements studied in TR 23.700-86 [2]. Specifically, it covers the following:

- The identified security and privacy issues, threats, and potential requirements for Ranging based services and sidelink positioning;

- The gap analysis in security and privacy issues between Ranging based services and ProSe/V2X applications;

- The potential solutions addressing the security and privacy issues specific to Ranging based services and sidelink positioning.

# 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 TR 23.700-86: "Study on Architecture Enhancement to support Ranging based services and sidelink positioning"

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

[4] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[5] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[6] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[7] 3GPP TS 22.261: "Service requirements for the 5G system".

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

[9] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[10] 3GPP TR 38.859: "Study on expanded and improved NR positioning".

[11] 3GPP TS 23.586: "Architectural Enhancements to support Ranging based services and Sidelink Positioning".

[12] 3GPP TS 38.305: "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[13] 3GPP TS 37.355: "LTE Positioning Protocol (LPP)".

[14] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[15] 3GPP TS 23.502: "Procedures for the 5G System".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

The following terms used in the present document are defined in TR 23.700-86 [2]:

**Ranging**

**SL Reference UE**

**Target UE**

**Assistant UE**

**Located UE**

**SL Positioning Server UE**

**SL Positioning Client UE**

**Sidelink Positioning**

**Positioning**

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

DoS Denial of Service

LMF Location Management Function

ProSe Proximity based Service

SL Sidelink

V2X Vehicle-to-Everything

# 4 Architecture assumptions

## 4.1 Reference architecture

As per TR 23.700-86 [2] clause 4.3, both Ranging-based services and Sidelink Positioning services are based on a common architecture. Such enhanced architecture is able to support Ranging and Sidelink Positioning in-coverage, partial coverage and out of network coverage scenarios.



Figure 4.1-1 Reference Architecture for Ranging/SL Positioning

With the assumption that all Ranging/SL positioning capable UEs are also ProSe or V2X capable as per TR 23.700-86 [2], for direct communication/discovery related aspects which are already defined for ProSe and V2X, architecture defined in TS 23.287 [3] and TS 23.304 [4] is used as the basis. Therefore, for discovery security and direct communication security, the solutions defined for V2X and ProSe in TS 33.536 [5] and TS 33.503 [6] will be reused as much as possible.

## 4.2 Reference points

The reference points over air interface in the architecture involve SR1, SR5, PC5, N1, N2, etc., among which SR1 is out of 3GPP scope. The functional description of these reference points can refer to TR 23.700-86 [2] clause 4.3.2.

The service-based interfaces in the architecture involve Nlmf, Nudm, Npcf, Nudr, Namf, etc. The functional description of these reference points can refer to TR 23.700-86 [2] clause 4.3.2.

# 5 Key issues

## 5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services

### 5.1.1 Key issue details

As the information of almost all Ranging/Sidelink Positioning services is related to location, all the UEs participating in Ranging/Sidelink Positioning, including the SL reference UE, target UE, assistant UE, etc., may need to disclose its location information to others. If such privacy sensitive information is not well protected, the UE’s privacy could be compromised. Among the requirements defined for Ranging services in clause 6.37.2 of TS 22.261 [7], there are following requirements concerning privacy protection for Ranging services:

*The 5G system shall be able to protect privacy of a UE and its user, ensuring that no identifiable information can be tracked by undesired entities during ranging.*

*The 5G system shall be able to ensure that user privacy is not violated during ranging, e.g., subject to regional or national regulatory requirements.*

Privacy protection is also raised in clause 4.1 of TR 23.700-86 [2] as one of the architecture assumptions for Ranging/SL Positioning services and is tasked for SA3 to study. In multiple solutions (e.g. solutions #6, #9, #13, #18, #21, #23, #24, #25) of TR 23.700-86 [2], privacy is considered as an issue to be addressed, either during discovery, or during Ranging/SL positioning procedure, or for service exposure.

### 5.1.2 Security threats

When UE’s identifiable information is disclosed to undesired/malicious UEs during discovery or during communication for Ranging/SL positioning, the UE’s behaviour will become trackable to others. Hence the UE’s privacy could be violated.

When the UE’s Ranging/SL positioning information (e.g. distance measurement, direction measurement, or both, or assistant data) and/or the associated UE’s identity are disclosed to undesired/malicious UEs or undesired network functions during communication for Ranging/SL positioning, the UE’s whereabouts and/or movements will become traceable to others. Hence the UE’s privacy could be violated.

### 5.1.3 Potential security requirements

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during discovery for Ranging/SL positioning.

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during communication for Ranging/SL positioning.

## 5.2 Key Issue #2: Authorization for Ranging/Sidelink Positioning Service

### 5.2.1 Key issue details

Ranging/Sidelink Positioning Service refers to the determination of the distance between two UEs and/or the direction of one UE, i.e. target UE, from the other one, i.e. SL reference UE, via direct device connection. Ranging based services can be used in a variety of verticals, such as consumer, smart home, smart city, smart transportation, smart retail, and industry 4.0. However, Ranging/Sidelink Positioning Service is exposed to various potential security threats such as unauthorized access.

To mitigate these security threats, authorization is indispensable. Without proper authorization, unauthorized entities will be able to participate in the position determination or obtain the positioning result, and arbitrarily consume the Ranging/Sidelink Positioning service. Furthermore, if one UE participating in the Ranging/Sidelink Positioning procedure is unauthorized, all the other UEs are subject to active or passive attacks, i.e. DoS attack, traffic analysis, or privacy leakage.

In addition, Solutions #17, #21, and #25 in the TR 23.700-86 [2] also describe the security issue on the support of service authorization, i.e.

*Editor's note: How AMF1 performs service authorization and privacy checking will be developed by SA3.*

*Editor's note: The security issue, e.g. whether the selected assistant UE is allowed to participate the Ranging/Sidelink positioning between UE1 and UE2 is FFS, which will be evaluated by SA3.*

*Editor's note: The security issue, e.g. whether the selected list of network assisted UE is allowed to have the Ranging/SL positioning information of the target UE, is FFS, which will be evaluated in SA WG3.*

From the security point of view, the system should be able to store the authorization information and determine whether an entity (a UE or network function or 3rd party server) is authorized to use Ranging/Sidelink Positioning service and obtain Ranging/Sidelink Positioning result of UEs. Privacy is UE specific, service authorization without identifying the UE is not able to meet the privacy requirement of the UE. Based on the authorization checking, the access to and exposure of Ranging/Sidelink positioning services can be controlled.

### 5.2.2 Security threats

An unauthorized UE can claim the role of the target UE, and arbitrarily consume the Ranging/SL positioning services, which may drain the energy of SL reference UE and invalidate the charging mechanism.

An unauthorized UE can claim the role of the SL reference UE/assistant UE, which may result in inaccurate position determination or privacy violation.

An unauthorized network function or third party server or a third party client UE can obtain the location information by triggering Ranging/SL positioning between the UEs, which may violate the privacy of the UEs involved in the Ranging/SL positioning.

### 5.2.3 Potential security requirements

The 5G Ranging/SL positioning system shall be able to support the authorization of the UE as a target UE/reference UE/assistant UE/Located UE/SL Positioning Server UE in the Ranging/Sidelink Positioning service.

The 5G Ranging/SL positioning system shall be able to support the authorization of a network function for triggering Ranging/Sidelink Positioning services and obtaining the location information of UEs.

The 5G Ranging/SL positioning system shall be able to support the authorization of a third party server for triggering Ranging/Sidelink Positioning services and obtaining the location information of UEs.

The 5G Ranging/SL positioning system shall be able to support the authorization of a SL Positioning Client UE for triggering Ranging/Sidelink Positioning services and obtaining the location information of UEs.

## 5.3 Key issue #3: Protection of discovery procedure

### 5.3.1 Key issue details

As per TR 23.700-86 [2], for discovery related aspects, the architecture and solutions defined for V2X and ProSe will be reused as much as possible. This provides the basis for reusing the direct discovery security defined for ProSe in TS 33.503 [6] to protect the direct discovery for Ranging/ SL Positioning services, which supports either Model A or Model B discovery.

For discovery of ProSe/V2X, the UEs can successfully discover each other if both UEs support the same ProSe/V2X service or the discovery filters provisioned to both UEs match and support the same ProSe/V2X service. Different from ProSe/V2X discovery, the discovery for Ranging/SL Positioning services needs to take the role of the UE (i.e. SL reference UE or target UE or assistant UE) into consideration. This means that when a UE discovers another UE for Ranging/SL Positioning service, both UE needs to know its own role and the role of the UE to be discovered.

In addition to the discovery initiated by the UE, in solutions #18 and #20 of TR 23.700-86 [2], the discovery for Ranging/SL positioning can also be triggered by the network (e.g. LMF) for discovering the Located UE.

Another difference between ProSe/V2X discovery and Ranging/SL Positioning discovery is that, for ProSe/V2X, the discovery message initiated by the announcing/discoverer UE only includes its own identity. While for Ranging/SL positioning, when a UE or the network starts to initiate a discovery procedure, it may already know which UE is to be discovered for Ranging and hence may include the identity of both UEs (the identity of the initiating UE and the identity of the UE to be discovered) in the discovery message.

### 5.3.2 Security threats

During discovery, if the authenticity of the discovery message cannot be verified, an attacker can impersonate the SL reference UE or target UE or assistant UE or Located UE, or even the network function triggering the discovery.

If the discovery messages are not integrity protected and anti-replay protected, the discovery parameters can be removed, intercepted, modified, or replayed by an attacker. Consequently, the UE may connect with a UE with an unexpected role (e.g. a SL reference UE connects with a SL reference UE) hence fails the Ranging/SL positioning service; or the UE may not connect with any UE, which is a form of DoS attack; or the UE may connect with a malicious UE which could launch more severe attacks.

If the discovery messages are not confidentiality protected, the privacy sensitive parameters (e.g. the identity of the initiating UE, the identity of the UE to be discovered) can be leaked to other irrelevant parties, hence the privacy of the UE(s) may be violated.

### 5.3.3 Potential security requirements

The 5G Ranging/SL Positioning system shall be able to support integrity protection and anti-replay protection of discovery messages.

The 5G Ranging/SL Positioning system shall be able to support confidentiality protection of discovery messages.

Editor's Note: whether verification of source authenticity is required for ranging/sidelink positioning is FFS.

## 5.4 Key issue #4: Protection of unicast direct communication

### 5.4.1 Key issue details

As per TR 23.700-86 [2], for direct communication between the UEs, the architecture and solutions defined for 5G V2X and 5G ProSe will be reused as much as possible. This provides the basis for reusing the direct communication security defined for 5G ProSe in TS 33.503 [6] or for 5G V2X in TS 33.536 [5] to protect the direct communication for Ranging/SL Positioning services.

Although the security mechanisms for direct communication of 5G ProSe or 5G V2X services can be reused for Ranging/SL Positioning services, there are still some scenarios in Ranging/SL Positioning services that are not discussed and studied for 5G ProSe or 5G V2X services. Considering the Ranging/SL Positioning services may have different processing procedures, it’s necessary to study the security of direct communication which is dedicated to the Ranging/SL Positioning services scenario.

In addition, for Ranging/Sidelink Positioning services, the information exchanged during SR5 direct communication between the UEs is location related, which is security/privacy sensitive. This is also an aspect different from 5G ProSe or 5G V2X services which do not always carry security/privacy sensitive information over PC5.

Moreover, as per TR 23.700-86 [2], SR5 is defined in the reference architecture to carry control signalling of Ranging/Sidelink Positioning service. Given that all Ranging/SL positioning capable UEs are also ProSe/V2X capable, the security protection of SR5 direct communication can rely on the existing security protection of PC5 direct communication as specified in TS 33.503 [6] and TS 33.536 [5]. There are options discussed in TR 23.700-86 [2] to use PC5-S or PC5-U to carry SR5 control messages. Then how to protect SR5 control messages also needs to be analysed.

### 5.4.2 Security threats

During direct communication establishment for one-to-one communication, if the UE cannot authenticate the peer UE to be the entity it intends to communicate with, it may lead to the impersonation of the peer UE by an attacker.

Failure to protect the integrity of Ranging/SL Positioning service information during direct communication will open vulnerability for attacks such as fabrication, modification, or removal of the signalling data such as positioning capability, positioning assistance data and location information.

Failure to protect the confidentiality of Ranging/SL Positioning service information during direct communication will open vulnerability for eavesdropping attacks resulting in privacy violations.

In case one UE is communicating with multiple peer UEs for Ranging/SL Positioning service, if there is no security isolation between the PC5 direct links with multiple peer UEs, one compromised peer UE or compromised PC5 link could lead to the compromise of all PC5 links with other peer UEs.

### 5.4.3 Potential security requirements

The 5G system shall support a means for the Ranging-capable UEs to mutually authenticate each other during SR5 one-to-one direct communication of Ranging/SL Positioning service.

The 5G system shall provide a means to support integrity and replay protection of the information transferred during SR5 direct communication for the Ranging/SL Positioning service.

The 5G system shall provide a means to support confidentiality protection of the information transferred during SR5 direct communication for the Ranging/SL Positioning service.

The 5G system shall support a means for the Ranging-capable UE to establish cryptographic separation for each PC5 interface and for each peer UE during the SR5 direct communication establishment of Ranging/SL Positioning service.

## 5.5 Key issue #5: Protection of groupcast/broadcast

### 5.5.1 Key issue details

Editor’s Note: This key issue details may need to be updated to align with the conclusion in RAN2.

In TR 38.859 [10], it is mentioned that using SLPP unicast messages between UEs is the baseline for SL positioning. In addition, sending part of SLPP positioning signalling among UEs via broadcast/groupcast is also possible:

“*Unicast/one-to-one operation is assumed as baseline for exchange of SLPP signaling between UEs. Unicast SLPP session-based operation is supported. At least “centralized” operation is supported, i.e., operation where one UE performs range and/or position calculations based on measurement/location information relating to itself and/or other UEs. It is feasible to send at least the following positioning signaling for groupcast/broadcast (in addition to unicast) from RAN2’s perspective:*

* *SL positioning capability*
* *SL positioning assistance data*

*Location information is not excluded and can be further considered in normative work.*”

Furthermore, in TR 38.859 [10], it is also mentioned that security issues should be considered on how to protect the SL groupcast/broadcast messages:

“*RAN2 will further discuss in normative work:*

*- The security issues (e.g., requirements for ciphering and/or integrity) on specific information of SL positioning capability and assistance data in groupcast/broadcast.*

*- The use cases for applying groupcast/broadcast.*”

### 5.5.2 Security threats

Failures to protect SL groupcast/broadcast communications will lead to the following threats:

- Passive attackers can eavesdrop on privacy sensitive data exchanged between UEs.

- Active attackers can intercept, modify or replay data packets exchanged between UEs.

- The broadcasting/groupcasting UE may be impersonated by an attacker.

### 5.5.3 Potential security requirements

The 5G System shall support a means to provide confidentiality, integrity and replay protection of SL positioning signalling in groupcast.

The 5G System shall support a means to provide confidentiality, integrity and replay protection of SL positioning signalling in broadcast.

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 | KI#4 | KI#5 |
| Solution #1: Privacy protection for UEs in Ranging | X |  |  |  |  |
| Solution #2: Authorization of 5GC NF for Ranging/SL positioning service exposure |  | X |  |  |  |
| Solution #3: Authorization of Application Server for Ranging/SL positioning service exposure |  | X |  |  |  |
| Solution #4: Subscription-based authorization of the role of the UE during discovery |  | X |  |  |  |
| Solution #5: Use of authorization tokens at PC5 security establishment |  | X |  |  |  |
| Solution #6: Protection of direct communication for Sidelink Positioning service |  |  |  | X |  |
| Solution #7: Security policy based protection for Ranging/SL positioning service operation | X |  |  | X |  |
| Solution #8: Security policy based protection for ranging result sent to SL Positioning Client UE | X |  |  |  |  |
| Solution #9: Ranging/SL Positioning discovery and link establishment procedure for V2X capable UEs |  |  | X | X |  |
| Solution #10: Use of authorization tokens after PC5 security establishment |  | X |  |  |  |
| Solution #11: Client UE authorization by Application Server for service exposure through sidelink |  | X |  |  |  |
| Solution #12: Ranging/SL Positioning discovery security for 5G ProSe capable UEs | X |  | X |  |  |
| Solution #13: Security of Ranging unicast communication |  |  |  | X |  |
| Solution #14: Direct communication security for Ranging-based services | X |  |  | X |  |
| Solution #15: Protection of information over group communication for Ranging/SL Positioning service | X |  |  |  | X |
| Solution #16: Privacy protection of Located UE during its discovery and selection | X |  |  |  |  |
| Solution #17: Client UE authorization for service exposure through 5GC network | X | X |  |  |  |
| Solution #18: Client UE authorization by 5GC for service exposure through PC5 | X | X |  |  |  |
| Solution #19: Protecting Ranging/SL Positioning discovery out of network coverage |  |  | X |  |  |
| Solution #20: Secure groupcast/broadcast of SL positioning data |  |  |  |  | X |
| Solution #21: Security of ranging/SL positioning groupcast communication |  |  |  |  | X |
| Solution #22: Protection of broadcast Sidelink Positioning data in coverage scenario |  |  |  |  | X |
| Solution #23: Provisioning groupcast/broadcast protection key out of coverage |  |  |  |  | X |
| Solution #24: Protecting groupcast/broadcast messages |  |  |  |  | X |
| Solution #25: Protection for groupcast of SLPP signalling | X |  |  |  | X |
| Solution #26: Protection of SLPP broadcast based on central key management function | X |  |  |  | X |
| Solution #27: Protection of broadcast communication |  |  |  |  | X |
| Solution #28: Protection of broadcast communication |  |  |  |  | X |
| Solution #29: Discovery security material and SL session root key provisioning for Ranging/SL positioning UE discovery |  |  | X |  |  |

## 6.1 Solution #1: Privacy protection for UEs in Ranging

### 6.1.1 Introduction

This solution resolves Key Issue #1 for privacy protection for Ranging/SL Positioning services. In particular, this solution tries to acquire the UE’s authorization. In addition, configuration information is exchanged between the UEs to decide the entity for result calculation.

### 6.1.2 Solution details

The high-level procedure as shown in Figure 6.1.2-1 is based on the procedure descripted in solution 3 of TR 23.700-86 [2].

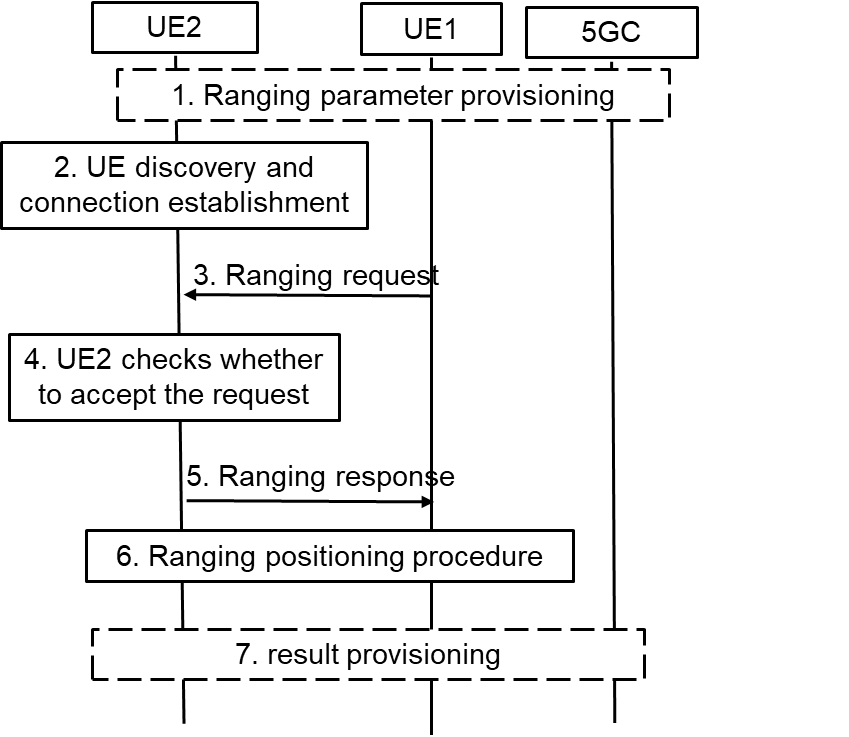


Figure 6.1.2-1: High-level Procedure for Ranging Operation Control

1. UE1 and UE2 may get the ranging parameters from 5GC during registration. UE1 gets the ranging request from the application layer, UE3 or 5GC NF. The ranging request includes the consumer info and/or the purpose of ranging positioning. For example, if the AF wants to acquire the distance between UE1 and UE2 for V2X service. The AF ID and purpose for V2X are included.

2. Discovery and the connection establishment procedure are performed between UE1 and UE2 based on the concluded procedure of TR 23.700-86 [2].

3. UE1 sends the ranging request in the Ranging/SL Positioning layer to the UE2 and negotiate the ranging parameters. The ranging request includes the ranging parameters, e.g. consumer info, purpose, result calculation entity. For example, UE1 decides to calculate the result and not share with UE2, then the result calculation entity means that “UE1 will calculate the ranging result”.

4. UE2 checks whether to accept the ranging request in step #3 in the Ranging/SL Positioning layer based on configuration. For example, UE2 checks whether to allow the ranging result to be provided to the consumer for the claimed purpose based on local policy. Based on received result calculation entity info, UE2 confirms whether the result can be acquired by UE1 or not.

NOTE 2: The configuration for privacy protection in the Ranging/SL Positioning layer is provided from application layer or other means. It is left to implementation.

5. UE2 sends the ranging response to the UE1. For example, if UE2 does not authorize the ranging positioning for the purpose or the consumer, the reject message with cause will be responded. If UE2 wants to change result calculation entity, for example due to its privacy consideration, result calculation entity is included.

NOTE 3: The solution assumes that UE1 and UE2 can trust each other on the authorization operations during the ranging parameter negotiation.

6. Ranging positioning procedure is performed. The ranging result is calculated based on the negotiation result in step #5.

7. The ranging results may not be shared between the UEs according to the negotiation result. The result calculation entity will provide the result to the application layer, UE3 or 5GC NF.

### 6.1.3 Evaluation

The solution fulfilled the requirement in Key Issue #1 for privacy protection for Ranging/SL Positioning services. Result calculation entity and ranging result sharing will be negotiated to limit the entity who can acquire the ranging result. Hence, the ranging result will not be disclosed to undesired UEs. UE will check whether to accept the Ranging request on consumer info, purpose or result calculation entity based on configuration, which may be provided from application layer. The negotiation is perfomed in the Ranging/SL Positioning layer. The UE determines whether to continue the ranging process according to the authorization and negotiation result.

Coordination with RAN2 is required for accommodating the signalling elements required for privacy negotiation in the Ranging/SL Positioning layer.

## 6.2 Solution #2: Authorization of 5GC NF for Ranging/SL positioning service exposure

### 6.2.1 Introduction

This solution addresses Key Issue #2 on Authorization for Ranging/SL Positioning service. Specifically, it addresses the second requirement in KI#2: “*The 5G Ranging/SL positioning system shall be able to support the authorization of a network function for triggering Ranging/Sidelink Positioning services and obtaining the location information*”.

According to TR 23.700-86 [2], 5GC NF is enabled to initiate SL positioning service to obtain the accurate location of a UE or obtain the distance between two UEs, for which the 5GC NF needs to be authorized at two levels:

* The first level of authorization is for service access, i.e. the 5GC NF should be authorized to request the SL positioning service. This level of authorization could be achieved by existing OAuth token-based authorization defined in TS 33.501 [8].
* The second level of authorization is for preserving UE privacy. This is because, even if the 5GC NF is authorized to request the SL positioning service, it does not mean that the requested service can always be exposed to the 5GC NF. For example, it is possible that the 5GC NF is allowed to request SL positioning info between UE1 and UE2, but may not be allowed to request SL positioning info between UE3 and UE4. Without further check on the authorization info of the involved UEs, there is still the risk that SL positioning information could be exposed to unauthorized 5GC NF. Therefore, the 5GC NF needs to be further authorized on whether it is allowed to acquire position information of the involved specific UEs.

This solution introduces a method for authorizing the 5GC NF which initiates SL positioning service targeting at specific UEs.

### 6.2.2 Solution details

The solution proposes that, when the 5GC NF initiates Ranging/SL Positioning service request, it initially interacts with the GMLC to check with the UDM about authorization information of the UEs for acquiring SL positioning information of the UEs, based on e.g. the privacy related parameters in UE’s subscription data stored in the UDM/UDR.

UE1 and UE2 refer to SL Reference UE and Target UE respectively for SL Positioning service.

0. Service authorization and policy/parameters provisioning procedure is performed between UE1/UE2 and the network respectively.

1. The 5GC NF sends the SL positioning service request to the GMLC.

2. The GMLC check with the UDM about the authorization info of UE1/UE2 via Nudm\_SDM\_Get service operation.

NOTE 1: regardless of whether UE1/UE2 are managed by different UDMs, separate Nudm\_SDM\_Get message needs to be sent as the API applies only for one target UE and for checking that UE’s subscription.

3. The UDM checks the authorization info of UE1 and UE2 against their subscription data respectively based on the UE1 ID and UE2 ID.

4. The UDM returns the authorization results of the UEs to the GMLC.

5. The GMLC checks the authorization results of both UEs. Since SL Positioning service concerns location of the UE, it could be possible that the authorization info of the UE is location specific (e.g. the UE allows its location to be exposed in area A but does not allow its location to be exposed in area B).

If none of the UE grants or one of the UEs does not grant authorization for Ranging/SL positioning, the GMLC responds with authorization failure to the 5GC NF to abort the Ranging/SL positioning service.

If both UEs grant authorization without location restriction, the GMLC proceeds to step #9.

Conditionally, if both UEs grant authorization which is restricted in a certain area, the GMLC proceeds to step #6.



Figure 6.2.2-1: Authorization of the 5GC NF for Service Exposure

6. [Conditional] The GMLC sends the Namf\_Location\_ProvideLocationInfo Request to the AMF.

NOTE 2: regardless of whether UE1/UE2 are managed by different or same AMF(s), separate Namf\_Location\_ProvideLocationInfo Request messages needs to be sent to the AMF as the API applies only for one UE.

7. [Conditional] The AMF of UE1/UE2 responds with the Namf\_Location\_ProvideLocationInfo Response to the GMLC which contains the coarse location of UE1/UE2 (e.g. TAI or Cell-ID of UE1/UE2).

8. [Conditional] Based on the coarse location of UE1/UE2, the GMLC checks whether the UE1/UE2 is within the area for requesting SL Positioning service.

9. If both UEs grant authorization in their current locations, the GMLC sends the SL Positioning service request from the 5GC NF to the AMF of one of the UEs (e.g. UE1) based on clause5.6.4 of TS 23.586 [xy].

10~13. The AMF selects a SL Positioning capable LMF (not shown in Figure 6.2.2-1) to perform the SL Positioning procedure between the network and the UE.

NOTE 3: The area granularity could be detailed in the UE privacy profile for SL positioning in UE subscription.

### 6.2.3 Evaluation

This solution addresses the second requirement “*The 5G Ranging/SL positioning system shall be able to support the authorization of a network function for triggering Ranging/Sidelink Positioning services and obtaining the location information”* in KI#2.

On top of the existing authorization of the 5GC NF on service level, the authorization in this solution is further performed on specific UE level, which ensures the privacy preservation of all involved UEs in a service, as Ranging/SL Positioning services request UE location information which is privacy sensitive.

This solution relies on the GMLC to check with the UDM for the authorization information of the involved UEs before forwarding the request from the 5GC NF to the AMF. Therefore, it is aligned with SA2 specification in TS 23.586 [11] which reuses the GMLC in LCS architecture specified in TS 23.273 [9] for Ranging/SL Positioning service exposure to 5GC NF.

NOTE: Whether the authorization is based on existing UE LCS privacy profile in UDM or whether its new data or profile is to be decided in normative work, and needs to be coordinated with SA2.

## 6.3 Solution #3: Authorization of Application Server for Ranging/SL positioning service exposure

### 6.3.1 Introduction

The solution addresses Key Issue #2: Authorization for Ranging/SL Positioning Services. It aims to meet one of the potential requirements in Key issue #2 on authorization of a third party server for triggering Ranging/Sidelink Positioning services.

As per TR 23.700-86 [2] solution #13, a Ranging/SL Positioning service request may be initiated by an application server. In the AF-initiated Ranging/SL Positioning procedure, the authorization on service permission is indispensable for protecting the UE’s privacy, for which the application server needs to be authorized at two levels:

* The first level of authorization is for service access. That means, when the NEF/GMLC receives the Ranging service request initiated by the Ranging application server (e.g. hosted in an AF), the NEF/GMLC can determine whether the application server/AF is authorized to request the Ranging service from the 5GC, according to clause 12.4 in TS 33.501 [8].
* The second level of authorization is for preserving UE privacy. This is because, even if the application server/AF is authorized to send requests to the 5GC for Ranging service, it does not mean that the service can always be exposed to the application server/AF. For example, it is possible that the application server/AF is allowed to request Ranging info between UE1 and UE2, but may not be allowed to request Ranging info between UE3 and UE4. Without further check on the authorization info of the involved UEs, there is still the risk that unauthorized Ranging/SL positioning information could be exposed to the application server/AF. Therefore, the application server/AF needs to be further authorized on whether it is allowed to acquire Ranging info of the involved specific UEs.

This solution proposes a method to meet the security requirement in AF-initiated procedure by using the existing network function GMLC/NEF. The GMLC/NEF interacts with the UDM to obtain the UE’s subscription data and interacts with the AMF to get the network provided location of the UE. Based on the above information, the GMLC/NEF is able to check the authorization of Ranging/SL positioning services and protect the ranging UE’s privacy.

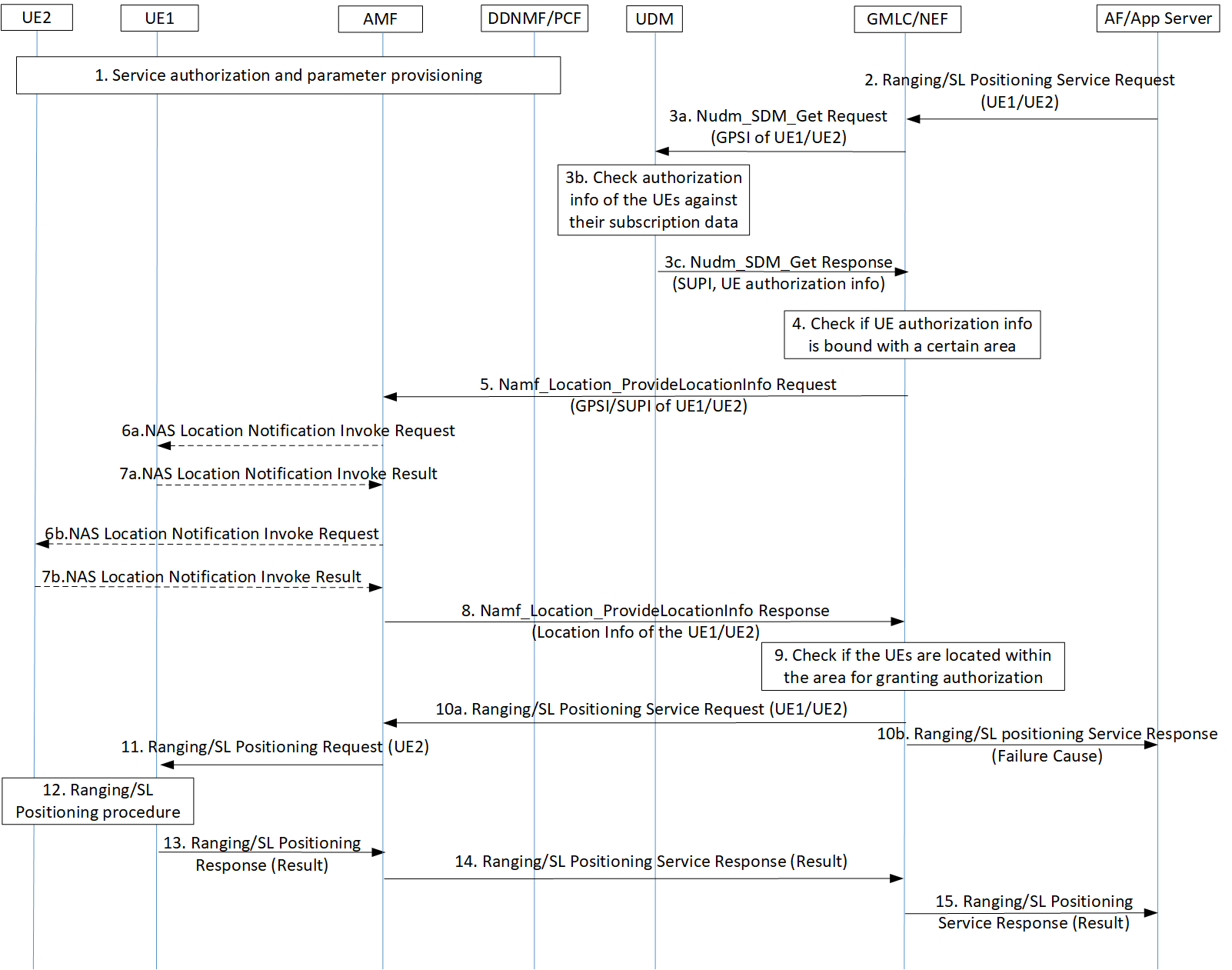
### 6.3.2 Solution details

The solution proposes that, when the GMLC/NEF checks with the UDM to discover the serving AMF(s) of the UEs, it also needs to check with the UDM to authorize the application server for acquiring Ranging information of the UEs, based on e.g. the privacy related parameters in UE’s subscription data stored in the UDM/UDR.

1. Service authorization policy/parameters are provisioned to UE1 and UE2.

2. The AF sends Ranging/SL positioning Service Request to the GMLC/NEF. If the Ranging/SL positioning Service Request is transmitted by the NEF/GMLC, the NEF/GMLC first determines whether the AF is authorized to request Ranging/SL Positioning service as defined in TS 33.501 [8], clause 12.4.

NOTE 1: UE1 can be either the target UE or the reference UE, which can be requested by the AF or can be decided during step #12.

Figure 6.3.2-1: Authorization of Application Server for Ranging/SL Positioning Service Exposure

3. The GMLC/NEF invokes a Nudm\_SDM\_Get service operation towards the UDM of the UE1/UE2 to get the authorization information of the UEs against e.g. their privacy profiles.

NOTE 2: For step 3a, regardless of whether UE1/UE2 are managed by different UDMs, separate Nudm\_SDM\_Get message needs to be sent as the API applies only for one target UE and for checking that UE’s subscription.

4. The GMLC/NEF checks the authorization results of both UEs. Since Ranging service concerns location of the UE, it could be possible that the authorization info of the UE is location specific (e.g. the UE allows its location to be exposed in area A but does not allow its location to be exposed in area B).

If none of the UE grants or one of the UEs does not grant permission for the requested Ranging/SL positioning service, the GMLC/NEF proceeds to step #10b.

If both UEs grant authorization without location restriction, the GMLC/NEF proceeds to step #10a.

Conditionally, if both UEs grant authorization which is restricted in a certain area, the GMLC/NEF proceeds to step #5. In addition, the GMLC/NEF invokes a Nudm\_UECM\_Get service operation towards the UDM of UE1/UE2. The UDM returns the network addresses of the current serving AMF of UE1/UE2.

NOTE 3: The area granularity could be detailed in the UE privacy profile for Ranging in UE subscription.

5. [Conditional] If both UEs grant permission which is however restricted in a certain area, the GMLC/NEF invokes the Namf\_Location\_ProvideLocationInfo service operation towards the AMF to request the Network provided location of the UE. This location request may also carry the result of the privacy check in step #3 which may include the Ranging/SL positioning service code or the identity of Ranging/SL positioning client provided by the AF and an indication of a privacy check related action (i.e. no action, notification, notification and verification, etc.)

NOTE 4: If UE1 and UE2 are managed by different AMFs, the GMLC/NEF shall send messages to the corresponding AMFs respectively.

6. [Conditional] If the indicator of privacy check related action indicates that the UE must either be notified or notified with privacy verification and if the UE supports Ranging notification (according to the UE capability information), a notification invoke message is sent by the AMF to the UE1/UE2, indicating the Ranging/SL positioning service code or the identity of Ranging/SL positioning client and whether privacy verification is required. If signalling connection establishment between UE2 and AMF fails, step 6 and step 7 are skipped, and the AMF answers to the GMLC with the last known location of the UE2 (i.e. Cell ID) together with the age of this location.

7. [Conditional] The UE1/UE2 returns a notification result to the AMF indicating, if privacy verification was requested, whether permission is granted or denied for the current Ranging request.

8. [Conditional] The AMF returns the Namf\_Location\_ProvideLocationInfo Response towards the GMLC/NEF to return the network provided location of the UE.

9. [Conditional] Based on the Network provided location of UE1/UE2, the GMLC/NEF checks whether the UE1/UE2 is within the area for granting service authorization to the application server/AF.

10a. If the privacy requirements are met, the GMLC/NEF forwards the Ranging/SL Positioning service request to the serving AMF.

10b. If none of the UEs grants or one of the UEs does not grant authorization in its current location, the GMLC/NEF responds to the application server/AF with a failure cause.

11~15. The rest of the Ranging service procedure is performed between the UE, the network and the application server/AF. If notification or notification with privacy verification fails in step 6, UE2 will be notified or notified with privacy verification via ranging layer before ranging measurement.

Alternatively, after the GMLC/NEF checks the authorization info of both UEs in step #4, if both UEs grant authorization which is however restricted in a certain area, the GMLC/NEF sends the Nudm\_ParameterProvision\_Get Request to the UDM and the UDM sends the Namf\_Location\_ProvideLocationInfo Request to the AMF. Then the AMF responds the Namf\_Location\_ProvideLocationInfo Response to the UDM and the UDM responds the Nudm\_ParameterProvision\_Get Response to the GMLC/NEF.

### 6.3.3 Evaluation

This consolidated solution addresses the third requirement on the authorization of a third party server for triggering Ranging services.

On top of the existing authorization of a third party server on service level, the authorization in this solution is further perform on specific UE level, which ensures the privacy of all involved UEs in a service, as Ranging/SL Positioning services per se request UE location information which is privacy sensitive.

This solution requires the GMLC/NEF to interact with the UDM to check the UE’s subscription data and interact with the AMF directly or indirectly to get the network provided location of the UE.

This solution assumes that the GMLC is involved in Ranging/Sidelink Positioning services if location-based service procedure defined in TS 23.273 [9] is reused.

The alternative solution is not aligned with SA2 conclusions for KI#5 in TR 23.700-86 [2]. The alternative to use the Nudm\_ParameterProvision\_Get Request to the UDM and the UDM sends the Namf\_Location\_ProvideLocationInfo Request to the AMF is not defined in SA2 LCS architecture. All the steps of the alternative solution for authorization in steps 3-5 would be new, with impact on UDM and GMLC/NEF.

The main solution is aligned with SA2 conclusions. The steps 4-5 would be new, with impact on GMLC/NEF.

NOTE: Whether the authorization is based on existing UE LCS privacy profile in UDM or whether its new data or profile is to be decided in normative work, and needs to be coordinated with SA2.

## 6.4 Solution #4: Subscription-based authorization of the role of the UE during discovery

### 6.4.1 Introduction

This solution addresses Key Issue #2 on Authorization for Ranging/SL Positioning service. Specifically, it addresses the first requirement in KI#2: “*The 5G Ranging/SL positioning system shall be able to support the authorization of the UE as a target UE/reference UE/assistant UE/Located UE in the Ranging/Sidelink Positioning service*”.

According to the definitions of various types of UE and their functionalities in Ranging/SL positioning services described in TR 23.700-86 [2], each of the UEs involved in a Ranging/SL positioning service plays a different role (e.g. SL Reference UE, Target UE, Assistant UE, Located UE, SL Positioning Server UE, SL Positioning Client UE). If the role of the UE is not claimed during discovery, the UEs may discover each other but may not be able to perform the requested service (e.g. a SL Reference UE having discovered another SL Reference UE). If the claimed role of the UE is not properly authorized during discovery, a UE can cheat its peer UEs in a service, resulting in service violation, privacy violation or charging invalidation.

This solution introduces a method for the network to authorize the role of the UE in a Ranging/SL positioning service during discovery. The authorization is performed in the security procedure for discovery, assuming Ranging/SL Positioning services reuse the discovery security procedure performed by ProSe capable UEs for ProSe services. Only after the role of the UE is successfully authorized, the network will then generate and provision discovery security materials to the UE.

### 6.4.2 Solution details

The solution assumes that the role that the UE is allowed to play in a Ranging/SL positioning service could be registered in the UE subscription (for SL positioning service) or in the specific service agreement (for Ranging service). That means, both the UDM and the Ranging Application Server could be the candidate function for authorizing the role of the UE for the requested Ranging/SL positioning service.

A UE may have the capabilities supporting multiple roles for Ranging/SL positioning services (e.g. SL Reference UE capable of handle position signal and Server SL Positioning UE capable of location calculation). But the role the UE is allowed to play is bound with a specific Ranging/SL positioning service (e.g. the UE is allowed to act as a SL Reference UE in service 1, while the same UE is only allowed to act as a SL Positioning Server UE in service 2).

The solution requires that the UE sends its own role in Ranging/SL positioning service to the network during discovery procedure. Then the Ranging Server or the UDM could authorize the UE by checking whether the UE is allowed to act in a specific Ranging/SL positioning service, against the service agreement or the UE subscription. The UE can obtain the discovery security material only after its role is authorized by the Ranging Server or the UDM. In this way, a misbehaving UE announcing an unauthorized role is not able to protect its announcement/solicitation messages, hence not able to cheat the peer UEs, which need to verify the received announcement/solicitation messages and ignore the unprotected messages.

**Authorization of the Role of the UE during Discovery – Model A**

Steps #1~#5 refer to an Announcing UE (A-UE):

1. A-UE sends a Discovery Request message including its assigned role for the requested service.

NOTE: Whether or not the Ranging capabilities can be used as the Ranging role is to be determined during normative phase.

2. The 5G DDNMF/PKMF of A-UE sends an Authorization Request to the Ranging Server or the UDM of A-UE for announcing authorization, which contains the UE’s role received from A-UE.

3. The Ranging Server checks against the service agreement or the UDM of A-UE checks against A-UE’s subscription, to determine whether A-UE is allowed to play the role(s) (e.g. whether A-UE is allowed to act as a Target/Server UE).

4. If there is a match between the received role and the allowed role(s) (e.g. A-UE is allowed to act as a Target UE or A-UE is allowed to act as both Target UE and Server UE), the Ranging Server or the UDM returns to the 5G DDNMF/PKMF an Authorization Response which contains the matched role(s) of A-UE. If there is no match between the received role and the allowed role(s) (e.g. A-UE is neither allowed to act as a Target UE nor allowed to act as a Server UE), the Ranging Server or the UDM returns an Authorization Response which contains the failure cause.

5. If the authorization with the Ranging Server or the UDM of A-UE is successful, the 5G DDNMF/PKMF of A-UE generates Discovery Security Material. The 5G DDNMF/PKMF of A-UE includes the Role(s) of A-UE authorized by the Ranging Server or the UDM and the Discovery Security Material in the Discovery Response. If the authorization with the Ranging Server or the UDM fails, the 5G DDNMF/PKMF of the A-UE does not generate Discovery Security Material and rejects the Discovery Request from the A-UE.

Steps #6~#15 refer to a Monitoring UE (M-UE):

6. M-UE sends a Discovery Request message including its assigned role for the requested service.

7. The 5G DDNMF/PKMF of M-UE sends an Authorization Request to the Ranging Server or the UDM of M-UE for monitoring authorization, which contains the UE’s role received from M-UE.



Figure 6.4.2-1: Authorization of the Role of the UE during Discovery – Model A

8. The Ranging Server checks against the service agreement or the UDM of M-UE checks against M-UE’s subscription, to determine whether M-UE is allowed to play the role(s) (e.g. whether M-UE is allowed to act as a SL Reference/Located UE).

9. If there is a match between the received role and the allowed role(s) (e.g. M-UE is allowed to act as a SL Reference UE or M-UE is allowed to act as both Reference UE and Located UE), the Ranging Server or the UDM returns to the 5G DDNMF/PKMF an Authorization Response which contains the matched role(s) of M-UE. If there is no match between the received role and the allowed role(s) (e.g. M-UE is neither allowed to act as a SL Reference UE nor allowed to act as a Located UE), the Ranging Server or the UDM returns an Authorization Response which contains the failure cause.

10. If the authorization with the Ranging Server or the UDM of M-UE is successful, the 5G DDNMF/PKMF of M-UE contacts the 5G DDNMF/PKMF of A-UE by sending a Monitor Request message.

11. The 5G DDNMF/PKMF of A-UE sends an Authorization Request to the Ranging Server or the UDM, which contains the authorized roles of both M-UE and A-UE.

12. The Ranging Server or the UDM checks whether the authorized roles of M-UE and A-UE match in the requested service (e.g. whether the roles are Target UE and SL Reference UE for a Ranging service, or whether the roles are Located UE and Target UE for a SL positioning service).

13. The Ranging Server or the UDM returns an Authorization Response indicating whether the authorization is successful.

14. If the authorization with the Ranging Server or the UDM is successful, the 5G DDNMF/PKMF of A-UE responds to the 5G DDNMF/PKMF of M-UE with a Monitor Response message including the Discovery Security Material. If the authorization with the Ranging Server or the UDM fails, the 5G DDNMF/PKMF of A-UE rejects the Monitor Request from the 5G DDNMF/PKMF of M-UE and the following steps are not performed.

15. The 5G DDNMF/PKMF of M-UE returns the Discovery Security Material, along with the Role(s) of M-UE authorized by the Ranging Server or the UDM of M-UE in the Discovery Response.

Steps #16~#18 occur over PC5:

16. A-UE starts announcing. A-UE forms the announcement message containing the authorized role of A-UE and protects it with the discovery security material.

17. M-UE listens for an announcement message and verifies the message with the discovery security material.

18. M-UE determines whether the claimed role of A-UE in the announcement message is the role it monitors for (e.g. if the Role of A-UE is Target UE, then M-UE acting as a Reference UE can determine that it found a match).

**Authorization of the Role of the UE during Ranging Discovery – Model B**

Steps #1~#15 are the same as the corresponding steps in the procedure for Model A.

Steps #16~#18 occur over PC5:

16. The discoverer (R-UE) forms the discovery solicitation message containing the authorized role of the discoverer and protects it with the discovery security material.

17. The discoveree (E-UE) listens for a discovery solicitation message and verifies the message with the discovery security material, after which the discoveree determines whether the claimed role of the discoverer in the solicitation message is the role it monitors for (e.g. if the Role of the discoverer is Target UE, then the discoveree acting as a Located UE can determine that it found a match).

18. The discoveree returns a discovery response message to the discoverer, which contains its own authorized role matching the role of the discoverer.



Figure 6.4.2-2: Authorization of the Role of the UE during Discovery – Model B

NOTE: The messages for authorization during discovery request procedure could be security specific messages.

### 6.4.3 Evaluation

This solution addresses the key issue #2 requirement on authorization of the UE as a target UE/SL reference UE/assistant UE/ Located UE during discovery procedure of a Ranging/Sidelink Positioning service.

The solution is based on ProSe direct discovery security mechanism, which needs to authorize whether the UE is allowed to use the service before provisioning discovery security materials to the UE. This solution enhances the existing mechanism by adding UE role authorization as an additional condition for provisioning discovery security materials to the UE. Only when the role of UE is successfully authorized, the network will then generate and provision discovery security materials. This ensures that unauthorized UE cannot discover other UEs as it is not able to protect discovery messages.

The only impact on the network is that the network functions need to authorize the role of the UE in the service after receiving discovery request from the UE and provision discovery security materials only to the UE after successful UE role authorization.

## 6.5 Solution #5: Use of authorization tokens at PC5 security establishment

### 6.5.1 Introduction

The solution addresses Key Issue #2: Authorization for Ranging/SL Positioning Services. It aims to meet one of the potential requirements in Key issue #2 the authorization of the UE as a target UE/reference UE/assistant UE/Located UE in the Ranging/Sidelink Positioning service.

As per TR 23.700-86 [2] KI#5, when a UE is not able to perform Uu based positioning estimation, the UE may use Sidelink Positioning to obtain relative positioning with a Located UE which is in network coverage. Considering the UE may be out of network coverage or in network coverage, the UE shall be able to independently check what SL positioning service the peer UE is authorized to use and what role the peer UE is authorized to act.

In addition, a Target UE may discover a Reference UE/Assistant UE who is out of network coverage to establish the PC5 link and perform the Ranging procedure. In this case, the UE shall be able to independently check what Ranging service the peer UE is authorized to use and what role the peer UE is authorized to act.

This solution proposes a token based method as in OAuth 2.0 to meet the above requirements. The network may provide a token stating what kind of Ranging/Sidelink Positioning service the UE can use and what role it can act in the service.

The token is signed by the network with a private key and can be verified by the UE using the public key. Based on the token, the UE can independently check the authorization of peer UE during the Discovery procedure and the PC5 security establishment procedure.

This solution assumes long term credentials are provisioned into the UE(s) and form the root of the security of the PC5 unicast link as specified in TS 33.536 [5].

NOTE 1: The token for the Ranging/SL Positioning service is based on the Oauth 2.0 token defined in Clause 13.4.1.1 of TS 33.501 [3]. The details of Ranging/SL Positioning token will be decided during normative phase.

NOTE 2: For the Ranging service triggered by Ranging Application Server, the token and the associated public key can be provisioned by the Ranging Application Server. For the SL Positioning service triggered by 5GC NF, the token and the associated public key can be provisioned by the DDNMF/PKMF.

This solution assumes long term credentials are provisioned into the UE(s) and form the root of the security of the PC5 unicast link as specified in TS 33.536 [5].

### 6.5.2 Solution details

### 6.5.2.1 Token based authorization for scenario of SL positioning services

#### 6.5.2.1.1 Security for network assisted Sidelink Positioning with full network coverage

0. The Target UE/Located UE are provisioned with discovery security materials and authorization tokens when they are in coverage. If the Target UE/Located UE is authorized to use the SL Positioning service under the specific role, the network provides a token claiming the specific SL positioning service it can use and what role it can act in the service. The token is signed by the network and can be verified by the UE.

This step can be perform at any step before step #4.

1. The AMF receives a Sidelink positioning request from any 5GC NF or AF.

2. The AMF sends the Sidelink positioning request to the selected LMF.

3. The LMF decides to use the network assisted Sidelink positioning for Target UE. The LMF triggers the discovery of a Located UE for positioning assistance or performs Sidelink positioning capability negotiation with Target UE.

NOTE: Whether or not located UE ID is provided by the LMF is to be aligned with SA2.

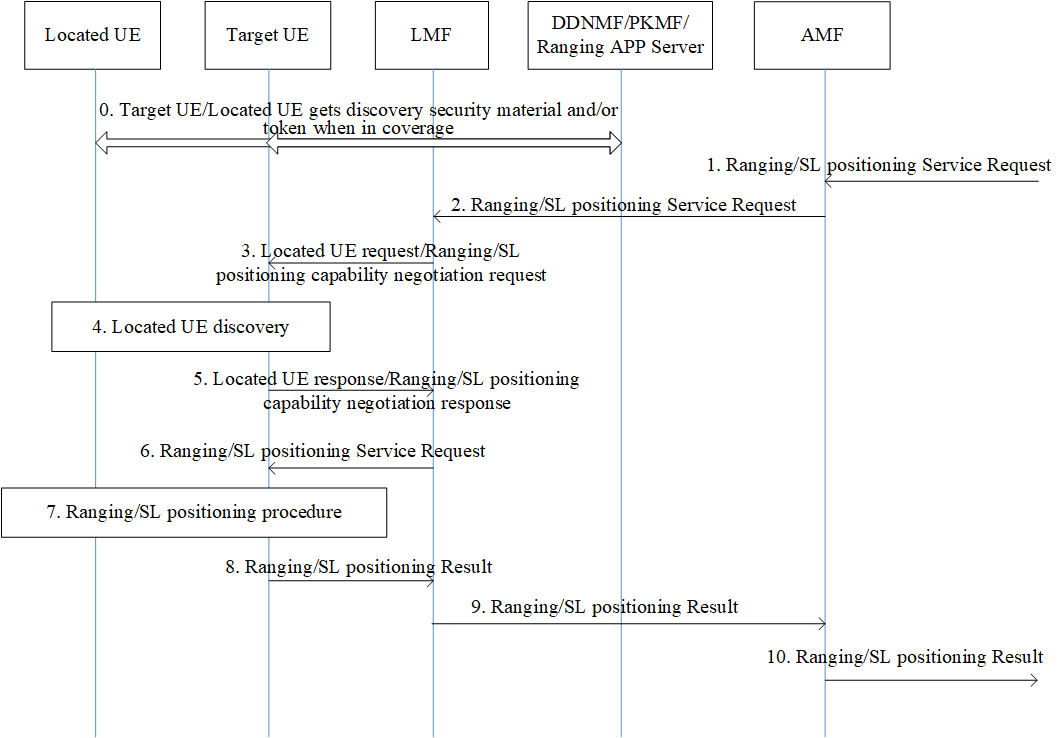


Figure 6.5.2-1: Security for Network Assisted Sidelink Positioning with Full Network Coverage

4. If the Located UE ID is provided by the LMF, Target UE performs Model B discovery with the selected Located UE. If no located UE ID is provided, Target UE performs Model A discovery by listening to announcement message send by the Located UE.

The Located UE provides the Service Code and optionally its token in the discovery message. Once receiving the discovery messages, the Target UE verifies the discovery message and optionally the token.

5. If the authorization checking is successful, the Target UE responds to LMF with the Located UE ID. If required, the Target UE also responds with the Target UE/Located UE’s Sidelink positioning capability.

6. The LMF determines the Sidelink positioning result calculation mode and the requested info. After that, the LMF sends the Sidelink positioning request to the Target UE

7. The Target UE establishes a PC5 link with the located UE for the SL positioning measurement as defined in TS 33.503 [6]. The Located UE and Target UE also exchange their tokens during the PC5 link establishment procedure for role authorization of each other. The Target UE performs Sidelink positioning procedure with the Located UE, and obtains the Sidelink positioning measurement data.

8~10. The rest of the procedure Sidelink Positioning service is performed between the Target UE and the network.

#### 6.5.2.1.2 Security for network assisted Sidelink Positioning with partial network coverage

Steps #0~#1 are the same as steps #0~#1 in clause 6.5.2.1.

2. The AMF sends the SL positioning service request to the selected LMF which includes Target UE ID and one or multiple Located UE ID(s)

3. When both Target UE ID and one or multiple Located UE ID(s) are received in the LCS service request, the LMF sends the Sidelink positioning request to one or multiple Located UE(s) to trigger the Sidelink positioning procedure.

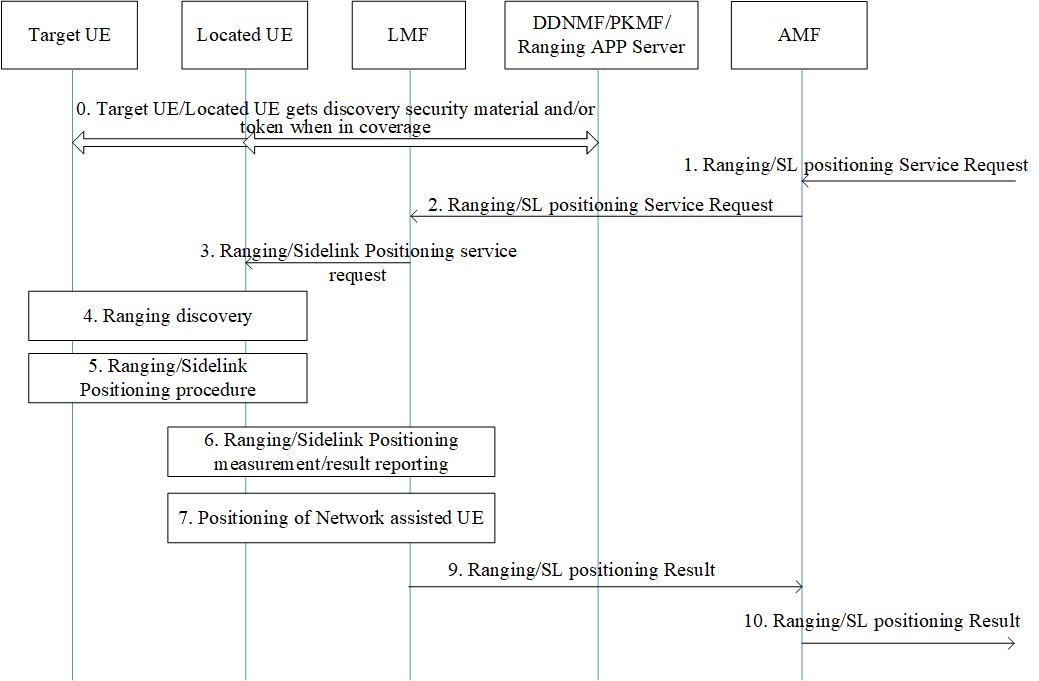


Figure 6.5.2-2: Security for Network Assisted Sidelink Positioning with Partial Network Coverage

4. The selected Located UE(s) performs the Discovery procedure (i.e. Model B discovery) to discover the Target UE which may move out of network coverage, and provides the Service Code and optionally its token to the Target UE. Once receiving the discovery messages, the Target UE verifies the integrity of discovery message and optionally the token.

5. If the authorization checking is successful, the Target UE establishes a PC5 link with the located UE for the SL positioning measurement as defined in TS 33.503 [6]. The Located UE and Target UE also exchange their tokens during the PC5 link establishment procedure for role authorization of each other.

6~9. The rest of the procedure of Sidelink Positioning service is performed between the Located UE and the network.

### 6.5.2.2 Token based authorization for scenario of Ranging services

#### 6.5.2.2.1 Security for Ranging procedure between Reference UE and Target UE

0. The Reference UE and the Target UE are provisioned with the discovery security materials and request authorization tokens when they are in 3GPP coverage.

1. The direct discovery procedure is performed by the Reference UE in order to discover the Target UE using the discovery parameters and discovery security material, based on the Ranging Service Code for the Ranging service.

2. If discovery result indicates the Target UE supports the Ranging service, the Reference UE sends a Direct Communication Request (DCR) that contains the Ranging Service Code (RSC) of the Ranging service and the authorization token of Reference UE which is retrieved from step #0, and also the Key\_Est\_Info used for direct authentication and key establishment. Protection of authorization token and RSC in DCR can be done in a similar way as described in TS33.503 [6].

3. Direct Auth and Key Establish procedure as specified in TS 33.536 [5] is performed.

4. The Target UE uses the public key provided by the network to verify the token1 of the Reference UE that the Reference UE is authorized to act as a Reference UE.



Figure 6.5.2-3: High-level Procedure of PC5 Security between Reference UE and Target UE

5. The Target UE derives KNRP and other security material as specified in TS 33.536 [5]. The Target UE sends a Direct Security Mode Command message to the Reference UE including the authorization token2 of the Target UE which is retrieved from step #0. The confidentiality protection is applied to the authorization token2.

6. The Reference UE uses the public key provided by the network to verify the token2 of the Target UE that the Target UE is authorized to act as a Target UE in the Ranging service. The Reference UE derives KNRP and other security material similar as the Target UE in step #5.

7. The Reference UE sends the Direct Security Mode Complete message to the Target UE.

8. The Reference UE and Target UE continue with the rest of procedure for the Ranging service over the secure PC5 link.

#### 6.5.2.2.2 Security for Ranging procedure between Reference UE/Target UE and Assistant UE

0. The Reference UE, the Assistant UE and Target UE are provisioned with the discovery security materials and request authorization tokens when they are in 3GPP coverage.

1. The direct discovery procedure is performed by the Reference UE in order to discover the Assistant UE using the discovery parameters and discovery security material, based on the Ranging Service Code for the Ranging service.



Figure 6.5.2-4: High-level Procedure of PC5 Security between Reference UE/Target UE and Assistant UE

2. If discovery result indicates the Assistant UE supports the Ranging service, the Reference UE sends a Direct Communication Request (DCR) that contains the Ranging Service Code (RSC) of the Ranging service and the authorization token1 of Reference UE which is retrieved from step #0, and also the Key\_Est\_Info used for direct authentication and key establishment. Protection of authorization token and RSC in DCR can be done in a similar way as described in TS33.503 [6].

3. Direct Auth and Key Establish procedure as specified in TS 33.536 [5] is performed.

4. The Assistant UE uses the public key provided by the network to verify the token1 of the Reference UE that the Reference UE is authorized to act as a Reference UE.

5. The Assistant UE derives KNRP and other security material as specified in TS 33.536 [5]. The Assistant UE sends a Direct Security Mode Command message to the Reference UE including the authorization token2 of the Assistant UE which is retrieved from step #0. The confidentiality protection is applied to the authorization token.

6. The Reference UE uses the public key provided by the network to verify the token2 of the Assistant UE that the Assistant UE is authorized to act as a Assistant UE in the Ranging service. The Reference UE derives KNRP and other security material similar as the Assistant UE in step #5.

7. The Reference UE sends the Direct Security Mode Complete message to the Assistant UE.

8. The Reference UE and Assistant UE continue with the rest of procedure for the Ranging service over the secure PC5 link.

9. Steps #1-#8 are repeated for PC5 security establishment between the Assistant UE and Target UE.

### 6.5.3 Evaluation

This solution, based on multiple solutions for KI#2 and KI#5 of TR 23.700-86 [2], addresses the first requirement in KI#2 on the authorization of the UE as a Target UE/Reference UE/Assistant UE/Located UE in the Ranging/Sidelink Positioning service.

This solution ensures that the peer UE can authorize the role of each other during Discovery procedure and PC5 link establishment procedure, covering both cases where they are in network coverage and out of network coverage.

The solution requires the network to provide the authorization token to the UE.

This solution requires the UEs to exchange their authorization tokens during Discovery procedure and PC5 link establishment procedure and verify the role.

## 6.6 Solution #6: Protection of direct communication for Sidelink Positioning service

### 6.6.1 Introduction

This solution addresses Key Issue #4 on protection of direct communication.

As assumed in clause 4.1, for Ranging/SL Positioning services, security protection for direct communication between UEs will reuse the solutions defined for V2X in TS 33.536 [5] and for ProSe in TS 33.503 [6] as much as possible. For V2X and ProSe services, direct communication security is built on the root of security, which is a long-term credential preconfigured in or provisioned to the UE by e.g. the providers of application/service. Such handling of credential configuration or provisioning can also be applied to Ranging based services, which are provided by Ranging application providers.

However, Sidelink Positioning services are primarily requested and used by the 5GC NFs in operator networks, to which the assumption of long-term credentials provisioned into each of the involved UEs in SL Positioning services can no longer apply. This is because the involved UEs (e.g. Located UE, Target UE) are not bound with a specific application and could possibly be selected arbitrarily by the network to act as the required role of UE (e.g. Located UE). In this way, long-term credential configuration in or provisioning to the involved UEs may not be practical. With the lack of long-term credential (the security root), the existing security mechanism for direct communication of V2X services or ProSe services cannot be reused.

This solution introduces a security method for protecting the direct communication for SL positioning between the UEs, which have no provisioned long-term credentials dedicated to the SL Positioning service.

### 6.6.2 Solution details

Instead of reusing direct communication security for ProSe/V2X services, this solution largely reuses the security mechanism for ProSe UE-to-Network Relay communication defined in TS 33.503 [6]. To support the security for SL Positioning services, there could be a SL Positioning Key Management Function (SLPKMF) deployed in each PLMN for generating and provisioning the security materials to the UE. Once a UE (UE-1) receives a network request to start SL positioning with another UE (UE-2), UE-1 can request a SL Positioning Key (SLPK) from its SLPKMF to be used as a root key for security establishment, before UE-1 sends the Direct Communication Request to UE-2.

1~3. UE-1 is triggered by a Sidelink Positioning Service Request message sent from any AF/5GC NF via the AMF and the LMF, requesting UE-1 to perform SL positioning operation with UE-2. The request message contains UE-1 ID and UE-2 ID.

4. Upon receiving the SL positioning request from the network, UE-1 sends a SL Positioning (SLP) Key Request to its SLPKMF. The message indicates that UE-1 is requesting a SLPK. If UE-1 already has a SLPK from the SLPKMF, the message also contains the ID of the SLPK.



Figure 6.6.2-1: Procedure of Direct Communication Security for Sidelink Positioning Service

5. The SLPKMF checks whether UE-1 is authorized to use SL Positioning service. If authorized, the SLPKMF sends a SLPK and SLPK ID to UE-1.

NOTE 1: The details of the generation of SLPK and SLPK ID are up to SLPKMF implementation.

6. The discovery procedure is performed between UE-1 and UE-2. This step can also be performed right after step #1.

7. UE-1 sends a Direct Communication Request (DCR) to UE-2 that contains the SLPK ID, SL Positioning Code (SLPC) of the SL Positioning Service and KSLP nonce 1.

NOTE 2: If UE-1 does not have a valid SLPK, UE-1 shall redo step 4 to request a new SLPK and SLPK ID before sending the DCR message.

8. UE-2 sends a SLP Key Request message to its SLPKMF that contains SLPK ID, SLPC and KSLP nonce 1.

9. The SLPKMF of UE-2 checks if UE-2 is authorized to use the SL positioning service indicated by the SLPC. If authorized, the SLPKMF of UE-2 sends the SLP Key Request with the SLPK ID to the SLPKMF of UE-1.

10. The SLPKMF of UE-1 shall check if UE-1 is authorized to use the SL positioning service indicated by the SLPC after received the SLP Key request from the SLPKMF of UE-2. The SL positioning service authorization check shall be based on the SLPK ID and SLPC included in the Key Request message.

The SLPKMF of UE-1 generates KSLP nonce 2 and derive KSLP using the SLPK identified by SLPK ID, SLPC, KSLP nonce 1 and KSLP nonce 2. Then, the SLPKMF of UE-1 returns to the SLPKMF of UE-2 a SLP Key Response message which contains KSLP and KSLP nonce 2.

11. The SLPKMF of UE-2 returns to UE-2 the SLP Key Response message containing KSLP, KSLP nonce 2, etc.

12. UE-2 derives the session key (KSLP-SESS) from KSLP and then derive the confidentiality key (SLPEK) (if applicable) and integrity key (SLPIK), and then sends a Direct Security Mode Command message including the KSLP nonce 2 to UE-1.

13. When receiving KSLP nonce 2, UE-1 derives KSLP using the SLPK, SLPC, KSLP nonce 1 and KSLP nonce 2. Then UE-1 derives the session key (KSLP-SESS) from KSLP and then derive the confidentiality key (SLPEK) (if applicable) and integrity key (SLPIK), and responds with a Direct Security Mode Complete message to UE-2 protected by SLPIK and SLPEK (if derived).

14. UE-2 responds a Direct Communication Accept message to UE-1 to complete the establishment of direct communication.

15. UE-1, UE-2 and the network proceeds the rest of the procedure.

### 6.6.3 Evaluation

This solution addresses all the potential requirements in key issue #4 for Sidelink Positioning services by reusing the security mechanisms for 5G ProSe UE-to-Network Relay communication. The solution does not rely on long-term credentials in the UE preconfigured by an application, hence could support the network to request SL positioning from any Target UE or Located UE.

The SL positioning capable UE needs to support 5G ProSe UE-to-Network Relay communication security.

Whether reusing the PKMF or defining a new function for SLPKMF is to be decided in normative phase.

## 6.7 Solution #7: Security policy based protection for Ranging/SL positioning service operation

### 6.7.1 Introduction

This solution addresses Key Issue #1 on Privacy protection for Ranging/SL Positioning services and Key issue #4 on Protection of direct communication.

In clause 8.4 of TR 23.700-86 [2], it is concluded for Key Issue #4 (Control of Operations for Ranging/Sidelink Positioning) that a Ranging/SL Positioning layer is introduced on the UE under application layer and above AS layer to control Ranging/SL Positioning operation. The functionalities supported by the Ranging/SL Positioning layer include discovery of the UE(s) participating in Ranging/SL Positioning service sessions and control signalling between UEs or between UE and LMF to manage Ranging/SL Positioning operations. The reference point for Ranging/SL Positioning layer is SR5 and Ranging/Sidelink Positioning Protocol (RSPP) is introduced for SR5 over the PC5 reference point between the UEs. RSPP supports the procedures for exchanging Ranging/SL Positioning capability, Ranging/SL Positioning assistant data and Ranging/SL positioning measurement data/result.



Figure 6.7.1-1: Ranging/SL Positioning Layer for Ranging/SL Positioning Operations

As SR5 is the interface of the Ranging/SL Positioning layer for direct communication between UEs, which carries the key information of Ranging/SL Positioning services (e.g. Ranging/SL positioning measurement data/result, assistant data), this solution introduce SR5 security policies which are used to activate the necessary integrity and confidentiality protection for direct communication between UEs for Ranging/SL Positioning services.

### 6.7.2 Solution details

As per clause 8.4 of TR 23.700-86 [2], SR5 direct communication between UEs over PC5 can reuse 5G ProSe Direct Communication procedure or V2X Communication procedure. Hence the security establishment for SR5 direct communication can also reuse the procedures for establishing PC5 direct communication security. According to TS 33.503 [6] and TS 33.536 [5], activation of PC5 link security relies on the PC5 security policies, which are provisioned to the UEs by the network (e.g. PCF) via a configured list of ProSe/V2X services and their corresponding PC5 security policies. Based on the security requirements of ProSe/V2X services run between the UEs, PC5 security policies could have three options of “REQUIRED”, “NOT NEEDED” and “PREFFERED”.

Accordingly for SR5 direct communication, it is proposed that the network (e.g. PCF) also configures a separate list of Ranging/Sidelink Positioning services and the corresponding SR5 security policies, and provisions to the UE during Service Authorization and Information Provisioning procedure. Such a list of SR5 security policies is configured separately from the list of PC5 security policies for ProSe/V2X services, because one UE could possibly support Ranging/SL positioning services in addition to ProSe/V2X services, while the security requirements for Ranging/SL positioning services could be different from those for ProSe/V2X services.

As the key information of Ranging/SL Positioning services carried between UEs are control plane RSPP/SLPP messages over SR5 reference point, SR5 security policies need to support the security requirements for protecting the RSPP/SLPP signalling, which is mostly location related (e.g. Ranging/SL positioning measurement data/result, assistant data). With such security/privacy sensitive information, integrity and confidentiality should always be activated for Ranging/SL Positioning operations to avoid violation of UE privacy and signalling tampering. Therefore, it is proposed that the SR5 security policies for integrity protection of Ranging/SL Positioning control messages should be set as “REQUIRED” only, and confidentiality protection of Ranging/SL Positioning control messages can be set as “REQUIRED”, “PREFERRED” or “NOT NEEDED” depending on operator’s configuration.

Alternatively, as SR5 security policies for Ranging/SL Positioning control messages should be set as “REQUIRED” which is the only option for security activation, it is possible that the UEs involved in direct communication over SR5 always activate the integrity protection and confidentiality protection for Ranging/SL positioning operation, without the network having to provision SR5 security policies to the UE. Then during SR5 communication security establishment procedure, the UEs only need to negotiate security algorithms but does not need to negotiate the security policies.

NOTE 1: Security is enforced on PDCP layer for either SR5 or PC5 reference point, hence security will not be established on both SR5 and PC5 for the same service session.

NOTE 2: There is only one set of security policies configured for one service (i.e. PC5 security policies for ProSe/V2X service, SR5 security policies for Ranging/SL positioning service).

### 6.7.3 Evaluation

The solution addresses the second requirement in KI#1 and the second and third requirements in KI#4.

It largely reuses the security policy based protection defined for ProSe/V2X services by configuring and provisioning SR5 security policies, hence has minimum impact on the network and the UE. Using a configuration list of Ranging/SL positioning services and corresponding SR5 security policies separate from the configuration list of ProSe/V2X services and corresponding PC5 security policies can avoid the impact on the existing security policy handling of PC5 direct communication for ProSe/V2X services when supporting the UE capable of running both ProSe/V2X services and Ranging/SL positioning services.

As per clause 8.4 of TR 23.700-86 [2], it is not determined yet whether the Ranging/SL Positioning layer is over V2X/ProSe layer or AS layer and whether SR5 is over PC5-S or PC5-U. Using SR5 security policies for Ranging/SL positioning control messages rather than PC5 security policies could ensure that the enforcement of SR5 security policies is independent from the pending conclusion in TR 23.700-86 [2]. Whichever layer or PC5 plane is determined to support Ranging/SL Positioning layer, it is SR5 security policies that should be enforced on PDCP layer for protecting Ranging/SL Positioning service operations.

Depending on the type of service (Ranging/SL positioning service or ProSe/V2X service) requested, the UE is then able to determine which security policies (SR5 security policies or PC5 security policies) to be enforced on PDCP layer.

This solution applies to unicast mode direct communication of Ranging/SL Positioning services.

## 6.8 Solution #8: Security policy based protection for ranging result sent to SL Positioning Client UE

### 6.8.1 Introduction

This solution addresses Key Issue #1 on Privacy protection for Ranging/SL Positioning services. Specifically, it addresses the second requirement in KI#1: “*The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during communication for Ranging/SL positioning*”.

In clause 8.6 of TR 23.700-86 [2], it is concluded that SL Positioning Client UE can invoke Ranging/SL positioning service for obtaining the Ranging/SL positioning result between two other UEs. SL Positioning Client UE does not have to support Ranging/SL positioning capability, but the communication between the SL Positioning Client UE and Reference/Target UE has to be established for the transmission of Ranging/SL positioning result, either via PC5 or via 5GC. If the communication can be established directly between the SL Positioning Client UE and Reference/Target UE, the ranging result is carried over PC5 link. If the communication between the SL Positioning Client UE and Reference/Target UE is established via 5GC, the ranging result transmitted from Reference/Target UE to SL Positioning Client UE is carried over the Uu link between Reference/Target UE and the network and the Uu link between SL Positioning Client UE and the network.

As ranging result contains UE location information which is security/privacy sensitive, this solution is introduced to ensure that the ranging result sent to the SL Positioning Client UE via PC5/5GC is confidentiality protected by configuring proper security policies.

### 6.8.2 Solution details

#### 6.8.2.1 Security policy configuration for ranging result sent via PC5

As per TR 23.700-86 [2], SL Positioning Client UE may not be Ranging/SL positioning capable, but should be ProSe/V2X capable to establish PC5 communication with Reference/Target UE. When ranging result is transmitted to SL Positioning Client UE via PC5, the PC5 link protection is based on PC5 security policies for ProSe/V2X layer, as specified in TS 33.503 [6] and TS 33.536 [5].



Figure 6.8.2-1: Ranging Result sent to SL Positioning Client UE via PC5

On ProSe/V2X layer, ranging result should be transmitted as the payload of PC5 direct communication. It means that, for protecting ranging result, integrity and confidentiality protection should always be activated for PC5 user plane. Therefore for ranging result transmission via PC5, the PC5 UP security policies on SL Positioning Client UE and the Reference/Target UE sending ranging result should to be configured as “REQUIRED” only for both integrity protection and confidentiality protection. The solution could be either 5GC-based or UE-based.

**5GC-based solution:**

For Ranging/SL positioning service exposed to SL Positioning Client UE, the network (e.g. PCF) sets the PC5 UP security policies as “REQUIRED” only for both integrity protection and confidentiality protection, and sets the PC5 CP security policies as “REQUIRED” only for integrity protection. The network (e.g. PCF) provisions such security policies to the involve UEs based on the Role of the UEs in the Ranging/SL Positioning Service, i.e. SL Positioning Client UE and Reference/Target UE sending the ranging result.

**UE-based solution:**

If there is no PC5 security policies provisioned from the network for Ranging/SL Positioning Service exposed to SL Positioning Client UE, the UE sending the ranging result (either Reference or Target UE) and the SL Positioning Client UE should always activate integrity and confidentiality protection on PC5 user plane, and always activate integrity protection on PC5 control plane.

#### 6.8.2.2 Security policy configuration for ranging result sent via 5GC

When ranging result is transmitted to SL Positioning Client UE via 5GC, the Uu link between the UE sending ranging result (Reference/Target UE) and the network should be integrity and confidentiality protected and the Uu link between the SL Positioning Client UE and the network should also be integrity and confidentiality protection.



Figure 6.8.2-2: Ranging Result sent to SL Positioning Client UE via 5GC

Ranging result/measurement from the Reference/Target UE to the network is always carried using LCS procedure, hence the integrity and confidentiality protection of ranging result on Uu interface can be ensured by NAS security.

For ranging result exposed by the network to the SL Positioning Client UE, either enhanced MO-LR procedure or Application exposure API can be used.

- When enhanced MO-LR procedure is used, ranging result is sent to the SL Positioning Client UE by the AMF in NAS signalling, hence the integrity and confidentiality protection of ranging result on Uu interface can be ensured by NAS security.

- When Application exposure API is used, ranging result is sent to the SL Positioning Client UE over user plane. Therefore, the integrity and confidentiality protection of ranging result on Uu interface rely on the UP security policies provided to the RAN by the 5GC (e.g. SMF) during PDU session establishment procedure, as specified in TS33.501 [8]. In this case, the SMF should be able to set the UP security policies for integrity protection and confidentiality protection to “REQUIRED” when establishing a PDU session for the Ranging/SL Positioning service exposed to SL Positioning Client UE.

### 6.8.3 Evaluation

The solution addresses the following key issue and requirement:

- The second requirement in KI#1: “The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during communication for Ranging/SL positioning”;

It largely reuses the security policy based protection defined for ProSe/V2X services by configuring proper PC5 security policies on the involved UEs, hence has minimum impact on the network and the UE. For ranging result exposed through the network, NAS security is available when using enhanced MO-LR procedure.

For PC5 communication established for ranging result transmission, if no PC5 security policies are provisioned by the network to the UE for Ranging/SL Positioning service exposure, the involved UEs simply activate integrity and confidentiality protection on PC5 user plane and integrity protection on PC5 control plane, without negotiation on security policies.

## 6.9 Solution #9: Ranging/SL Positioning discovery and link establishment procedure for V2X capable UEs

### 6.9.1 Introduction

The solution addresses Key Issue #1: Privacy protection for Ranging/SL Positioning services, Key Issue #3: Protection of discovery procedure and Key Issue #4: Protection of direct communication. It largely reuses the mechanism of Restricted Discovery procedure defined in TS 33.503 [6] and Direct Security Establishment procedure defined in TS 33.536 [5]

For V2X capable UEs, Ranging/SL Positioning discovery procedure is integrated into PC5 unicast link establishment procedure. By broadcasting the DCR message, the Reference UE and Target UE can discover each other. However, the broadcast UE identity may compromise the user’s privacy information and the missing of discovery procedure may introduce additional security threats, e.g. the unauthorized Assistance UE/Reference UE can arbitrarily initiate Ranging/SL Positioning operations with the Target UE.

This solution uses the code security parameters provided by the network to protect the privacy-sensitive information in the DCR message and uses the security materials (i.e. the long term credential) to secure the link establishment. To obtain the code security parameters, the Reference UE/Target UE and/or Assistance UE need to send the Discovery Request to the network. Once receiving the Discovery Request, the network can check the authorization, which reuses the Restricted Discovery procedure specified in TS 33.503 [6]. By authorization checking and direct authentication, the PC5 link can be securely established for Ranging/SL Positionging Service.

### 6.9.2 Solution details

#### 6.9.2.1 Security for direct discovery and communication for V2X capable UEs

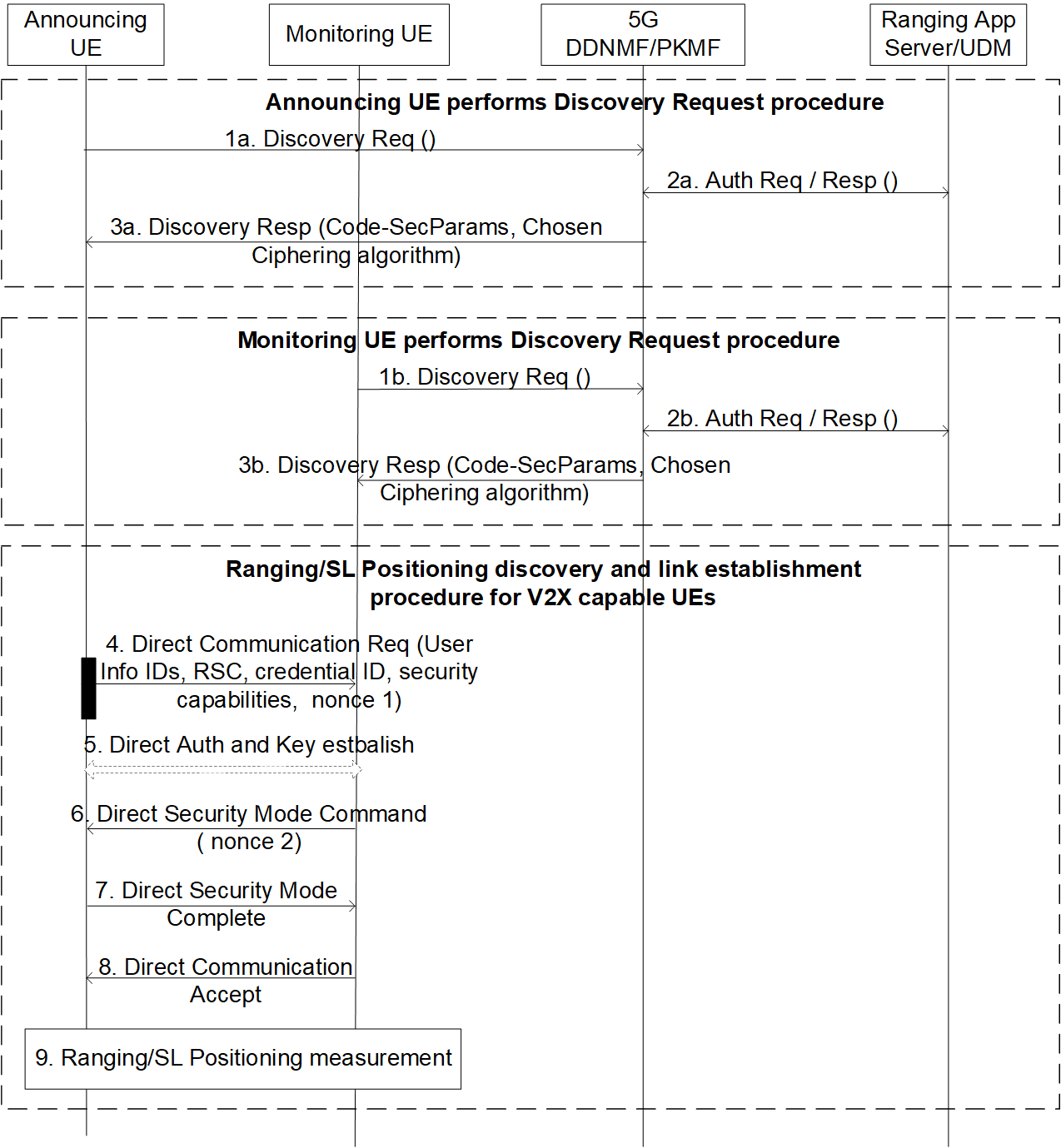


Figure 6.9.2-1: Direct discovery and communication for V2X capable UEs

Steps 1a-3a refer to the Announcing UE:

1a. The Announcing UE sends a Discovery Request message containing UE ID, the Ranging Service Code, UE security capability, the authorized role to the 5G DDNMF/PKMF in order to get the associated security material.

NOTE 1: The Announcing UE and Monitoring UE can be seen as the Reference UE, Target UE, and/ or Located UE in the Ranging/SL Positioning Service.

2a. The 5G DDNMF/PKMF may check for the authorization with the UDM/Ranging Application Server based on the UE ID, Ranging Service Code and the received role. If, based on the permission settings, the UE ID is allowed to access Ranging/SL Positioning service, the Ranging Application Server/UDM returns an authorization response.

3a. The 5G DDNMF/PKMF in the HPLMN of the Announcing UE returns the corresponding Code Security Parameters. The Code Security Parameters provide the necessary information for the Announcing UE to protect the information in the DCR message. The 5G DDNMF/PKMF of the Announcing UE also includes the chosen ciphering algorithm in the Discovery Response message. The 5G DDNMF/PKMF determines the chosen ciphering algorithm based on the Ranging Service Code and the received UE security capability in step 1a. The UE stores the chosen ciphering algorithm together with the Ranging Service Code.

Steps 1b-3b refer to the Monitoring UE:

1b. The Monitoring UE sends a Discovery Request message containing UE ID, Ranging Service Code, the authorized role and the UE security capability to the 5G DDNMF/PKMF in order to be allowed to access Ranging/SL Positioning service.

2b. The 5G DDNMF/PKMF of Monitoring UE sends an authorization request to the Ranging Application Server/UDM. If, based on the permission settings, the UE ID is allowed to access Ranging/SL Positioning service, the Ranging Application Server/UDM returns an authorization response.

3b. If the Discovery Request is authorized and the UE security capability in step 1b includes the chosen ciphering algorithm, the 5G DDNMF/PKMF responds with the Discovery Response message including the corresponding Code Security Parameters and the chosen ciphering algorithm (based on the information/keys stored in step 3a).

Steps 4-9 refer to the direct discovery and communication procedure for V2X capable UEs:

4. The Announcing UE wants to establish unicast communication with the Monitoring UE to perform Ranging/SL Positioning measurement. Then the Announcing UE broadcasts Direct Communication Request containing UE ID, Ranging Service Code, role, credential ID, nonce 1 and its security capabilities, which is integrity protected as specified in TS 33.503 [6]. The UE ID is protected by the code security parameters based on the chosen ciphering algorithm.

NOTE 2: The long term credential and long term credential ID could be pre-configured on the V2X capable UE (incl. Announcing UE and Monitoring UE) or provisioned by the network e.g. during Service Authorization and Provisioning procedure.

5. The Monitoring UE verifies the DCR message by using the code security parameter and check the Ranging Service Code and the role. If the checking is passed, the Monitoring UE may initiate a Direct Auth and Key Establish procedure with Announcing UE to generate the KNRP.

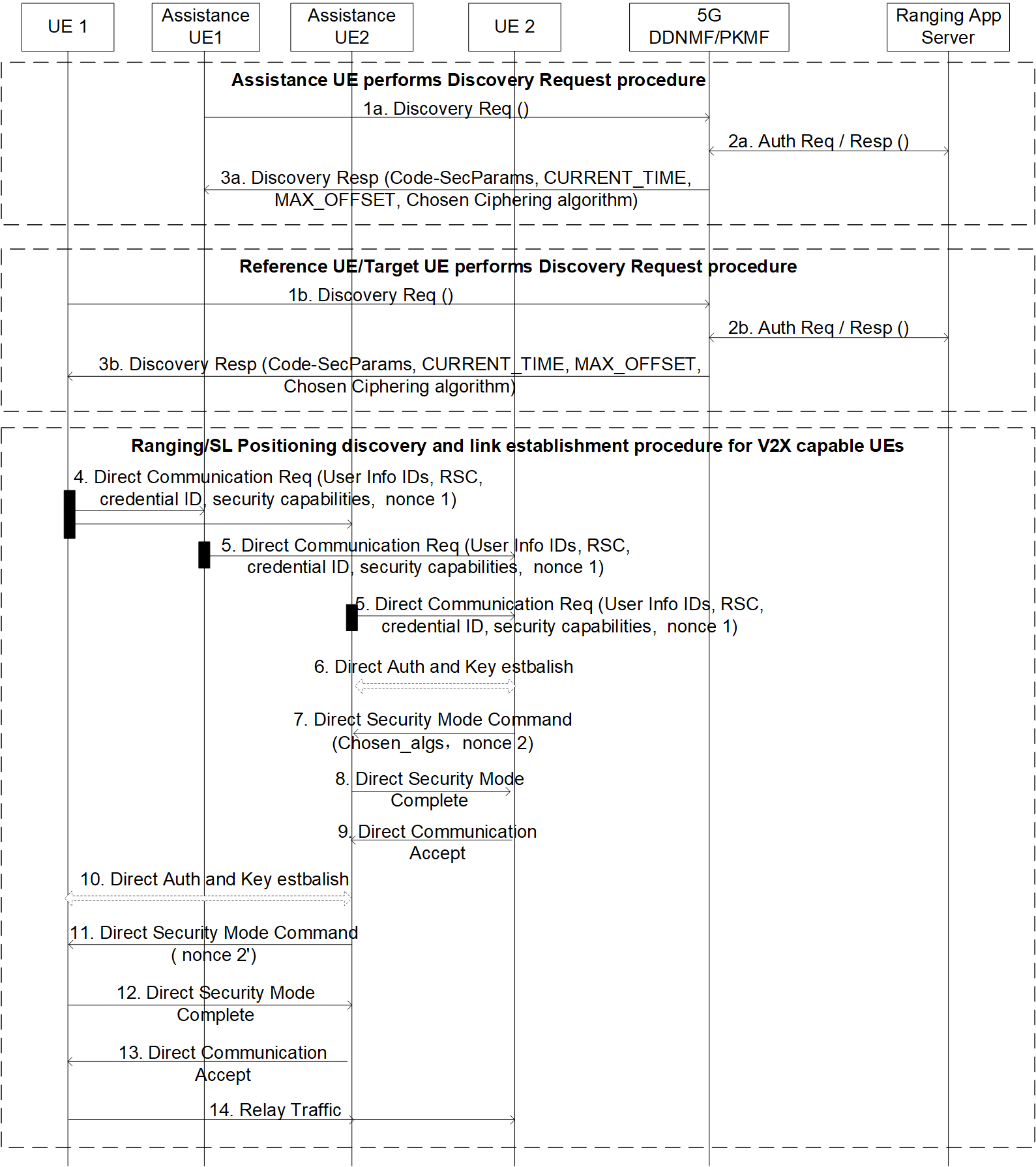
6. The Monitoring UE derives the session key (KNRP-SESS) from KNRP and then derives the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5/SR5 security policies. The Monitoring UE sends a Direct Security Mode Command message to the Announcing UE. This message includes the chosen security algorithm, nonce 2, and is protected as specified in TS 33.536 [5].

7. The Announcing UE responds with a Direct Security Mode Complete message to the Monitoring UE as specified in TS 33.536 [5].

8. Once receiving the Direct Security Mode Complete message from the Announcing UE, the Monitoring UE sends the Direct Communication Accept message to the Announcing UE.

9. The Announcing UE and the Monitoring UE perform the Ranging/SL Positioning measurement.

#### 6.9.2.2 Security for Assistant UE discovery and communication for V2X capable UEs



**Figure 6.9.2-2: Assistant UE discovery and communication for V2X capable UEs**

Steps 1a-3a refer to the Discovery Key Request procedure of Assistance UE.

1a. The Assistance UE sends a Discovery Request message to its 5G DDNMF/PKMF in order to get the associated code security parameters. The Discovery Request may contain the UE ID, its PC5 UE security capability, the role of Ranging/SL Positioning service, and Ranging Service Code, etc.

2a. The 5G DDNMF/PKMF may check for the authorization with the Ranging Application Server.

3a. The 5G DDNMF/PKMF returns the corresponding code security parameters, which provide the necessary information for the Assistance UE to protect the information in the broadcast DCR message and are stored with the Ranging Service Code. The 5G DDNMF/PKMF may also include the chosen ciphering algorithm in the Discovery Response message. The Assistance UE stores the chosen ciphering algorithm together with the Ranging Service Code.

Steps 1b-3b refer to the Discovery Key Request procedure of Reference UE/Target UE. In this solution, UE1 and UE2 refer to Reference UE and Target UE.

1b. UE1/UE2 sends a Discovery Request message containing its UE ID, its PC5 UE security capability, the role of Ranging/SL Positioning service, and Ranging Service Code to its 5G DDNMF/PKMF in order to get the associated code security parameters.

2b. The 5G DDNMF/PKMF sends an authorization request to the Ranging Application Server.

3b. If the Discovery Request is authorized and the PC5 UE security capability in step 1b includes the chosen ciphering algorithm, the 5G DDNMF/PKMF responds with the Discovery Response message including the corresponding code security parameters and the chosen ciphering algorithm (based on the information/keys stored in step 3a). UE1/UE2 stores the code security parameters, the chosen ciphering algorithm together with the Ranging Service Code.

Steps 4-14 refer to the integrated Ranging/SL Positioning discovery and link establishment procedure for V2X capable UEs over PC5 reference point.

4. UE1 wants to initiate the Ranging/SL Positioning measurement with UE2 via an Assistance UE. Then UE1 broadcasts Direct Communication Request containing UE1 ID and UE2 ID, Ranging Service Code, long term credential ID, nonce 1 and its security capabilities. The message will be received by the Assistance UE-1, Assistance UE-2. The UE1 ID and UE2 ID are protected by the code security parameters.

NOTE: The long term credential and long term credential ID could be pre-configured on the V2X capable UE (incl. Reference UE, Target UE, Assistance UE) or provisioned by the network e.g. during Service Authorization and Provisioning procedure.

5. The Assistance UE-1 and Assistance UE-2 receive the DCR message and check the Ranging Service Code. If they are authorized to provide the Ranging/SL Positioning service, then broadcast a new Direct Communication Request message. The new Direct Communication Request message may includes UE1 ID, UE2 ID and Assistance UE ID, long term credential ID, nonce 1’ and its security capabilities. The UE1 ID, UE2 ID and Assistance UE ID are protected by the code security parameters.

6. UE2 receives the Direct Communication Requests from the Assistance UE-1 and Assistance UE-2. UE2 verifies the DCR message by using the code security parameters and cshooses one Assistance UE (e.g. Assistance UE-2). UE2 may initiate a Direct Auth and Key Establish procedure with the Assistance UE-2 to generate the KNRP.

7. UE2 derives the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK). UE2 sends a Direct Security Mode Command message to the Assistance UE-2. This message includes the chosen PC5 security algorithm, nonce 2’, and is protected as specified in TS 33.536 [5].

8. The Assistance UE-2 responds with a Direct Security Mode Complete message to UE2 as specified in TS 33.536 [5].

9. Once receiving the Direct Security Mode Complete message from the Assistance UE-2, UE2 sends the Direct Communication Accept message.

10. The Assistance UE-2 may initiate a Direct Auth and Key Establish procedure with UE1 to generate the KNRP’.

11. The Assistance UE-2 derives the session key (KNRP-SESS’) from KNRP’ and then derives the confidentiality key (NRPEK’) (if applicable) and integrity key (NRPIK’). The Assistance UE-2 sends a Direct Security Mode Command message to UE1. This message includes the chosen PC5 security algorithm, the nonce 2, and is protected as specified in TS 33.536 [5].

12. UE1 responds with a Direct Security Mode Complete message.

13. The Assistance UE-2 sends the Direct Communication Accept message.

14. The secure PC5 link between UE1 and UE2 via the Assistance UE-2 is established. UE1 and UE2 can perform the Ranging/SL Positioning measurement procedure with the support of Assistance UE-2.

### 6.9.3 Evaluation

The solution fulfills the security requirements of Key issue #1: Privacy protection for Ranging/SL Positioning services, Key Issue #3: Protection of discovery procedure and Key Issue #4: Protection of unicast direct communication.

The solution addresses how the V2X-capable Ranging UEs discover and establish the PC5 link. To secure the link establishment, the security materials (i.e. the long term credentials) are used. By reusing the direct security establishment procedure specified in TS 33.536 [5], the peer Ranging UEs can authenticate each other and protect the Ranging/SL Positioning information.

In this solution, the V2X-capable Ranging UEs use the discovery security materials associated with Ranging Service Code to protect the privacy information in DCR messages. The provisioning of discovery security materials reuses the discovery request procedure defined in clause 6.1.3.2 of TS 33.503 [6].

The V2X capable UEs may not have a secure connection with the 5G DDNMF to get the security materials.

The Ranging Service Code can be seen as the Ranging/SL Positioning Application Identifier specified in TS 23.586 [11].

NOTE: Which identifier is used in the Ranging/SL Positioning needs to be coordinated with SA2.

## 6.10 Solution #10: Use of authorization tokens after PC5 security establishment

### 6.10.1 Introduction

This solution addresses Key issue #2: Authorization for Ranging/Sidelink Positioning Service. This solution addresses the authorization of the UE acting as a Target UE/Located UE in the Ranging/Sidelink Positioning service.

This solution proposes that the UE’s exchange authorization tokens after PC5 link establishment.

In the Ranging/Sidelink Positioning service, a Target UE could be out of 3GPP coverage via Uu interface and needs assistance from another UE e.g. a Located UE which is in 3GPP coverage via Uu interface or a Target UE could be in 3GPP coverage via Uu interface but needs assistance from another UE which is out of 3GPP coverage.

This solution provides a mechanism for the 5G Ranging/SL positioning system to be able to support the authorization of a UE using a specific Ranging/Sidelink Positioning service or a UE acting as a Target UE or a Located UE.

This solution assumes long term credentials are provisioned into the UE(s) and form the root of the security of the PC5 unicast link as specified in TS 33.536 [9].

This solution proposes to use authorization tokens as in OAuth 2.0.

When the UE registers in the 3GPP network then the PCF provides the authorization policy to the UE indicating whether the UE is authorized to act as a Target UE/Located UE.

The network may also provide a token stating what kind of Ranging/Sidelink Positioning service the UE can use. The token has an expiration time (i.e. a corresponding lifetime) and is signed with a private key. The network also provides the public key to the UEs to be used for verifying the token from other UE’s.

If the token needs to be revoked due to its lifetime has expired, then the UE needs to connect to the 3GPP network via Uu interface in order to retrieve a new public key from the network.

Editor’s Note: Which network function provides authorization token and how the UEs get the public key of token signing entity are FFS.

Editor’s Note: For the token verification, why public key is required is FFS.

Editor’s Note: The necessity for the role authorization is FFS.

### 6.10.2 Solution details

Figure 6.10.2-1 illustrates the high-level procedure of the proposed solution.

The signalling flow describes the use case when the Target UE is in 3GPP coverage via Uu interface and Located UE is out of 3GPP coverage.

The same signalling flow applies also to the use case when the Located UE is in 3GPP coverage via Uu interface and Target UE is out of 3GPP coverage. The Located UE would take the role as Target UE and the Target UE would take the role as the Located UE in this case in the solution below.



Figure 6.10.2-1: High-level procedure of exchange of authorization tokens between Located UE and Target UE after PC5 security establishment

0. The Target UE and the Located UE are provisioned with the discovery security materials and request authorization tokens when they are in 3GPP coverage.

1. The direct discovery procedure is performed by the Target UE in order to discover the Located UE using the discovery parameters and discovery security material, based on the Relay Service Code for the Ranging service.

2. If discovery result indicates the Located UE supports the Ranging service, the Target UE sends a Direct Communication Request (DCR) that contains the Relay Service Code (RSC) of the Ranging service which is retrieved from step 0, and also the Key\_Est\_Info used for direct authentication and key establishment. Protection of RSC in DCR can be done in a similar way as described in TS33.503 [6].

3. Direct Auth and Key Establish procedure as specified in TS 33.536 [9] is performed.

4. The Located UE derives KNRP and other security material as specified in TS 33.536 [9]. The Located UE sends a Direct Security Mode Command message to the Target UE.

5. The Target UE sends the Direct Security Mode Complete message to the Located UE.

6. The Located UE send the Direct Security Mode Accept to the Target UE.

7. The Target UE and the Located UE exchange the authorization tokens in separate signaling messages.

7a. The Target UE uses the public key provided by the network to verify the token of the Located UE e.g. whether Located UE is allowed to use the Ranging service and/or whether it’s allowed to act as a Located UE etc.

7a. The Located UE uses the public key provided by the network to verify the token of the Target UE e.g. whether Target UE is allowed to use the Ranging service and/or whether it’s allowed to act as a Target UE etc.

8. The Target UE and the Located releases the PC5 link if the verification of the authorization tokens fails.

### 6.10.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

## 6.11 Solution #11: Client UE authorization for service exposure through sidelink

### 6.11.1 Introduction

This solution addresses Key Issue #2 on authorization for Ranging/Sidelink Positioning Service. Specifically, it addresses the fourth requirement in KI#2: “*The 5G Ranging/SL positioning system shall be able to support the authorization of a SL Positioning Client UE for triggering Ranging/Sidelink Positioning services and obtaining the location information*”.

In clause 8.6 of TR 23.700-86 [2], it is concluded that SL Positioning Client UE can invoke Ranging/SL positioning service to be performed between two other UEs. For accessing Ranging/SL positioning service and obtaining the Ranging/SL positioning result of other UEs, SL Positioning Client UE needs to be authorized, so as to avoid privacy violation of the involved UEs and charging invalidation. Authorization of SL Positioning Client UE needs to be performed at different levels:

- The first level of authorization is for service access, i.e. SL Positioning Client UE should be authorized to request Ranging/SL positioning service. This level of authorization could be achieved with the existing authorization method during direct discovery and communication establishment as defined in TS 33.503 [6].

- The second level of authorization is for preserving UE privacy. This is because, even if SL Positioning Client UE is authorized to request Ranging/SL positioning service, it does not mean that Ranging/SL positioning result of a pair of any UEs can always be exposed to SL Positioning Client UE. For example, it is possible that SL Positioning Client UE is allowed to request ranging result between UE1 and UE2, but may not be allowed to request ranging result between UE3 and UE4. Without further check on the authorization info of the involved UEs, there is still the risk that ranging result between specific UEs could be exposed to unauthorized SL Positioning Client UE. Therefore, SL Positioning Client UE needs to be further authorized on whether it is allowed to obtain ranging result of the involved UEs.

Also as per clause 8.6 of TR 23.700-86 [2], the Ranging/SL positioning service can be exposed to a SL Positioning Client UE either through sidelink or through 5GC network. This solution introduces a method of finer level of authorization for preserving UE privacy before SL Positioning Client UE requests to obtain ranging result between two specific UEs through sidelink.

### 6.11.2 Solution details

#### 6.11.2.1 Authorization of SL Positioning Client UE during direct link establishment

As per TR 23.700-86 [2], SL Positioning Client UE may not support Ranging/SL positioning operation, but is able to establish PC5 direct communicate with the Reference/Target UE which sends ranging results to the SL Positioning Client UE. During the establishment of direct communication, to prevent the SL Positioning Client UE from requesting ranging results of the UEs it is not allowed to have, the Reference/Target UE should be able to authorize the SL Positioning Client UE based on the information of the involved UEs sent by the SL Positioning Client UE in the Direct Communication Request.

As the Reference/Target UE itself may lack the information required to authorize the SL Positioning Client UE, it needs the support from the network for the authorization. The network function which is able to support the authorization could be the network function provisioning the information of Ranging/SL positioning exposure to the UE during Service Authorization and Information Provisioning procedure. Based on the authorization result provided by the network, the Reference/Target UE then determines whether to proceed with security establishment for the PC5 connection or not.



Figure 6.11.2-1: Authorization of SL Positioning Client UE during Direct Link Establishment

1. SL Positioning Client UE and one of the involved UEs (UE1) discover each other using Model B discovery.

2. SL Positioning Client UE performs direct PC5 link establishment procedure with UE1 by sending the Direct Communication Request (DCR) message. The message contains at least the Source info (Client UE info), the Destination info (UE1 info), the Service info (Ranging Service Code), as well as the target UE info (UE2 info) of which the Client UE intends to request the ranging result.

3. Upon receiving the DCR message from the SL Positioning Client UE, UE1 sends an Authorization Request message to its PKMF/PCF. The message contains at least the Client UE info, the involved UE info (UE1/UE2 info) and the Ranging Service Code.

NOTE: UE1 (the UE that the SL Positioning Client UE communicates with) needs to be in network coverage.

4. Based on the information in the received request, the PKMF/PCF of UE1 sends the Authorization Request message to the PKMF/PCF of the Client UE, which authorizes whether the Client UE is allowed to request ranging result of UE1/UE2 based on its local information. Or the PKMF/PCF of the Client UE further interacts with the Ranging/SL positioning server for authorizing the Client UE. Or the PKMF/PCF of UE1 sends the Authorization Request message directly to the Ranging/SL positioning server for authorizing whether the Client UE is allowed to request ranging result of UE1/UE2. The message contains at least the Client info, the involved UE info (UE1/UE2 info) and the Ranging Service Code. The Ranging/SL positioning server then returns the authorization result to the PKMF/PCF of the UE1 directly or via the PKMF/PCF of the Client UE.

5. The PKMF/PCF of UE1 returns the authorization result to UE1.

6a. If the authorization is successful, UE1 performs a Direct Auth & Key Establish procedure with the SL Positioning Client UE. Then UE1 proceeds to step #7.

6b. If the authorization fails, the UE1 sends a Direct Communication Reject message to the SL Positioning Client UE, which may contain the failure cause. Then the following steps are not performed.

7. UE1 sends Direct Security Mode Command message to the SL Positioning Client UE for establishing PC5 security context.

8. Upon receiving Direct Security Mode Command, the SL Positioning Client UE responds Direct Security Mode Complete message to UE1.

9. Upon receiving Direct Security Mode Complete, UE1 starts to perform the Ranging/SL positioning procedure with the involved UEs (UE1/UE2) respectively.

10. UE1 calculates the ranging result between the involved UEs and responds to the SL Positioning Client UE with Direct Communication Accept message, which contains the ranging result between the involved UEs (UE1/UE2).

#### 6.11.2.2 Authorization of SL Positioning Client UE after direct link establishment

If the SL Positioning Client UE is Ranging/SL Positioning capable, and if the Ranging/SL Positioning layer is above ProSe/V2X layer (pending on the conclusion in TR 23.700-86 [2]), it is proposed to authorize SL Positioning Client UE after PC5 link establishment, so that the existing PC5 direct communication procedure defined for ProSe/V2X layer will not be impacted. That means the authorization of SL Positioning Client UE is performed during the control operation procedures via SR5 interface over the established PC5 link and probably using RSPP/SLPP protocol.



Figure 6.11.2-2: Authorization of SL Positioning Client UE after Direct Link Establishment

1. SL Positioning Client UE and one of the involved UEs (UE1) discover each other using Model B discovery.

2. SL Positioning Client UE and UE1 establish a PC5 link, which is protected using the PC5 direct communication security mechanism defined in TS 33.503 [6].

3. To invoke the Ranging/SL positioning between UE1 and UE2, the SL Positioning Client UE sends a ranging service request to UE1 on SR5 interface (e.g. using RSPP protocol) to request ranging result between UE1 and UE2. The SR5 message may include the SL Positioning Client UE info and the involved UE (UE1/UE2) info.

4. UE1 sends an Authorization Request message to its PKMF/PCF. The message contains at least the SL Positioning Client UE info, UE1/UE2 info and the Ranging Service Code.

5a. Based on the information in the received request, the PKMF/PCF of UE1 sends the Authorization Request message to the PKMF/PCF of the Client UE. The PKMF/PCF of the Client UE authorizes whether the Client UE is allowed to request ranging result of UE1/UE2 based on its local information, or the PKMF/PCF of the Client UE further interacts with the Ranging/SL positioning server for authorizing the Client UE. The message contains at least the Client UE info, the involved UE info (UE1/UE2 info) and the Ranging Service Code.

5b. Based on the information in the received request, the PKMF/PCF of UE1 sends an Authorization Request message to the Ranging/SL positioning server to authorize whether the Client UE is allowed to request ranging result of UE1/UE2. The message contains at least the Client UE info, the involved UE info (UE1/UE2 info) and the Ranging Service Code.

6a. The PKMF/PCF of the Client UE returns the authorization result to the PKMF/PCF of UE1, or the Ranging/SL positioning server returns the authorization result to the PKMF/PCF of UE1 via the PKMF/PCF of the Client UE.

6b. The Ranging/SL positioning server returns the authorization result to the PKMF/PCF of UE1.

7. The PKMF/PCF of UE1 returns the authorization result to UE1.

8a. If the authorization is successful, UE1 starts to perform the Ranging/SL positioning procedure with UE2. Then UE1 proceeds to step #9.

8b. If the authorization fails, UE1 does not perform ranging with UE2 but responds to the SL Positioning Client UE with the Ranging service response, which may contain the failure cause. Then the following steps are not performed.

9. UE1 calculates the ranging result between the involved UEs and responds to the SL Positioning Client UE with the Ranging service response. The ranging service response includes the ranging result between the involved UEs (UE1/UE2).

#### 6.11.2.3 Authorization of SL Positioning Client UE during direct discovery

Though SL Positioning Client UE may not support Ranging/SL positioning operation, it still needs to perform direct discovery procedure to discover one of the UEs (Reference/Target UE) performing Ranging/SL positioning operations. If the SL Positioning Client UE already knows the specific UEs from which it expects to obtain the ranging result when performing discovery procedure with the network, it is then able to send the information of the specific UEs to the network, which then could help to authorize the SL Positioning Client UE based on the UE information. Only after the SL Positioning Client UE is successfully authorized (service access authorization + UE privacy authorization), the network will provision the discovery security materials to the SL Positioning Client UE. In this way, the SL Positioning Client UE not allowed to acquire the Ranging result of the expected UEs will not be able to discover the UEs without getting the required discovery security materials.



Figure 6.11.2-3: Authorization of SL Positioning Client UE during Discovery

1. UE1 sends a Discovery Request message to its PKMF/DDNMF/PCF. The message includes at least the Ranging service code for which the discovery is performed.

2. The PKMF/DDNMF/PCF of UE1 checks with the Ranging/SL Positioning Server whether UE1 is authorized to use Ranging/SL Positioning service.

3. The PKMF/DDNMF/PCF of UE1 generates the discovery security materials for UE1 according to TS 33.503 [6] by associating the discovery keys with the Ranging service code.

4. The PKMF/DDNMF/PCF of UE1 responds to UE1 with discovery security materials.

5~7. UE2 requesting the same Ranging service (with the same Ranging service code) performs the same procedure as UE1 and obtains the discovery security materials associated with the Ranging service code from the PKMF/DDNMF/PCF of UE1.

8. The Client UE sends a Discovery Request message to its PKMF/DDNMF/PCF. The message includes at least the Ranging service code for which the discovery is performed. If the Client UE already knows the specific UEs of which the Ranging result is requested, the message also contains the list of the UEs, e.g. UE1/UE2.

9. The PKMF/DDNMF/PCF of the Client UE first checks with the Ranging/SL Positioning Server whether the Client UE is authorized to use Ranging/SL Positioning service against the Ranging service code (i.e. service access authorization). Then it checks whether the Client UE is authorized to request the Ranging result of the specific UEs against the list of the UEs (i.e. UE privacy authorization).

10a. If the authorization succeeds, the PKMF/DDNMF/PCF of the Client UE sends a Discovery Request to the PKMF/DDNMF/PCF of one of the listed UE (UE1). The request contains at least the Ranging service code, the Client UE info and the list of the UEs.

10b. If the authorization fails, the PKMF/DDNMF/PCF of the Client UE returns a Discovery Response to the Client UE with a failure cause.

11. The PKMF/DDNMF/PCF of UE1 may also contact the Ranging/SL Positioning Server to check whether the Client UE is authorized to request Ranging result of the UEs. The check is performed against the Client UE info and the list of the UEs.

12a. If the check with Ranging/SL Positioning Server succeeds, the PKMF/DDNMF/PCF of UE1 responds to the PKMF/DDNMF/PCF of the Client UE with the discovery security materials.

12b. If the check with Ranging/SL Positioning Server fails, the PKMF/DDNMF/PCF of UE1 responds to the PKMF/DDNMF/PCF of the Client UE with a failure cause.

13. The PKMF/DDNMF/PCF of the Client UE provides the discovery security materials to the Client UE.

14. UE1 starts to broadcast announcement messages protected by the discovery security materials. The announcement message includes at least the UE1 info, Ranging service code, etc.

15. The Client UE and UE2 start to monitor announcement messages broadcast by neighbouring UEs (UE1), and respond to UE1 after verifying the announcement message with the discovery security materials.

16. The UEs successfully discover each other.

17. Direct link is set up between UE1 and the Client UE.

18. The Client UE sends a ranging service request to UE1, requesting Ranging estimation between UE1 and UE2.

19. UE1 performs the ranging and positioning procedure with UE2.

20. UE1 calculates the Ranging result of UE1/UE2.

21. UE1 returns to the Client UE the ranging result of UE1/UE2

### 6.11.3 Evaluation

This solution fulfils the fourth requirement in KI#2. It also addresses NOTE 1 in clause 8.6 of TR 23.700-86 [2].

Authorization through the network during discovery is already supported by the relevant 5GC NFs.

Authorization through the network during link establishment or during Ranging/SL positioning operations is a new requirement on the UE, but it has no impact on the procedures of link establishment and Ranging/SL positioning per se. The UE only needs to determine when to request authorization from the network in between the procedure.

The detailed check for per UE authorization is done by the Ranging/SL Positioning server. The UE and the relevant 5GC NFs only need to send the info of all involved UEs (Client UE and to-be-measured UEs) to the Ranging/SL Positioning server.

The solution can accommodate different conditions with the three options:

- If the SL Positioning Client UE can already determine the to-be-measured UEs when initiating discovery, the authorization can be performed during discovery.

- If the SL Positioning Client UE cannot determine the to-be-measured UEs yet when initiating discovery, the authorization needs to be performed after discovery.

a) With Client UE not Ranging/SL positioning capable, the authorization can only be performed during link establishment over PC5.

b) With Ranging/SL positioning capable Client UE, the authorization can be performed either during link establishment or during Ranging/SL positioning operations. On which stage the authorization should be performed for Ranging/SL positioning capable Client UE is to be determined during normative work.

## 6.12 Solution #12: Ranging/SL Positioning discovery security for 5G ProSe capable UEs

### 6.12.1 Introduction

This solution addresses Key Issue #3 on protection of discovery procedure as well as Key Issue #1 on privacy protection for Ranging/SL Positioning services.

### 6.12.2 Solution details

As per clause 8.3 of TR 23.700-86 [2], it is concluded that, for Ranging/Sidelink Positioning device discovery between 5G ProSe capable UEs, 5G ProSe Direct Discovery procedures (including both Model A and Model B) defined in 6.3.1 of TS 23.304 [4] are used. Based on such conclusion, it is proposed in this solution that the following security mechanisms defined in clause 6.1.3.2 of TS 33.503 [6] are reused for Ranging/Sidelink Positioning device discovery between 5G ProSe capable UEs:

- For Ranging-based services provided by application providers, discovery security materials are provided by the 5G PKMF.- For network assisted SL positioning services provided by operators, assuming the SL positioning service code (similar as RSC) is configured in or provisioned to the UE before discovery, then discovery security materials can be provided in the same way as for 5G ProSe UE-to-Network Relay discovery defined in TS 33.503 [6].

- Security materials used by a sending UE to protect discovery messages are provided in the Code-Sending Security Parameters. Security materials used by a UE receiving discovery messages are provided in the Code-Receiving Security Parameters. The security parameters contain the keys for integrity protection, message-specific confidentiality and scrambling of discovery messages based on the configuration by network.- The ciphering algorithm for discovery message confidentiality is configured by the network during discovery request procedure.

### 6.12.3 Evaluation

This solution fulfils all potential requirements in key issue #3 for discovery message protection and the first requirement in key issue #1, by reusing the security mechanism defined for restricted 5G ProSe Direct Discovery, hence has no new impact on the UE or the network.

The solution applies to both Ranging-based services provided by application providers and network assisted SL positioning services provided by operators.

The solution applies to 5G ProSe capable UEs.

## 6.13 Solution #13: Security of Ranging unicast communication

### 6.13.1 Introduction

This solution addresses the protection of direct communication (unicast) for Ranging/SL Positioning service as specified in Key Issue #4. Generally, the solution uses the direct communication security defined for 5G ProSe in TS 33.503 [6] and/or for 5G V2X in TS 33.536 [5] as a baseline and adjusts to the Ranging/SL Positioning scenario.

### 6.13.2 Solution details

In this solution, the Ranging/SL positioning capable UEs are provisioned with the list of Ranging/SL Positioning services, with Geographical Area(s) and their PC5 security policies. The definition of the PC5 security policies follows the definition in 5G eV2X in TS 33.536 [5] and/or in ProSe in TS 33.503 [6].

During the establishment of the direct communication for the Ranging/SL positioning service, the UEs use the PC5 security policy to negotiate the final security protection status, as defined in 5G ProSe in TS 33.503 [6] and/or in 5G V2X in TS 33.536 [5]. The Ranging/SL Positioning signalling are protected based on the PC5 UP security policies.

If multiple V2X/ProSe services use the same PC5 unicast link, it shall be checked whether the security in use for the PC5 unicast link satisfies the PC5 signalling and user plane security policies of the to-be added V2X/ProSe services, as specified in TS 33.536 [5].

### 6.13.3 Evaluation

This solution addresses the first three security requirements of Key Issue #4. The mutual authentication between two UEs during one-to-one communication is supported by reusing the PC5 security establishment procedure in 5G ProSe in TS 33.503 [6] and/or in 5G V2X in TS 33.536 [5]. If multiple V2X/ProSe services use the same PC5 unicast link, it shall be checked whether the security in use for the PC5 unicast link satisfies the PC5 signalling and user plane security policies of the to-be-added V2X/ProSe services, as specified in TS 33.536 [5].

## 6.14 Solution #14: Direct communication security for Ranging-based services

### 6.14.1 Introduction

This solution addresses Key Issue #4 on protection of unicast direct communication and Key Issue #1 on privacy protection for Ranging/SL Positioning services.

### 6.14.2 Solution details

As per clause 8.4 of TR 23.700-86 [2], it is concluded for control of Ranging/SL positioning operations that, Ranging/SL Positioning Protocol (RSPP) is introduced for SR5 over PC5 reference point between UEs. Though whether RSPP is over PC5-U or over PDCP is to be aligned with RAN WG decision, SA2 WG assumes that Ranging/SL Positioning signaling is carried between UEs over PC5-U, for which V2X communication procedures defined in TS 23.287 [3] and 5G ProSe Direct Communication procedures defined in TS 23.304 [4] are reused. Based on such conclusion, it is proposed in this solution that the following security mechanisms for V2X unicast mode communication defined in clause 5.3 of TS 33.536 [5] and for 5G ProSe unicast mode Direct Communication defined in clause 6.2 of TS 33.503 [6] are reused for unicast direct communication of Ranging-based services:

- Long-term credentials are provisioned into the UE to form the root of security for PC5 unicast link. Long-term credentials can be preconfigured in the UE by Ranging application providers or provided by Ranging applications on the UE.

- Triggered by the received Direct Communication Request (DCR) message, Direct Auth and Key Establishment procedure is performed for mutual authentication between the UEs, during which the key KNRP is derived using the long-term credentials. The authentication method is application specific and out of 3GPP scope.

- Direct communication security is established between the UEs through Direct Security Mode Command procedure based on KNRP.

NOTE 1: Procedure details can refer to steps 4~8 of solution #9 in clause 6.9.2.1.

- If RSPP signalling on SR5 reference point is carried over PC5-U, SR5 security policies are applied for PC5-U security activation.

NOTE 2: Provision and configuration of SR5 security policies can refer to solution #7.

### 6.14.3 Evaluation

This solution fulfils all potential requirements in key issue #4 for protection of unicast direct communication, by reusing the security mechanisms defined for V2X unicast mode communication in TS 33.536 [5] and for 5G ProSe unicast mode Direct Communication in TS 33.503 [6]. Hence the solution has no new impact on the UE and the network.

As confidentiality protection is provided by the reused security mechanism, the solution also fulfils the second requirement in key issue #1 for privacy protection during communication.

The solution applies to Ranging-based services provided by application providers.

The solution applies to both V2X capable UEs and 5G ProSe capable UEs.

## 6.15 Solution #15: Protection of information over group communication for Ranging/SL Positioning service

### 6.15.1 Introduction

This solution addresses the Key Issue #1 (second requirement) and #5.

This solution provides a security mechanism in SLPP layer to protect the information exchanged between UEs using group communication. The mechanism proposes to provision security materials to the UEs which belong to a particular group for a SL positioning service. By using the provisioned security materials, a UE in the group can send confidentiality and integrity protected messages that include information related to the SL positioning service, and other UEs in the same group can undo the protection of the received messages. Note that this solution supports both in-coverage and out-of-coverage UEs by provisioning multiple sets of security materials associated with different expiry times.

### 6.15.2 Solution details

#### 6.15.2.1 Security flows



Figure 6.15.2.1-1: Security flows for Sidelink Positioning one-to-many communication

0a and 0b. The UE is provided with the Ranging/SL positioning application identifier during the parameters/policy provisioning for Ranging/SL positioning service as specified in clause 5.1 of TS 23.586 [11].

NOTE 1: The SLPP one-to-many communication can use either broadcast or groupcast at the AS layer.

NOTE 2: For ProSe UEs, the Ranging/SL positioning application identifier is the ProSe identifier as per TS 23.586 [11].

NOTE 3: For V2X UEs, the Ranging/SL positioning application identifier is the V2X service type as per TS 23.586 [11].

NOTE 4: Whether to include group ID and group member ID in the SLPP message will be decided during normative work.

Editor’s Note: whether V2X UEs can support the same procedure would be determined by SA2.

Steps 1 – 3 refer to a sending UE.

1a. The UE establishes a secure connection with the Sidelink Positioning Key Management Function (SLPKMF) based on the security procedures specified in clause 5.2.5 of TS 33.503 [6]. The UE sends a Key Request message to Sidelink Positioning Key Management Function (SLPKMF) including the Ranging /SL positioning application identifier.

1b. The SLPKMF replies with the Key Response message containing the Sidelink Positioning Group Key (SLPGK), the key ID (SLPGK ID), the validity time, and the chosen ciphering and integrity algorithms. In addition, the Key Response message can include multiple SLPGK and SLPGK ID pairs with different validity times. Group member ID can be either assigned by the SLPKMF or generated at the UE. In the former case, the Group member ID is included in the Key Response message. In the latter case, the UE generates a Group member ID randomly so that it is uniquely identified in a group.

NOTE 5: In case the SLPLMF of a receiving UE is different from the SLPKMF of a sending UE, the provisioning of security materials as specified in clause 6. 1.3.2 in TS 33.503 [6] is reused.

NOTE 6: Group refers to the Ranging/SL positioning service. Accordingly, Group ID refers to the Ranging/SL positioning application identifier and Group member ID refers to the identifier of the UE that is authorized to receive the Ranging/SL positioning service.

NOTE 7: The length of a Group member ID will be determined during the normative work. When the Group member ID is randomly generated by the UE, its length should be long enough to avoid collision.

NOTE 8: Whether group member ID is provisioned by the network or self-selected will be decided during normative work.

2. Upon receiving the Key Request message, the UE derives the Sidelink Positioning Traffic Key (SLPTK) from SLPGK using Group ID, Group member ID, and SLPTK ID. SLPTK ID is a counter set to a unique value in the sending UE that has not been previously used together with the same SLPGK and the associated SLPGK ID. The UE further calculates the Sidelink Positioning Encryption Key (SLPEK) and Sidelink Positioning Integrity Key (SLPIK) from SLPTK using the chosen algorithm IDs, respectively.

3. The UE protects the messages as described in clause 6.15.2.2.1, and sends the messages to the group.

Steps 4 – 5 refer to receiving UEs.

4. The UE performs a Key Request procedure to get security materials from the SLPKMF. This step is same as the step 1.

5. Upon receiving the message from sending UE in the group, the UE calculates SLPTK, SLPEK and SLPIK. The derivation of security keys is same as the step 3 except that the UE takes Group ID, SLPGK ID, SLPTK ID and Group member ID (if it is included) in the received message as input parameters for key derivation. Then, the UE unprotects the message and verifies the integrity of the message as described in clause 6.15.2.2.2.

#### 6.15.2.2 Protection of messages between UEs

##### 6.15.2.2.1 Message processing in the sending UE

The UE sending a message to the group does the following steps:

1. Form message header that contains Group ID, Group member ID, SLPGK ID, SLPTK ID, and Counter. Then, append the Payload to it as illustrated in figure 6.15.2.2.1-1.

2. If the network configuration is to use integrity protection, calculate MAC of the message header and the Payload based on the chosen integrity algorithm. The integrity algorithms specified in Annex D in TS 33.501 [8] are used to calculate MAC. If the network configuration is not to use integrity protection, then the sending UE shall set the MAC to all zeroes or a random number in the message header.

NOTE 9: setting the MAC to all zeroes is less preferred.

3. If the network configuration is to use confidentiality protection, add confidentiality to the Payload and MAC based on the chosen ciphering algorithm. The ciphering algorithms specified in Annex D in TS 33.501 [8] are used for the confidentiality protection.

NOTE 10: the details of input parameters to the integrity algorithms and ciphering algorithms will be specified in normative work.



Figure 6.15.2.2.1-1: SLPP message format for Sidelink Positioning group communication

Editor’s Note: privacy for the Group ID and Group member ID is FFS.

##### 6.15.2.2.2 Protected message processing in the receiving UE

The UE receiving a message does the following steps:

1. If the network configuration is to use confidentiality protection, undo confidentiality protection based on the chosen ciphering algorithm.

2. If the network configuration is to use integrity protection, verify the integrity of the received message by checking MAC based on the chosen integrity algorithm.

### 6.15.3 Evaluation

This solution addresses the second security requirement in Key Issue #1 (privacy protection during communication for Ranging/SL positioning) and all the security requirements in Key Issue #5 (Confidentiality, integrity, and replay protection of SLPP signaling over groupcast and broadcast).

This solution supports both in-coverage and out-of-coverage UEs.

Editor’s Note: Further evaluation is FFS.

## 6.16 Solution #16: Privacy protection of Located UE during its discovery and selection

### 6.16.1 Introduction

This solution addresses Key Issue #1 on Privacy protection for Ranging/SL Positioning services.

In clause 5.2.2 of TS 23.586 [11], it is specified that a Target UE may discover and select one or more Located UEs to be used in the Ranging/SL positioning procedures to facilitate the accurate positioning of the Target UE. However, if the Target UE discovers and selects a Located UE which does not allow the exposure of its location information, the privacy of the Located UE is then violated. This solution introduces a method to preserve the privacy of the Located UE when it is being discovered and selected by the Target UE.

### 6.16.2 Solution details

According to clause 5.2.2 of TS 23.586 [11], for network assisted Ranging/SL positioning, the Target UE shall discover and select a Located UE that is in the same serving PLMN of the Target UE, and privacy aspects of exposing and sharing the location of the Located UE (e.g. to any Target UE) during discovery needs to be considered. Based on such specification, the privacy requirement of the Located UE needs to be checked during discovery procedure before the Located UE is selected by the Target UE.

This solution proposes that, while the Located UE requests discovery keys from the network, the network needs to check the privacy requirements of the Located UE before providing discovery keys to the Located UE. The network function initiating the check of UE privacy could be the network function responsible for generating and provisioning discovery keys. The method of UE privacy profile check specified for LCS in TS 23.273 [9] can be reused.

If the Located UE is already preconfigured with the privacy verification information from either the network via e.g. service authorization and information provisioning procedure or from the application layer, the Located UE checks its locally available privacy profile to determine whether it is discoverable or not in terms of privacy.



Figure 6.16.2-1: Privacy Check of the Located UE during the Discovery Procedure – Model A

Assuming the Located UE does not have locally available information to determine whether it is discoverable in terms of privacy:

1. The Located UE sends a Discovery Key Request to the DDNMF/PCF/PKMF, which includes at least the UE ID, SL positioning service code and the role the UE intends to play (i.e. Located UE).

2. The DDNMF/PCF/PKMF contacts the UDM to check whether the UE is authorized to act as a Located UE for the SL positioning service against its subscription information.

3. If the authorization is successful, the DDNMF/PCF/PKMF requests to retrieve UE privacy profile from the UDM via Nudm\_SDM\_Get request.

4. The UDM returns the privacy profile of the Located UE to the DDNMF/PCF/PKMF via Nudm\_SDM\_Get response.

5. The DDNMF/PCF/PKMF checks whether the Located UE allows its location information to be obtained by the network against the UE privacy profile.

6. Optionally, the DDNMF/PCF/PKMF notifies the UE via the AMF for privacy verification by the user, based on the privacy verification procedure defined in TS 23.273 [9].

NOTE 1: Details on privacy profile additions for Ranging/SL positioning need to be determined in coordination with SA2.

7a. If the privacy check is successful, the DDNMF/PCF/PKMF generates the discovery security materials for the UE and proceeds to step #8.

7b. If the privacy check fails, the DDNMF/PCF/PKMF returns a Discovery Key Response to the UE with a failure cause, and the Located UE aborts the discovery procedure.

Editor’s Note: LCS profile is supposed to be used by GMLC/NEF to check user authorization information to expose UE’s location towards a 3rd party (e.g. LCS client, AF). In this case, Located UE itself can determine whether or not it wants to be discoverable. It’s FFS why the Network needs to reject a discovery key request from the UE itself, who wants to be discoverable.

8. The DDNMF/PCF/PKMF returns a Discovery Key Response to the UE including the generated discovery security materials.

NOTE 2: There can be different levels of acceptable exposure for the located UE, e.g., some located UEs may accept sharing its location with the target UE, or some located UEs may only accept sharing its location with LMF. Thus, next to the discovery parameters, also a privacy policy may need to be configured in Target UE / Located UE. Details can be determined during normative work.

9. If model A is used for discovery, the Located UE starts to broadcast announcement message including its own UE info and the SL positioning service code. The message is protected using the received discovery security materials.

10. The Target UE monitors the broadcasted announcement messages. If the Located UE info in the announcement message matches the Located UE info provided by the LMF, the Target UE sends a Discovery Key Request to the DDNMF/PCF/PKMF, which includes at least the UE ID, SL positioning service code, the role the UE intends to play (i.e. Target UE) and the role of UE to discover (i.e. Located UE).

11. The DDNMF/PCF/PKMF interacts the UDM to authorize the role of the Target UE against its subscription information.

12. The DDNMF/PCF/PKMF returns a Discovery Key Response to the UE including the discovery security materials generated in step #7a.

13. Upon receiving the discovery security materials, the Target UE is able to verify the received announcement message.

14. The Target UE selects the Located UE by sending a Direct Communication Request (DCR) to the Located UE.

15. The Located UE returns a Direct Communication Accept (DCA) to the Target UE.

16. The rest of the SL positioning procedure is performed.

17. UE1 obtains the SL positioning result and sends it to the Client UE via PC5 link.

If model B is used for discovery, the Target UE broadcasts a solicitation message which contains the Located UE info provided by the LMF. The Located UE monitors the broadcasted solicitation message to find whether the message contains the Location UE info matching its own UE info. If there is a match, the Located UE verifies the solicitation message and sends a response message. When receiving a response from a Located UE, the Target UE selects the Located UE by sending a DCR message.



Figure 6.16.2-2: Privacy Check of the Located UE during the Discovery Procedure – Model B

### 6.16.3 Evaluation

This solution fulfils the first requirement in KI#1. It also addresses the Editor’s Note in clause 5.2.2 of TS 23.586 [11].

If the Located UE does not have locally available information to determine whether it is discoverable or not in terms of privacy, the privacy check is triggered by the PCF/DDNMF/PKMF when receiving discovery (key) request, which then interacts with the UDM, in the same way as the GMLC using the mechanism defined in TS 23.273 [9]. Only after successful privacy check of the Located UE, the PCF/DDNMF/PKMF will then generate discovery security materials for the Located UE.

Hence the main impact of the solution is on the network function generating discovery security materials, and the solution has no impact on the UE.

## 6.17 Solution #17: Client UE authorization for service exposure through 5GC network

### 6.17.1 Introduction

This solution addresses Key Issue #2 on Authorization for Ranging/Sidelink Positioning Service. Specifically, it addresses the fourth requirement in KI#2: “*The 5G Ranging/SL positioning system shall be able to support the authorization of a SL Positioning Client UE for triggering Ranging/Sidelink Positioning services and obtaining the location information*”. This solution also addresses Key Issue #1 on Privacy protection for Ranging/SL Positioning services.

Based on the introduction in clause 6.11.1, this solution introduces a method of finer level of authorization for preserving UE privacy before SL Positioning Client UE requests to obtain ranging result between two specific UEs through 5GC network.

### 6.17.2 Solution details

As per clause 5.6.2 of TS 23.586 [11], for Ranging/SL positioning service exposure to a SL Positioning Client UE through the network, the Client UE shall first send an enhanced MO-LR request to the AMF, which invokes a the Ranging/SL positioning request to the GMLC. The GMLC reuses the procedure as defined (for service exposure to the AF) in clause 5.6.3 of TS 23.586 [11] and sends the Ranging/SL positioning result to the AMF, which returns the result to the SL Positioning Client UE.

Based on the above procedure, it is proposed that the GMLC, which receives the Ranging/SL positioning request (containing Client UE info and the info of the to-be-measured UEs e.g. UE1/UE2), should initiate the authorization check of SL Positioning Client UE with the UDM, which has the Client UE’s subscription data for Ranging/SL positioning service containing e.g. the information on the UEs (e.g. UE1/UE2) from which the Client UE is allowed to request Ranging result.

After checking the Client UE’s authorization information, the GMLC also needs to check whether the to-be-measured UEs (UE1/UE2) allow their positions to be exposed. Only after successful authorization check on the Client UE and privacy check on the to-be-measured UEs, the Ranging/SL positioning procedure will then be initiated by the GMLC.



Figure 6.17.2-1: Authorization of SL Positioning Client UE for Service Exposure through 5GC Network

1. The Client UE triggers Ranging/SL Positioning Service by establishing a signalling connection with the AMF.

2. The UE sends an MO-LR Request message to the AMF included in a UL NAS TRANSPORT message. The MO-LR Request includes at least the info of Client UE and the to-be-measured UEs (UE1/UE2).

3. The AMF sends a Ranging/SL Positioning Request to the GMLC which also includes the info of Client UE and UE1/UE2.

4. The GMLC sends an Authorization Request to the UDM with the info of Client UE and UE1/UE2.

5. The UDM checks whether the Client UE is allowed to obtain the ranging/SL positioning information against the Client UE’s subscription data for SL positioning service, which could also contain the information on the to-be-measured UEs (UE1/UE2), from which the Client UE is allowed to request positions.

NOTE 1: The relevant subscription data could be configured offline in the UDM, or provided and updated in the UDM based on the requests from the AF offering Ranging/SL positioning services.

6. The UDM returns the authorization result to the GMLC.

7a~9a. If the authorization succeeds, the GMLC further checks whether UE1 and UE2 allow their location related information to be exposed, against the UE privacy profile in their subscription data.

NOTE 2: These steps can refer to solution #3 in clause 6.3.

7b/9b. If the authorization fails, the GMLC returns a Ranging/SL positioning response to the AMF with a failure cause.

10. Following step 9a, the rest of Ranging/SL positioning procedure is performed between the GMLC, AMF, LMF and UE1/UE2.

11. The GMLC sends the UE1/UE2 ranging/SL positioning result to the AMF.

10. The AMF sends the UE1/UE2 ranging/SL positioning result received from the GMLC to the Client UE.

### 6.17.3 Evaluation

This solution fulfils the fourth requirement in KI#2. It also addresses the Editor’s Note in clause 5.6.2.3 of TS 23.586 [11].

The authorization is triggered by the GMLC when receiving Ranging/SL positioning request, which then interacts with the UDM for checking UE subscription. The privacy check is also performed by the GMLC by reusing the mechanism defined in TS 23.273 [9].

The solution has no impact on the UE.

In MO-LR procedure defined in TS 23.273, it is specified that “The AMF verifies the subscription profile of the UE and decides if the requested service is allowed or not by checking the Mobile Originated data retrieved from UDM”, i.e. AMF is responsible for MO-LR authorization and retrieve subscription for MO-LR from UDM for UE authorization. Authorizing the MO-LR request from Client UE could be done similarly by AMF in step 2, instead of step 5 and 6. It is unclear whether the additional procedure performed by GMLC in this solution is aligned with existing SA2 baseline.

Also, configuring UDM with subscription data of the to-be-measured UEs (UE1/UE2), regarding authorization information about from which individual (Client)UEs are allowed to request positions of the to-be-measured UEs, is to be determined by SA2.

## 6.18 Solution #18: Client UE authorization by 5GC for service exposure through PC5

### 6.18.1 Introduction

This solution addresses Key Issue #2 on Authorization for Ranging/Sidelink Positioning Service. Specifically, it addresses the fourth requirement in KI#2: “*The 5G Ranging/SL positioning system shall be able to support the authorization of a SL Positioning Client UE for triggering Ranging/Sidelink Positioning services and obtaining the location information*”. This solution also addresses Key Issue #1 on Privacy protection for Ranging/SL Positioning services.

Based on the introduction in clause 6.11.1, this solution introduces another method of finer level of authorization for preserving UE privacy before SL Positioning Client UE obtains ranging result between two UEs. Rather than relying on the Ranging server for authorizing the Client UE in solution #11, this solution relies on the core network to authorize the Client UE by checking the subscription information of the Client UE and the privacy setting of the to-be-measured UEs.

### 6.18.2 Solution details

#### 6.18.2.1 General

As per clause 5.6.2.2 of TS 23.586 [11], for Ranging/SL positioning service exposure to a SL Positioning Client UE through PC5, the Client UE shall first discovers one of to-be-measured UE, and then invokes the Ranging/SL Positioning service request to the discovered UE for obtaining the Ranging/SL positioning result of the to-be-measured UEs. The request includes the info of the Client UE and the to-be-measured UEs. The UE providing the exposure service triggers the authorization of the Client UE for service invocation/exposure, based on which returns the Ranging/SL positioning result to the Client UE.

Based on the above procedure, it is proposed that the UE discovered by the Client UE should initiate the authorization check of the Client UE by sending an authorization request to the core network. The core network check with the UDM, which has the Client UE’s subscription data for Ranging/SL positioning service containing e.g. the information on the UEs (e.g. UE1/UE2) from which the Client UE is allowed to request Ranging result.

After checking the Client UE’s authorization information, the GMLC also needs to check whether the to-be-measured UEs (UE1/UE2) allow their positions to be exposed. Only after successful authorization check on the Client UE and privacy check on the to-be-measured UEs, the UE discovered by the Client UE will then proceed the subsequent procedures.

#### 6.18.2.1 Authorization of SL Positioning Client UE during direct link establishment

If the Client UE is not Ranging/SL positioning capable, it can only request and obtain Ranging/SL positioning result using PC5 messages. So when the Client UE sends the Direct Communication Request to the discovered UE, the DCR should include the service code of the requested Ranging/SL positioning service and the info of the to-be-measured UEs. In this case, the discovered UE (UE1) can initiate the Client UE authorization once receiving the DCR from the Client UE.



Figure 6.18.2-1: Authorization of the Client UE for Service Exposure through PC5 during PC5 Establishment

1~2. The Client and UE1 (one of the to-be-measured UEs) discover each other by broadcasting solicitation message, which includes at least the UE1 info and service code for the requested Ranging/SL positioning service, and response message respectively.

3. Upon receiving the response message from UE1, the Client UE performs PC5 link establishment procedure with UE1 by sending the Direct Communication Request (DCR) message. The message contains at least the Source info (Client UE info), the Service info (SL Positioning Service Code), and the to-be-measured UE info (UE1/UE2 info).

4. For authorizing the Client UE, UE1 sends an Authorization Request message to the AMF via NAS signalling upon receiving the DCR message. The request contains at least the Client UE info, the to-be-measured UEs info (UE1/UE2 info), and the SL Positioning Service Code.

5. The AMF sends a Ranging/SL Positioning Authorization Request to the GMLC which also includes the info of Client UE and UE1/UE2.

6. The GMLC sends an Authorization Request to the UDM with the info of Client UE and UE1/UE2.

7. The UDM checks whether the Client UE is allowed to obtain the Ranging/SL positioning result against the Client UE’s subscription data for SL positioning service, which could also contain the information on the to-be-measured UEs (UE1/UE2), from which the Client UE is allowed to request positions.

NOTE: The relevant subscription data could be configured offline in the UDM, or provided and updated in the UDM based on the requests from the AF offering Ranging/SL positioning services.

8. The UDM returns the authorization result to the GMLC.

9a~10. If the authorization succeeds, the GMLC further checks whether UE1 and UE2 allow their location related information to be exposed, against the UE privacy profile in their subscription info.

NOTE: These steps can refer to solution #3 in clause 6.3.

11. The GMLC returns an SL Positioning Authorization Response to the AMF.

12. The AMF forwards the authorization result to UE1 via NAS message.

13a. If the authorization is successful, UE1 performs a Direct Auth & Key Establish procedure with the Client UE. Then UE1 proceeds to step #14.

13b. If the authorization fails, UE1 sends a Direct Communication Reject message to the Client UE, which may contain the failure cause. Then the following steps do not need to be performed.

14~17. The rest of PC5 link establishment procedure and SL positioning procedure are performed.

#### 6.18.2.2 Authorization of SL Positioning Client UE during Ranging/SL positioning procedure

If the Client UE is Ranging/SL positioning capable, the authorization check of the Client UE may also be performed by UE1 when receiving a Ranging/SL positioning request message from the Client UE on RSPP/SLPP layer over the established PC5 link.



Figure 6.18.2-2: Authorization of the Client UE for Service Exposure through PC5 during Ranging/SL Positioning Procedure

Steps 1~2 can refer to steps 1~2 in 6.18.2.1.

3. PC5 link is securely established between the Client UE and UE1.

4. The Client UE sends a Ranging/SL positioning request to UE1 over RSPP/SLPP layer, which contains at least the Source info (Client UE info), the Service info (SL Positioning Service Code), as well as the to-be-measured UE info (UE1/UE2 info).

Steps 5~13 can refer to steps 4~12 in 6.18.2.1.

14~15. Upon successful authorization, UE1 performs the Ranging/SL positioning procedure with the other to-be-measured UE (i.e. UE2) and then returns the SL positioning result of UE1/UE2 to the Client UE over RSPP/SLPP layer.

### 6.18.3 Evaluation

This solution fulfils the fourth requirement in KI#2. It also addresses the Editor’s Note in clause 5.6.2.2 of TS 23.586 [11].

Authorization through the network during link establishment or during Ranging/SL positioning operations is a new requirement on the UE, but it has no impact on the procedures of link establishment and Ranging/SL positioning per se. The UE only needs to determine when to request authorization from the network in between the procedure.

The authorization is performed by the UDM against UE subscription. The privacy check is performed by the GMLC by reusing the mechanism defined in TS 23.273 [9]. The UE and the involved 5GC NFs only need to send the info of all involved UEs (Client UE and to-be-measured UEs) to the UDM.

The solution can accommodate different conditions with two options:

a) With Client UE not Ranging/SL positioning capable, the authorization can be performed during PC5 link establishment.

b) With Ranging/SL positioning capable Client UE, the authorization can be performed either during link establishment or during Ranging/SL positioning operations. On which stage the authorization should be performed for Ranging/SL positioning capable Client UE is to be determined during normative work.

## 6.19 Solution #19: Protecting Ranging/SL Positioning discovery out of network coverage

### 6.19.1 Introduction

The solution addresses Key Issue #3: Protection of discovery procedure, in particular, protects Ranging/SL Positioning discovery when UEs are out of network coverage.

In Ranging/SL Positioning services, there are use cases in which the UEs can be determined before using the Ranging/SL Positioning services, e.g., public safety, etc. By pre-provisioning shared root key materials for UEs that are to use Ranging/SL Positioning discovery services, UEs are able to discover each other when there is no network coverage. The shared root key materials may be pre-provisioned to the UEs via user settings at the application layer or pre-configured by the 3GPP network or Ranging/SL Positioning application server before the discovery procedure. Discovery request authorization is implicit, i.e., the UEs which are provided the shared root key materials are considered authorized UEs and can initiate discovery requests.

The UEs which want to discover others and also want to be discovered use the root key KRSLP to derive the discovery request MIC code, and this code is used to determine whether the discovery is matched or not as well as for integrity protection. In TS 33.503 Prose discovery security [6], the 5G network provides CURRENT\_TIME to ensure the UE’s local UTC time counter is close to true time to anti-replay attacks. The proposed solution uses a random-nonce-based challenge-response mechanism to anti-replay attacks, since it may be difficult to ensure the UE’s local time is not fooled when there is no 5G coverage. Furthermore, the root key can also be used for other purposes, such as Ranging/SL Positioning direct unicast communications.

The solution only works for ProSe-capable UEs.

### 6.19.2 Solution details



Figure 6.19.2-1: Ranging/SL Positioning discovery protection procedure when UEs are out of coverage

1. The UEs are pre-provisioned with a shared root key KRSLP and associated valid number of the root key usage times for the specific Ranging/SL Positioning service. The shared root key materials can be pre-provisioned to the UEs via user settings at the application layer or pre-configured by the 3GPP network or Ranging/SL Positioning application server before the discovery procedure. The Ranging/SL Positioning service is identified by Ranging/SL Positioning service code, which is assumed known to UEs prior to the discovery procedure. It can be understood as the real-time Restricted Code and Security Parameters generation process by 5G DDNMF/PKMF in TS 33.503 Security for 5G ProSe Discovery [6] are made as pre-provisioning in this solution.

Editor’s Note: Whether the network only pre-provisions the root key materials and the Ranging/SL Positioning service code or all of the discovery security materials (code, confidentiality & integrity key materials, etc.) are pre-provisioned from the network is FFS.

NOTE 1: If UEs will use more than Ranging/SL Positioning services when they are out of coverage, UEs are pre-provisioned with independent root keys for each Ranging/SL Positioning service. The root key associated with a specific Ranging/SL Positioning service can be identified by Ranging/SL Positioning service code.

NOTE 2: The root key KRSLP lifetime is implemented by the valid number of the root key usage times since trusted synchronous time may be not available. When the root key expires (i.e., the valid number of the root key usage times is exhausted), the root key shall be re-provisioned via certain methods which can be the same as the above-mentioned root key pre-provisioning methods.

1. UE A is a UE which wants to discover other UEs nearby and also wants to be discovered by other UEs. UE A first checks the valid number of the root key usage times is not exhausted. Then UE A chooses a random number nonce 1, and a specific ciphering algorithm. UE A derives Ranging/SL Positioning Discovery Confidentiality Key (RSLPDCK), Ranging/SL Positioning Discovery Integrity Key (RSLPDIK) using the shared root key KRSLP, Ranging/SL Positioning service code, and nonce 1, updates the valid number of the root key usage times as the current valid number of the root key usage times minus 1. UE A encrypts the Ranging/SL Positioning service code using the chosen ciphering algorithm and the RSLPDCK to avoid being tracked by unauthorized parties if UE A constantly sends the same cleartext Ranging/SL Positioning service code. UE A may optionally encrypt its role since the cleartext UE A role may also be considered as privacy. Then UE A generates discovery request message integrity check (DREQ MIC) code using RSLDIK, Ranging/SL Positioning service code, chosen ciphering algorithm identifier, UE A role, and nonce 1.

NOTE 3: How the RSLPDCK, RSLPDIK, and DREQ MIC code is calculated (e.g., using what ciphering algorithm) is left for normative work.

NOTE 4: UE A and UE B can be Reference UE, Target UE, and/or Located UE in the Ranging/SL Positioning service. The UE’s role may be determined by the application layer before the discovery procedures.

1. UE A broadcasts Discovery Request message, including Encrypted Ranging/SL Positioning service code, chosen ciphering algorithm, [Encrypted] UE A role, nonce 1, DREQ MIC code.
2. UE B is a UE in the proximity of UE A. UE B listens for the Discovery Request message, checks the valid number of the root key usage times is not exhausted, derives RSLDCK’and RSLDIK’ the same as which in step 1, and updates the valid number of the root key usage times as the valid number of the root key usage times minus 1. UE B decrypts the Ranging/SL Positioning service code and UE A role (if encrypted) using RSLDCK’. UE B checks the received DREQ MIC code according to RSLDIK’, the decrypted Ranging/SL Positioning service code, the received ciphering algorithm identifier, UE A role, and the received nonce 1. If checked, the Discovery Request message is pre-considered matched and goes to step 4, otherwise, disregards this Discovery Request and keeps listening to other Discovery Request messages.

Editor’s Note: How could UE B know what service UE A is discovering for is FFS if the Ranging/SL Positioning service code was encrypted.

1. UE B chooses a random number nonce 2, and sends Discovery Response message, including UE B role (encrypted using RSLDCK’ if needed), nonce 2, and Discovery Resp Message Integrity Check (DRESP MIC) code. The DRESP MIC is generated by RSLDIK’, the Ranging/SL Positioning service code, UE B role, nonce1, nonce2.

NOTE 5: How the DRESP MIC code is calculated is left for normative work.

1. UE A listens for the Discovery Response message. It checks the received DRESP MIC code according to RSLDIK’, the Ranging/SL Positioning service code, the decrypted (if it was encrypted) UE B role, nonce1, and the received nonce2. If checked, the Discovery Response message is considered fresh and integral, and goes to step 6, otherwise, disregards this Discovery Response and keeps listening to other Discovery Response.
2. UE A sends Discovery Freshness Proof message, including Discovery Freshness Proof Message Integrity Check (DFP MIC) Code. The DFP MIC code is generated by RSLDIK, the Ranging/SL Positioning service code, and the received nonce2.

NOTE 6: How the DFP MIC code is calculated is left for normative work. The DREQ MIC code, DRESP MIC code, and DFP MIC code shall be calculated with different input arguments to avoid replay attacks, e.g., replay DRESP MIC code as DFP MIC code in step 6.

1. UE B listens for Discovery Freshness Proof Message, and checks the received DFP MIC code according to RSLDIK’, the Ranging/SL Positioning service code, and the nonce2, if checked, the Discovery Request is considered fresh and matched, otherwise, disregards the Discovery Request and keeps listening to other Discovery Request.

### 6.19.3 Evaluation

TBD.

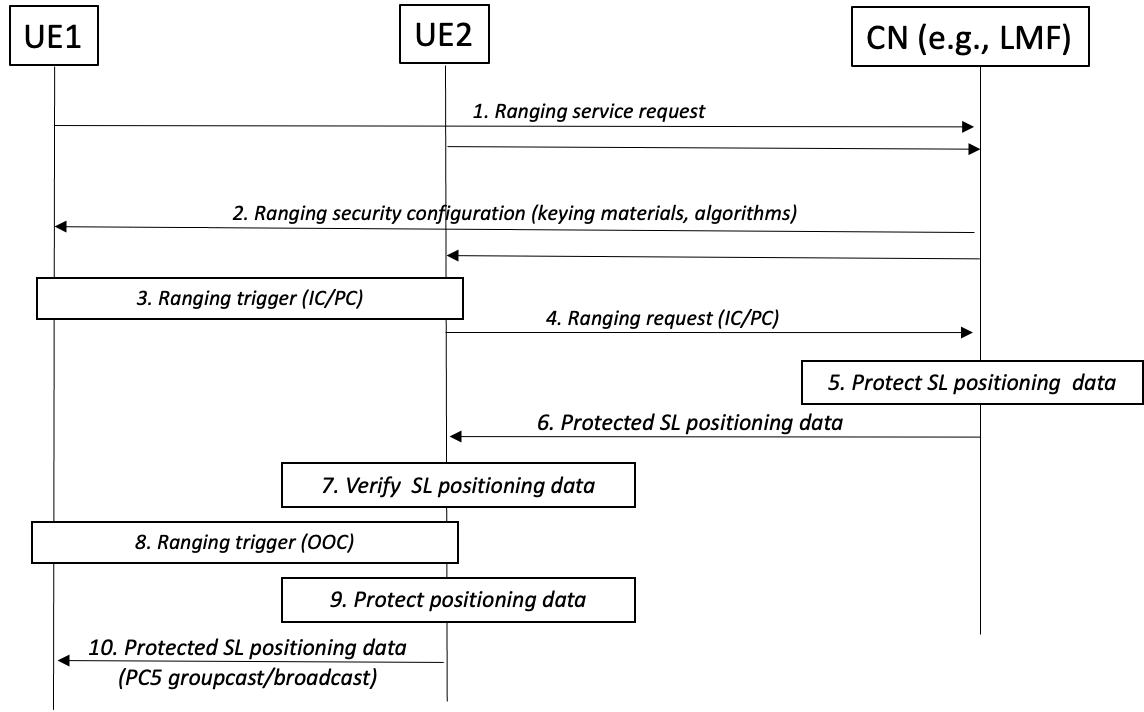
## 6.20 Solution #20: Secure groupcast/broadcast of SL positioning data

### 6.20.1 Introduction

This solution addresses KI#5.

This solution proposes to protect the groupcast/broadcast of SL positioning data, in particular, SL positioning capability and SL positioning assistance data, by adapting the communication flow and security mechanisms in TS 38.305 [12] (Clause 7.5) and TS 37.355 [13] (Clause 7.5) used for the protection of positioning assistance data.

### 6.20.2 Solution details



**Figure 6.20.2-1 Message flow for secure broadcast/groupcast**

The overall message flow proposed by this solution is as follows:

* Step 1: UE1 (and UE2) send a request to join a ranging service.
* Step 2: UE 1 (and UE2) are configured with the corresponding security information as applicable to the ranging service, if the UEs are authorized.

Editor’s Note: it is ffs which entity handles the keys, how UEs are identified and authorized by the CN, and how the ranging service request is protected.

* Step 3: UE 1 / UE 2 determine a ranging trigger that requires the distribution of SL ranging data when in in-coverage (IC) or partial coverage (PC).
* Step 4: UE2 sends a ranging request to retrieve SL positioning data.
* Step 5: CN, e.g., LMF, determines suitable SL positioning data, and protects it as in TS 37.355 [13].
* Step 6: Protected SL positioning data is transferred to UE2 in charge of local groupcast/broadcast.
* Step 7: Optionally, UE2 verifies received SL positioning data before broadcast/groupcast.
* Step 8: UE 1 / UE 2 determine a ranging trigger that requires the distribution of SL positioning data when out of 3GPP coverage.
* Step 9: Optionally, UE2 adds further protection (e.g., scrambling/integrity protection) to SL positioning data.
* Step 10: Protected SL positioning data is sent by means of groupcast/broadcast.

Editor’s Note: message fields required for data protection are left for ffs in normative phase.

In Step 2, UEs may be configured:

* with keys as in TS 37.355 [13] for confidentiality protection when Ues are IC/PC.
* with keys as in TS 37.355 [13] for usage when Ues are OOC. In this case, UE2 uses its key (e.g., as in step 9) for confidentiality protection of SL positioning data.
* With keys for the computation of a MIC that allows e.g., UE1 to verify SL positioning data transmitted in groupcast/broadcast.
* With keys for the scrambling of SL positioning data transmitted in groupcast/broadcast to prevent privacy threats.

If devices are out of 3GPP coverage, Steps 3-7 are not applicable. Instead, the UE (e.g., UE2) may implement the functionality of server UE thus replacing LMF functionality.

If devices are in-coverage / partial coverage, it is preferable to use Steps 3-7, although these steps may be skipped based on a policy/configuration.

Message in Step 6 may be securely transferred, e.g., as a NAS message.

Protection in Step 9 can be based on TS 37.355 [13] for confidentiality and may include further protection (e.g., integrity protection and/or scrambling protection).

NOTE: The choice of specific security algorithms/keys is left to normative phase.

Editor’s Note: further clarification about how the solution works in inter-PLMN use cases it is ffs.

### 6.20.3 Evaluation

TBD

## 6.21 Solution #21: Security of ranging/SL positioning groupcast communication

### 6.21.1 Introduction

This solution addresses the security requirement of KI #1 and protects the ranging/SL positioning groupcast communication. This solution reuses the existing security mechanism of one-to-many ProSe direct communication defined in clause 6.2 of TS 33.303 [14] along with some modification to set up the security of ranging/SL positioning groupcast communication.

### 6.21.2 Solution details

This solution reuses the existing security mechanism of one-to-many ProSe direct communication defined in clause 6.2 of TS 33.303 [14] along with some modification to set up the security of ranging/SL positioning groupcast communication.

The security for ranging/SL positioning establishment follows the procedure below:

* Configuration: The UE participating in the groupcast communication and the PKMF should be pre-configured with the group information for the ranging/SL positioning service, e.g., the Group Identity information including the Group Identity and Group member identity.
* The member UE and the PKMF should establish a security connection to transmit the key request message and key response message as specified in clause 5.2.5 of TS 33.503 [6]. The UE uses these messages to request keys for particular groups, while the PKMF uses these messages to provide the UE with its Group member identity and the security algorithms to use with the various groups. The Key Response message is used to transport the group security material from the PKMF to the UE, which contains PGK, identifier of the PGK, and the expiry time.

For roaming scenario, the PKMF in the HPLMN and VPLMN of the UE exchange the Key Request message and Key Response message to provision the member UE with the group security material.

* The sending UE should generate a PTK to further generate the PEK and PIK to protect the groupcast traffic between sending UE and receiving UE, the protection of traffic between UEs is specified in clause 6.2.3.6 of 33.303 [14].

The Group Identity and Group member identity are carried in the encrypted payload of PDCP packet, thus preventing the attacker to impersonate any UE in a specific group.

Editor’s Note: How to serve these UEs subscribed with different operators is FFS.

Editor’s Note: Whether PDCP for LTE ProSe one-to-many communication can be used for 5G-capable/V2X-capable UEs is FFS.

### 6.21.3 Evaluation

TBA.

## 6.22 Solution #22: Protection of broadcast Sidelink Positioning data in coverage scenario

### 6.22.1 Introduction

This solution addresses Key issue #5: Protection of groupcast/broadcast.

The solution proposes a procedure of provisioning broadcast protection keys to Target/Reference UEs when the UEs broadcast/receive Sidelink Positioning data in coverage scenario.

This solution proposes to reuse the broadcast protection key provision mechanism defined in clause 6.14.2 of TS 23.273 [9] for provisioning broadcast protection keys to the Target/Reference UEs when the UEs broadcast/receive Sidelink Positioning data in coverage scenario.

The key provision procedure is protected by the NAS security.

The Target/Reference UE needs to obtain the broadcast protection keys from its HPLMN's AMF and LMF. How to synchronize keys between different LMFs is not addressed by this solution.

### 6.22.2 Solution details

The broadcast protection key provision procedure is shown in the following figure.



Figure 6.22.2-1: Procedure of protecting broadcast Sidelink Positioning data in coverage scenario

1. The LMF invokes the Nlmf\_Broadcast\_CipheringKeyData Notify service operation towards the AMF carrying one or more SL Positioning broadcast Encryption Key (SPEK) and Integrity Key (SPIK), which are specified with key value, key identifier, validity period, a set of applicable tracking areas and a set of applicable types of SL positioning broadcast data.

NOTE 1: The LMF may send new ciphering and/or integrity keys (SPEK and/or SPIK) to the AMF at a time T1 if this will start to be used to cipher SL positioning broadcast data at a later time T2 (e.g. will replace a previous ciphering keys which expire at time T2). The value of (T2 - T1) should exceed the longest periodic registration timer of any UE subscribed to receive ciphering keys to ensure that periodic registration can be used to request new ciphering keys as described in NOTE 2.

Editor’s Note: What triggers the LMF to generate and send the ciphering key is FFS.

Editor’s Note: The assistant data broadcasted by the UE may not be from the LMF. The necessity of the LMF being involved in the security procedure is FFS.

2. The AMF stores the ciphering and/or integrity keys including the validity periods, applicable tracking areas and the types of applicable SL positioning broadcast data.

3. The Target/Reference UE sends a Registration Request to the AMF. The Registration Request may be sent as part of normal mobility management, A Registration Request may also be sent specifically to request and obtain SL positioning broadcast ciphering and/or integrity keys. The UE includes in the Registration Request an indication that SL positioning broadcast ciphering and/or integrity keys are requested. Other details of the Registration Request are as defined in TS 23.502 [15].

NOTE 2: A UE should request new SL positioning broadcast ciphering and/or integrity keys using a Registration Request caused by periodic registration if the remaining validity period for one or more SL positioning broadcast ciphering and/or integrity keys received earlier by the UE is less than the periodic registration timer value. This can help avoid all UEs initiating a Registration procedure at the same time to obtain new ciphering and/or integrity keys when a validity period for a ciphering and/or integrity key is about to expire. A UE should also request new ciphering and/or integrity keys for a Registration Request caused by entering a new tracking area if previous ciphering and/or integrity keys are not applicable to the new tracking area.

4. The AMF returns a Registration Accept to the Target UE. If the Target UE is subscribed to receive ciphered SL positioning broadcast data, the AMF includes in the Registration Accept one or more SL positioning broadcast ciphering and/or integrity keys applicable to the current tracking area for the UE. The AMF also includes for each ciphering and/or integrity key the ciphering key value, the ciphering key identifier, the validity period, the set of applicable tracking areas and the set of applicable types of SL positioning broadcast data.

NOTE 3: The AMF does not need to keep a record of SL positioning broadcast ciphering and/or integrity keys delivered to a UE and may instead send all SL positioning broadcast ciphering and/or integrity keys stored at step 2 that are applicable to the current tracking area, for which the UE has a subscription and whose validity period has not yet expired.

NOTE 4: A UE that receives no ciphering keys in response to a request for ciphering keys may assume that the UE does not have a subscription to receive ciphering keys in the serving PLMN.

5. The Reference UE sends the ciphered SL positioning broadcast data to the UE. The Target UE may start to use each SL positioning broadcast ciphering and/or integrity key to decipher SL positioning broadcast data once the validity period for the ciphering and/or integrity key has started and if the UE is currently in an applicable tracking area. The UE shall cease using a SL positioning broadcast ciphering and/or integrity key when entering a tracking area not applicable to the SL positioning broadcast ciphering and/or integrity key. The UE shall cease using and shall delete a SL positioning broadcast ciphering and/or integrity key when the validity period for the SL positioning broadcast ciphering and/or integrity key has expired.

How to protect the confidentiality and integrity of broadcast messages is out of the scope of this solution.

6. The AMF deletes all information for a SL positioning broadcast ciphering and/or integrity keys when the key validity period has expired.

Editor’s Note: With this solution, a UE only allowed to receive broadcast message can also send fake broadcast message. It is FFS how to prevent the receiving UE from sending fake broadcast messages.

### 6.22.3 Evaluation

This solution addresses the key issue #5.

This solution proposes to reuse the broadcast key provision mechanism defined in TS 23.273 [9] for provisioning broadcast protection keys to the Target/Reference UEs when the UEs broadcast/receive Sidelink Positioning data in coverage scenario.

This solution does not address how to use ciphering and/or integrity keys to protect broadcast messages. For message protection issue, other solutions in this TR can be considered.

Editor’s Note: Further evaluation is FFS.

## 6.23 Solution #23: Provisioning groupcast/broadcast protection key out of coverage

### 6.23.1 Introduction

This solution addresses Key issue #5: Protection of groupcast/broadcast.

The solution proposes a key provision mechanism that can securely provide groupcast/broadcast protection keys to Target/Reference UEs when they are out of coverage.

In this solution, the groupcast/broadcast protection keys are encapsulated in a key packet, and the Target/Reference UEs are provisioned with a symmetric key for decrypting the key packet, as well as a public key for verifying the signature of the key packet.

The Target/Reference UEs need to obtain the key packet decryption keys and signature verification keys when they are in coverage. The Server UEs need to obtain the key packets when they are in coverage. The Server UEs will distribute the key packets to the Target/Reference UEs when these UEs are out of coverage.

### 6.23.2 Solution details

The groupcast/broadcast protection key provision architecture is shown in the following figure.



Figure 6.23.2-1: Groupcast/broadcast protection key provision architecture in out of coverage scenario

The keys used to protect the groupcast/broadcast messages are generated by LMF or Key Management Function (KMF). The groupcast/broadcast protection keys are encrypted using the key packet encryption key, and then the key packet is signed using a private key by the LMF/KMF. The key packet encryption keys and signature verification public keys are pre-provisioned to Target/Reference UEs when they are in coverage. The encrypted and signed key packets are provisioned to Server UEs when they are in coverage. When Target/Reference/Server UEs are out of coverage, the Target/Reference UEs can download the encrypted and signed key packets from the Server UEs, and then use the signature verification key to verify the signature and then decrypt the encrypted groupcast/broadcast protection keys.

This mechanism can be used to provision broadcast protection keys (encryption protection keys and integrate protection keys) or groupcast protection keys (group keys).

The groupcast/broadcast protection key provision procedure is shown in the following figure.



Figure 6.23.2-2: Groupcast/broadcast protection key provision procedure in out of coverage scenario

0. In the cast where KMF is used to provide encrypted and signed groupcast/broadcast protection key packets, PCF can be used to provide the address of KMF to the Target/Reference/Server UEs.

In the case where AMF-LMF is used to provide encrypted and signed groupcast/broadcast protection key packets, this step is not required.

Editor's Note: Whether LMF can generate and provision the keys needs to be coordinated with SA2.

1. In the cast where KMF is used to provide encrypted and signed groupcast/broadcast protection key packets, the Target/Reference UE should establish a secure connection with the KMF when it is in coverage. The secure connection relies on Ua security if GBA specified in TS 33.220 [14] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [15] is used (see clause 5.2.5.4).

In the case where AMF-LMF is used to provide encrypted and signed groupcast/broadcast protection key packets, the data security is provided by the NAS security.

After secure connection is established, the UE sends key packet encryption key and verification key request to the AMF-LMF/KMF.

Editor's Note: The UE, while in coverage, is able obtain broadcast keys directly from the network or obtain encryption/public keys from the network proposed in this solution. Under which condition the UE should obtain encryption/public keys rather than broadcast keys is FFS.

2. The AMF-LMF/KMF checks whether the Target/Reference UE is authorized to receive key packet decryption key and key packet signature verification public key. If the UE is authorized, AMF-LMF/KMF returns a list of key packet decryption keys and a list of key packet signature verification public keys. Each decryption key or signature verification public key is associated with the key id and key validity time.

NOTE: In cases where UE comes from different PLMNs and AMF-LMF is used, key synchronization needs to be done between LMFs of different PLMNs. It is out of the scope of this solution.

3. Similar to the Target/Reference UE, the Server UE needs to establish a secure connection with the AMF-LMF/KMF, and then sends groupcast/broadcast protection key packet request to the AMF-LMF/KMF.

4. The AMF-LMF/KMF checks whether the Server UE is authorized to distribute the groupcast/broadcast protection key packets to Target/Reference UEs. If the UE is authorized, AMF-LMF/KMF returns a list of groupcast/broadcast protection key packets. Each key packet is associated with the packet id, packet validity time, packet decryption key id, packet signature verification public key id. The structure, encryption algorithm, and signature algorithm of the key packet are left to the normative phase stage.

Editor's Note: The risk of distributing the same key packet to different Server UEs is FFS.

5. The Target/Reference UE establishes a unicast communication with the Server UE using the security mechanism defined in clause 6.2 of TS 33.503 [3], and then sends a groupcast/broadcast protection key packet download request to the Server UE.

Editor's Note: The solution requires the Server UE to establish unicast links with both Target/Reference UE for distributing the key packet, while SL Positioning service does not require that the Server UE shall establish unicast links with both Target/Reference UE. How to ensure that the key packets can be distributed to both Target/Reference UEs is FFS.

6. The Server UE checks whether the Target/Reference UE is authorized to receive the groupcast/broadcast protection key packets. If the UE is authorized, the Server UE returns a list of applicable key packets to the Target/Reference UE. How the Target/Reference UE is authorized is not addressed in this solution.

7. The Target/Reference UE uses the public key indicated by the packet signature verification public key id to verify the signature of the key packet, and uses the decryption key indicated by the packet decryption key id to decrypt the key packet.

8. The Target/Reference UE uses the groupcast/broadcast protection keys to protect groupcast/broadcast messages. This solution does not specify how to use groupcast/broadcast protection keys to protect groupcast/broadcast messages.

Editor's Note: Whether this solution is applicable to V2X-capble UEs is FFS.

### 6.23.3 Evaluation

This solution addresses the key issue #5.

This solution proposes a key provision solution that can securely distribute groupcast/broadcast protection keys to Target/Reference UEs when they are out of coverage. The data packet that carries groupcast/broadcast protection keys is encrypted and signed by the key management function. The decryption keys and signature verification keys are securely provisioned to the UEs when they are in coverage. Therefore, only valid UEs can retrieve the groupcast/broadcast protection keys.

This solution does not provide a detailed data structure for the key packet, which is left to normative stage.

This solution does not address how to use the keys carried in the key packet to protect groupcast/broadcast messages. For message protection issue, other solutions in this TR can be considered.

Editor's Note: Further evaluation is FFS.

## 6.24 Solution #24: Protecting groupcast/broadcast messages

### 6.24.1 Introduction

This solution addresses Key issue #5: Protection of groupcast/broadcast.

This solution proposes key hierarchies and message formats for protecting groupcast and broadcast messages.

Editor's Note: Privacy of group ID and group member ID and group key ID is FFS.

Editor's Note: Setting MIC to zero when integrity is disabled is FFS.

### 6.24.2 Solution details

#### 6.24.2.1 Protecting groupcast message

##### 6.24.2.1.1 Groupcast security key hierarchy

The groupcast security key hierarchy is shown in the following figure.



Figure 6.24.2.1.1-1: Groupcast security key hierarchy

- Positioning Group Key (PGK): A key is provided by a KMF to a group member. This key is used to derive the PTK for a group member in the group.

- Positioning Traffic Key (PTK): This key is bound to a group member. The PTK is derived using the PGK based on Group ID, Group member ID, and Group key ID.

- Positioning Session Key (PSK): This key is generated by a group member using its PTK based on key generation time and a nonce. The key is used to generate PEK and PIK.

- Positioning Encryption Key (PEK): This key is generated using PSK and used for message encryption protection.

- Positioning Integrity Key (PIK): This key is generated using PSK and used for message integrity protection.

Editor's Note: Whether the PSK is necessary is FFS.

The detailed generation method for these keys will be determined in normative work. This solution does not specify how UE obtains PGK.

##### 6.24.2.1.2 Groupcast security

The format of SLPP message for Sidelink Positioning groupcast is shown in the following figure.



Figure 6.24.2.1.2-1: SLPP message format for Sidelink Positioning groupcast

The message sending UE performs the following operations:

- Construct the message as shown in figure 6.24.2.1.2-1.

- Selects a valid PGK stored locally, generate the PTK using the PGK based on Group ID, Group member ID and Group key ID, generate PSK using the PTK based on current time and a nonce, and generate PEK and PIK using the PSK.

- If message integrity protection is enabled, calculate MAC of the message, otherwise the MAC field will be filled with all zeroes. The integrity algorithms specified in Annex D in TS 33.501 [8] are used to calculate MAC.

- If message confidentiality protection is enabled, encrypt the Payload and MAC. The ciphering algorithms specified in Annex D in TS 33.501 [8] are used for the confidentiality protection.

The message receiving UE performs the following operations:

- Select a locally stored PGK using the Group key ID carried in the message, calculate PTK, PSK, PEK and PIK in the same way as sending UE based on the parameters carried in the message.

- If message confidentiality protection is enabled, decrypt the ciphertext.

- If message integrity protection is enabled, verify integrity protection by checking the MAC of the message.

#### 6.24.2.2 Protecting broadcast message

##### 6.24.2.2.1 Broadcast security key hierarchy

The broadcast security key hierarchy contains the following keys.

- Positioning Encryption Key (PEK): This key is used for message encryption protection. PEK is provided by a KMF.

- Positioning Integrity Key (PIK): This key is used for message integrity protection. PIK is provided by a KMF.

This solution does not specify how UE obtains PEK and PIK.

##### 6.24.2.2.2 Broadcast security

The format of SLPP message for Sidelink Positioning broadcast is shown in the following figure.



Figure 6.24.2.2.2-1: SLPP message format for Sidelink Positioning broadcast

The message sending UE performs the following operations:

- Construct the message as shown in figure 6.24.2.2.2-1.

-- If message integrity protection is enabled, calculate MAC of the message, otherwise the MAC field will be filled with all zeroes. The integrity algorithms specified in Annex D in TS 33.501 [8] are used to calculate MAC.

- If message confidentiality protection is enabled, encrypt the Payload and MAC. The ciphering algorithms specified in Annex D in TS 33.501 [8] are used for the confidentiality protection.

The message receiving UE performs the following operations:

- Use the PEK ID and PIK ID carried in the message to select the locally stored PEK and PIK.

- If message confidentiality protection is enabled, decrypt the ciphertext.

- If message integrity protection is enabled, verify integrity protection by checking the MAC of the message.

### 6.24.3 Evaluation

This solution addresses the key issue #5.

This solution proposes key hierarchies and message formats for protecting groupcast and broadcast messages.

This solution does not address how to provision PGK used in groupcast and PEK/PIK use in broadcast to UEs. For key provision issue, other solutions in this TR can be considered.

Editor's Note: Further evaluation is FFS.

## 6.25 Solution #25: Protection for groupcast of SLPP signalling

### 6.25.1 Introduction

This solution addresses Key Issue #5 on Protection of groupcast/broadcast and Key Issue #1 on Privacy protection for Ranging/SL Positioning services. Specifically, it addresses the first requirement in KI#5 and the second requirement in KI#1.

### 6.25.2 Solution details

#### 6.25.2.1 General

For a group of UEs, when one of the UEs needs to groupcast SLPP signaling and the rest of the group need to receive SLPP signaling, they are normally groupcasting and receiving for the same Ranging/SL positioning Service. Otherwise, the SLPP signaling (e.g. positioning assistant information) groupcasted for service A may not be of any use for the receiving UE of service B, and the information of the groupcasting UE of service A will be unnecessarily exposed to the receiving UE of service B, which leads to privacy issue. In addition, as per TS 23.586 [11], group management can be performed at application layer, which may provide group identifier information to the Ranging/SL Positioning layer. Hence, it is expected that SLPP signaling groupcast is associated with a specific Ranging/SL positioning service. To enable groupcast protection per group and per Ranging/SL positioning service, it is proposed to associate the groupcast keys with group ID (indicating the specific group) and Ranging/SL positioning service code (RSSC) (indicating the specific Ranging/SL positioning service).

To set up unicast communication for exchanging SLPP signaling between a pair of UEs, discovery messages are broadcasted/groupcasted by the UE and the security of discovery messages are protected with discovery security materials provided by the network. For a groupcast capable UE, it should be able to groupcast SLPP signaling without having to establish unicast connection hence no need of performing discovery. Still, the procedure of provisioning discovery security materials can be adapted to provisioning security keys for SLPP groupcast protection.

Furthermore, it is mostly possible that the two or more UEs involved in a Ranging/SL positioning service may not be subscribed with the same operator. Thus, it is proposed that the 5GC NF serving the groupcasting UE (in one PLMN) generates the groupcast keys, and the 5GC NF serving the receiving UE (probably in another PLMN) obtains the groupcast keys from the generating 5GC NF. The 5GC NF of the receiving UE finds the 5GC NF of the groupcasting UE based on the groupcasting UE info (containing the PLMN ID of the groupcasting UE).

The groupcast keys obtained by the group members could be symmetric or asymmetric keys. To prevent one receiver in a group from impersonating the groupcaster in the group, asymmetric key pairs can be created for SLPP signaling groupcast, of which the private key is provisioned to the groupcaster and the public key is provisioned to the receiver.

#### 6.25.2.2 Key provisioning for SLPP signalling groupcast



Figure 6.25.2-1: Key Provisioning for SLPP Groupcast Protection

It is assumed that the UEs in a group are all provisioned with a Group ID allocated by the Ranging/SL positioning application and the Group ID contains the service identifier of a specific Ranging/SL positioning service.

1. The UE intending to groupcast SLPP signaling (G-UE) sends a Key Request message to its PKMF/DDNMF/PCF. The message includes at least the Group ID, G-UE info, an indicator of the UE as a groupcaster.

2~4. The PKMF/DDNMF/PCF of G-UE checks with the Ranging/SL Positioning Server on whether G-UE is allowed to perform SLPP signaling groupcast for the Group of the Ranging/SL Positioning service indicated by the Group ID.

5. The PKMF/DDNMF/PCF of G-UE generates the groupcast keys by associating the keys with the Group ID (so that groupcast keys of one group cannot be used by another group). A groupcast key identifier (GKID) is also generated to identify the keys. The PKMF/DDNMF/PCF of G-UE stores the groupcast keys associated with the Group ID. The groupcast keys could be symmetric or asymmetric key pairs (Private/Public keys), of which the Private key is sent to the groupcaster and the Public key is sent to the receivers.

6. The PKMF/DDNMF/PCF of G-UE responds to G-UE with the groupcast keys (e.g. Private key) and GKID.

7. The UE intending to receive the groupcast SLPP signaling (R-UE) sends a Key Request message to its PKMF/DDNMF/PCF. The message includes at least the Group ID, R-UE info, an indicator of the UE as a receiver.

8~10. The PKMF/DDNMF/PCF of R-UE checks with the Ranging/SL Positioning Server on whether R-UE is allowed to receive groupcasted SLPP signaling for the Group of the Ranging/SL Positioning service indicated by the Group ID. In addition to the Authorization Result, the Ranging/SL Positioning Server also provides the G-UE info of the Group to the PKMF/DDNMF/PCF of R-UE.

11. If the authorization succeeds, the PKMF/DDNMF/PCF of R-UE sends a Key Request to the PKMF/DDNMF/PCF of G-UE. If the G-UE and R-UE are served by the same PKMF/DDNMF/PCF, this step can be skipped. If the G-UE and R-UE are served by different PKMFs/DDNMFs/PCFs, the PKMF/DDNMF/PCF of R-UE finds the PKMF/DDNMF/PCF of G-UE based on the G-UE info (containing PLMN ID of G-UE). The Key Request contains at least the Group ID, R-UE info, the indicator of the UE as a receiver.

12~14. Optionally, the PKMF/DDNMF/PCF of G-UE may check with the Ranging/SL Positioning Server on whether G-UE and R-UE are matching for groupcasting and receiving SLPP signaling for the Group. The request contains at least the Group ID, G-UE info and R-UE info.

15. If the check with the Ranging/SL Positioning Server succeeds, the PKMF/DDNMF/PCF of G-UE responds to the PKMF/DDNMF/PCF of R-UE with the groupcast keys (e.g. Public key) and GKID. If the G-UE and R-UE are served by the same PKMF/DDNMF/PCF, this step can be skipped.

16. The PKMF/DDNMF/PCF of R-UE provides the groupcast keys (e.g. Public key) and GKID to R-UE.

17. G-UE starts to groupcast SLPP signaling which is protected by the group keys (e.g. Private key) received from the network. The groupcast message includes at least the Group ID, GKID, SLPP signaling.

18. R-UE starts to monitor the groupcast messages. When receiving the groupcasted signaling from G-UE, R-UE retrieves the groupcast keys using the received GKID and verifies the groupcasted message using the groupcast keys (e.g. Public key).

#### 6.25.2.3 SLPP signaling protection and verification

For protecting the groupcast message, G-UE does the following steps:

1. Form SLPP message: SLPP header (incl. GKID) and SLPP payload (SLPP signaling).

2. Encrypt SLPP payload (SLPP signaling) using the group key (encryption key).

3. Calculate the MAC of SLPP message (GKID+SLPP signaling) using the group key (integrity key).

4. Form L2 message by including the protected SLPP message (SLPP message + MAC) as the L2 payload and append the L2 header (incl. Destination/Group ID).



Figure 6.25.2-2: Exemplar Format of Protected SLPP Message

For receiving and verifying the protected groupcast message, R-UE does the following steps:

1. Receive the groupcast message for the expected group by identifying the L2 Destination/Group ID, which is mapped from the Group ID allocated by the application layer.

2. Retrieve the groupcast keys for verification by identify the GKID in the received message.

3. Verify the message by checking the MAC of the received message using the groupcast key (integrity key). This is to ensure that the GKID and SLPP signaling are not tampered during groupcasting.

4. Decrypt the encrypted SLPP payload using the groupcast key (encryption key).

NOTE 1: It is possible that L2 Destination/Group ID may be tampered because the UE cannot protect L2 header which is below PDCP layer. But even if L2 Destination/Group ID is tampered by an attacker, R-UE is able to detect the attack because the integrity protected GKID is associated with Group ID. When R-UE detects that the Group ID associated with GKID is not identical to the Group ID mapped from the L2 Destination ID, R-UE will drop the received message.

NOTE 2: If the groupcast keys are symmetric keys (groupcaster and receivers in a group sharing the same keys), there is the risk that a receiver in a group can impersonate the groupcaster in the group. If the groupcast keys are asymmetric keys (groupcaster holding private key and receiver holding public key), it is not possible for a receiver in a group to impersonate the groupcast in the group. Therefore, it is recommended to generate asymmetric keys for SLPP signaling groupcast.

### 6.25.3 Evaluation

This solution fulfils the first requirement in KI#5.

The solution largely reuses the mechanism of discovery key provisioning defined in TS 33.503 [6] for provisioning groupcast keys. Such solution ensures that:

- The multiple UEs involved in a group of Ranging/SL positioning service but subscribed with different operators are provisioned with the same set of groupcast keys generated by a single network function.

- The groupcasters and receivers are authorized per role by the network before obtaining the groupcast keys.

- The receivers are able to detect whether the unprotected L2 header (containing L2 Destination/Group ID) of the received groupcast message is tampered or not, based on the integrity protected GKID.

- A receiver in a group cannot impersonate the groupcast in the group if asymmetric keys are generated for SLPP signaling groupcast.

## 6.26 Solution #26: Protection of SLPP broadcast based on central key management function

### 6.26.1 Introduction

This solution addresses Key Issue #5 on Protection of groupcast/broadcast and Key Issue #1 on Privacy protection for Ranging/SL Positioning services. Specifically, it addresses the second requirement in KI#5 and the second requirement in KI#1.

### 6.26.2 Solution details

#### 6.26.2.1 General

According to RAN2, SLPP signalling broadcast could be service independent, e.g. SLPP signalling broadcasted by a UE can be received and used by other UEs in different Ranging/SL positioning services. The UEs do not need to perform discovery procedure and link establishment procedure for broadcasting and/or receiving SLPP signalling. Hence it is proposed to provision the broadcast keys to the UE as earlier as in Registration procedure.

To support SLPP signaling broadcast, it is assumed that the information on whether a Ranging/SL positioning capable UE is allowed to broadcast and/or receive SLPP signaling or not is included in the UE subscription. Based on such information in the subscription and UE’s capability, the core network can then determine whether broadcast keys need to be provisioned to the UE when it is registering to the network.

For Ranging/SL positioning services, it is mostly possible that the broadcasting and receiving UEs may not be subscribed with the same operator. If the involved UEs are subscribed with different operators, it would not be possible for the 5GC NF in one PLMN to create the same broadcast keys for all involved UEs belonging to different PLMNs during Registration. Therefore, it is proposed to use a centralized key management function which could be connected with different PLMNs for creating and providing the broadcast keys to the 5GC NFs in different PLMNs. The 5GC NF then provisions the broadcast keys to the UEs in its own PLMN.

The 5GC NF provisioning the broadcast keys could be the PCF which sends the keys to the UE as part of UE security policy configuration information; or could be the LMF which sends the keys to the UE using the existing procedure defined in clause 6.14.2 of TS 23.273 [9]. If the deployment of SLPP signalling broadcast requires that receiving UEs should be subscribed in the same PLMN of the broadcasting UE, the centralized key management function can be collocated with the PCF or the LMF.

#### 6.26.2.2 Key provisioning via the PCF



Figure 6.26.2-1: Key Provisioning via the PCF for SLPP Broadcast Protection

1. The UE intending to broadcast SLPP signaling (B-UE) sends a (Periodic) Registration Request message to its AMF, which contains B-UE ID and an indicator of Requesting Broadcast Keys.

2. The AMF of B-UE checks with the UDM whether B-UE is allowed to broadcast SLPP signaling against the UE subscription information.

3. If B-UE is allowed to broadcast SLPP signaling, the AMF of B-UE sends e.g. a UE Policy Create Request to the PCF of B-UE with the indicator of Requesting Broadcast Keys for Broadcaster.

4. The PCF of B-UE sends a Key Request to the Central Key Management Function to request keys for broadcasting SLPP signaling.

5. The Central Key Management Function generates the keys for broadcasting SLPP signaling. The broadcast keys could be e.g. a pair of asymmetric private/public keys or a pair of symmetric integrity and encryption keys.

6. The Central Key Management Function returns the broadcast keys (e.g. the private key) in the Key Response to the PCF of B-UE.

7. The PCF of B-UE returns the broadcast keys to the AMF of B-UE in e.g. the UE Policy Create Response.

8. The AMF of B-UE sends the broadcast keys to B-UE in the Registration Accept.

9. The UE intending to receive the broadcast SL positioning signaling (R-UE) sends a (Periodic) Registration Request message to its AMF, which contains R-UE ID and an indicator of Requesting Broadcast Keys.

10. The AMF of R-UE checks with the UDM whether R-UE is allowed to receive broadcasted SLPP signaling against the UE subscription information.

11. If R-UE is allowed to receive broadcasted SLPP signaling, the AMF of R-UE sends e.g. a UE Policy Create Request to the PCF of R-UE with the indicator of Requesting Broadcast Keys for Receiver.

12. The PCF of R-UE sends a Key Request to the Central Key Management Function to request keys for receiving broadcasted SLPP signaling.

13. The Central Key Management Function returns the keys for receiving broadcasted SLPP signaling in the Key Response to the PCF of R-UE. The keys could be e.g. the public key of the asymmetric private/public keys created in step #5.

14. The PCF of R-UE returns the keys for receiving broadcasted SLPP signaling to the AMF of R-UE in e.g. the UE Policy Create Response.

15. The AMF of R-UE sends the keys for receiving broadcasted SLPP signaling to R-UE in the Registration Accept.

16. B-UE starts to broadcast positioning signaling which is protected by the broadcast keys received from the network.

17. R-UE starts to monitor the broadcasted messages. When receiving the broadcast signaling from B-UE, R-UE verifies the broadcast message with the keys received from the network.

NOTE: Each of the keys is assigned with a validity timer. When the timer expires, the UE needs to request new keys by initiating a periodic registration procedure again.

#### 6.26.2.3 Key provisioning via the LMF

The 5GC NF provisioning the broadcast keys to the UE could also be the LMF for reusing the existing procedure of Ciphering Keys Delivery for Broadcast Assistance Data defined in clause 6.14.2 of TS 23.273 [9]. The LMF is used when the broadcasting UE needs to acquire positioning assistant data from the core network. In this case, the UE sends a request to the AMF, which selects a LMF for invoking network assistant data transfer. Before the LMF starts to deliver the network assistant data, it needs to obtain the broadcast keys for protecting the network assistant data.



Figure 6.26.2-2: Key Provisioning via the LMF for SLPP Broadcast Protection

1. Upon receiving the request for network assistant data delivery, the LMF of B-UE sends a key request to the Central Key Management Function to request keys for the UE to broadcast SLPP signaling.

2. The Central Key Management Function returns the broadcast keys for SLPP signaling to the LMF of B-UE.

3. The LMF of B-UE invokes the Nlmf\_Broadcast\_CipheringKeyData Notify service operation towards the AMF of B-UE containing the received security keys for SLPP signaling broadcast.

4. The AMF of B-UE stores the broadcast keys received from the LMF of B-UE.

5. B-UE intending to broadcast SLPP signaling sends a (Periodic) Registration Request message to its AMF, which contains B-UE ID and an indicator of Requesting Broadcast Keys.

6. The AMF of B-UE checks with the UDM whether B-UE is allowed to broadcast SLPP signaling against the UE subscription information.

7. The AMF of B-UE sends the stored broadcast keys to B-UE in the Registration Accept.

8. As in step #1, the LMF of R-UE sends a key request to the Central Key Management Function to request broadcast keys for the UE to receive broadcasted SLPP signaling.

9. The Central Key Management Function returns the broadcast keys for receiving broadcasted SLPP signaling to the LMF of R-UE.

10. The LMF of R-UE invokes the Nlmf\_Broadcast\_CipheringKeyData Notify service operation towards the AMF of R-UE containing the received broadcast keys.

11. The AMF of R-UE stores the broadcast keys received from the LMF of R-UE.

12. R-UE intending to receive broadcasted SLPP signaling sends a (Periodic) Registration Request message to its AMF, which contains R-UE ID and an indicator of Requesting Broadcast Keys.

13. The AMF of R-UE checks with the UDM whether R-UE is allowed to receive broadcasted SLPP signaling against the UE subscription information.

14. The AMF of R-UE sends the stored broadcast keys to R-UE in the Registration Accept.

15. B-UE starts to broadcast positioning signaling which is protected by the broadcast keys received from the network.

16. R-UE start to monitor the broadcasted messages. When receiving the broadcast signaling from B-UE, R-UE verifies the broadcast message with the broadcast keys received from the network.

NOTE: In case that the LMF requests broadcast keys from the Central Key Management Function, only symmetric keys can be generated, because the LMF does not know whether the requesting UE intends to broadcast or receive SLPP signaling when sending registration request.

### 6.26.3 Evaluation

This solution fulfils the second requirement in KI#5.

The broadcast keys are generated and provisioned by a Centralized Key Management Function during Registration procedure. Such solution ensures that:

- The UE does not need to be specifically triggered to request broadcast keys.

- The broadcasting and receiving UEs subscribed with different operators can be provisioned with the same set of broadcast keys generated by a single network function.

- The broadcasters and receivers are authorized per role by the network before obtaining the broadcast keys.

- The existing procedure of Ciphering Keys Delivery for Broadcast Assistance Data defined in clause 6.14.2 of TS 23.273 [9] can be partially reused, when the broadcaster needs positioning assistant data from the LMF.

## 6.27 Solution #27: Protection of broadcast communication

### 6.27.1 Introduction

This solution solves key issue # 5 “Protection of groupcast/broadcast”. In order to meet the requirements of KI #5, this solution provides a secure Sidelink Positioning broadcast procedure that fulfills confidentiality, integrity, and replay protection for the location information. This solution is summarized into four phases:

1) The broadcast key request phase of the sending UE-1. The sending UE-1 initiates an SL broadcast key request. After authorization, the corresponding Sidelink Positioning Key Management Function (SLPKMF) selects the Sidelink Positioning Broadcast Key (SLPBK), Sidelink Positioning Secret Key (SLPSK), Sidelink Positioning Public Key (SLPPK), SLPBK-ID, and responds the keys to the UE-1.

2) The broadcast phase of the sending UE-1. The sending UE-1 broadcasts protected positioning signaling, the SLPBK-ID, and a token associated with this broadcast message. The token is used to enable the receiving UE-x to verify whether the sending UE-1 does have permission to broadcast, preventing UEs that have obtained SLPBK from impersonating UE-1. In broadcast communications, all the UEs subscribed to the same Sidelink Positioning Services in the proximity of UE-1 have permission to receive and decrypt broadcasted positioning signaling, but whether a UE can broadcast positioning signaling should be authorized. Since SLPBK is the key protects broadcast message, all the subscribed UEs in the proximity of UE-1 will obtain SLPBK from 5GC to undo the protection of the broadcast message. These UEs may impersonate UE-1 to send broadcast message.

3) The key retrieval phase of the receiving UE-x. The receiving UE-x sends an SL broadcast key retrieval request to the corresponding SLPKMF. The SLPKMF of UE-x determines whether the sending UE-1 and receiving UE-x are with the same HPLMN. If they are with the same HPLMN, the SLPKMF of UE-x directly returns a key retrieval response to the UE-x; Otherwise, the SLPKMF of UE-x establishes a secure connection with the SLPKMF of UE-1 to obtain the broadcast key, and then returns a key retrieval response to the UE-x.

4) The decryption phase of the receiving UE-x. The receiving UE-x verifies the token and decrypts the broadcast message.

The solution assumes the receiving UEs are in coverage.

### 6.27.2 Solution details



Figure 6.27.2-1: protection of broadcast information between UEs

Step 1-6：The broadcast key request phase of the sending UE-1.

1. The sending UE-1 wants to send broadcast message, it prepares positioning signaling (e.g., SL positioning assistance data/SL positioning capability) and perhaps other broadcast data in advance.
2. The UE-1 sends SL broadcast key request messages to the serving SLPKMF of UE-1, including the UE-1-ID, the Sidelink Application identifier (SLAPP-ID), and the SL security capabilities.

NOTE 1: The SLPKMF may be an existing key management NF in 5GC, such as Prose PKMF. Therefore, the communications between UE and SLPKMF are assumed secure.

1. The UE-1’s serving SLPKMF sends SL broadcast authorization request to the ranging/SL application server to authorize UE-1’s broadcast request, including UE-1-ID.
2. The ranging/SL application server authorizes the request based on UE-1's subscription. If the authorization is successful, continue with step 4, otherwise reject the SL authorization request.
3. The ranging/SL application server provides the SL authorization response to the serving SLPKMF of UE-1.
4. The serving SLPKMF of UE-1 selects the Sidelink Positioning Broadcast Key (SLPBK) and corresponding key identifier (SLPBK-ID), as well as a key pair: Sidelink Positioning Secret Key (SLPSK) and Sidelink Positioning Public Key (SLPPK) for UE-1. In addition, the serving SLPKMF of UE-1 sets an expiration time for the broadcast key materials. Once SLPBK, SLPSK and SLPPK expire, the SLPKMFs and UEs delete the broadcast keys SLPBK, SLPSK and SLPPK.
5. The serving SLPKMF of UE-1 returns a broadcast key response to UE-1, including SLPBK, SLPBK-ID, SLPSK of UE-1, and expiration time.

Step 7：The broadcast phase of the sending UE-1.

1. The sending UE-1 encrypts the UE-1-ID and SL positioning assistance data /SL positioning capability using SLPBK. In addition, the UE-1 generates a token using SLPSK, then sends broadcast message, including SLPBK-ID, token, encrypted UE-1-ID and protected broadcast data (i.e., the positioning signaling).

NOTE 2: whether UE-1-ID and other information encrypted are separate may be implementation-specific, for example, it may depend on whether the encryption algorithms support the decryption of partial ciphertext.

Editor’s Note: how to encrypt and integrity protect the broadcast message is FFS.

Step 8-13：The key retrieval phase of the receiving UE x.

1. If the the receiving UE-x doesn’t have the SLPBK associated with the received SLPBK-ID or the UE-x has the SLPBK but after decrypts the UE-1-ID, the UE-x find it has no SLPPK of the UE-1, the UE-x sends an SL broadcast key retrieval request to its serving SLPKMF. The SL broadcast key retrieval request message includes UE-x-ID, SLPBK-ID, and encrypted UE-1-ID. If the receiving UE-x has both SLPBK associated with the received SLPBK-ID and SLPPK of the sending UE-1, skip the steps 8~13.

NOTE 3: the SLPBK-ID contains UE-1’s HPLMN ID and necessary routing information to enable UE-x’s serving SLPKMF can route to UE-1’s serving SLPKMF.

1. The serving SLPKMF of UE-x determines whether the sending UE-1 and receiving UE-x are with the same HPLMN based on SLPBK-ID. If they are with the same HPLMN, skip steps 10~12. Otherwise, the serving SLPKMF of UE-x should send a key query request to the serving SLPKMF of UE-1 based on SLPBK-ID.
2. The serving SLPKMF of UE-x sends a key query request to the serving SLPKMF of UE-1, with SLPBK-ID and encrypted UE-1-ID.
3. The serving SLPKMF of UE-1 checks whether to return the key based on local policy. If checked, go to step 12.
4. The serving SLPKMF of UE-1 decrypts the encrypted UE-1-ID, determines SLPPK of UE-1 choosed in step 5. The serving SLPKMF of UE-1 returns the key query response to the serving SLPKMF of UE-x, including SLPBK, UE-1's SLPPK, SLAPP-ID, and key expiration time.
5. The serving SLPKMF of UE-x identifies the SL positioning service and the corresponding ranging/SL application server according to the received SLAPP-ID. It sends SL broadcast receiving authorization request which includes UE-x-ID to the ranging/SL application server to authorize UE-x to receive broadcast messages.
6. The ranging/SL application server authorizes the request based on UE-x's subscription. If the authorization is successful, continue with step 15, otherwise reject the SL broadcast receiving authorization request.
7. The ranging/SL application server provides the SL broadcast receiving authorization response to the serving SLPKMF of UE-x.
8. The serving SLPKMF of UE-x sends a key retrieval response to the UE-x, including SLPBK, SLPPKUE-1, key expiration time.

Editor’s Note: whether it is feasible to provide every public keys of potential senders to all participating UEs is FFS.

Step14：The decryption stage of the receiving UE-x.

1. The receiving UE-x verifies the token using SLPPKUE-1. If the verification is successful, the UE-x decrypt the broadcast message using the SLPBK. Otherwise, the UE-x disregards the broadcast message.

Editor’s Note: whether token based authorization is needed is FFS.

NOTE 4: After the above procedures, the UE-x will also get an SLPBK, if now the UE-x wants to send broadcast message and the SLPBK is unexpired, steps 1-14 still need to be carried out for the UE-x. But to avoid the UEs’ key management overhead, in step 5, the serving SLPKMF of the UE-x may decide directly choose the above SLPBK and associated SLPBK-ID for the UE-x to protect its broadcast message, and only choose a new key pair (SLPSKUE-x, SLPPKUE-x) for the UE-x. The serving SLPKMF of the UE-x can realize the UE-x has already got an SLPBK for a specific SLAPP (the step 12 above contains SLAPP-ID).

### 6.27.3 Solution Evaluation

TBD.

## 6.28 Solution #28: Protection of broadcast communication

### 6.28.1 Introduction

This solution addresses KI#5 “Protection of groupcast/broadcast”.

The solution is based on the nature of broadcast messaging that the initiator UE broadcasts the message unprotected so that all potentially responding UEs can process it. The sensitive information is resulting in the SL Ranging/Positioning procedure and sent from the responding UEs to the initiator UE. Therefore, the responding UEs are grouped to an temporary Ad-Hoc Group only for the time of the procedure, the communication is protected with an assigned group key so that UEs not involved in the communication are not able to access the sensitive information of the ranging/positioning procedure.

### 6.28.2 Solution details

The requirement on the communication protection is on the responses from the participating UEs of the ranging/positioning action, since the SL positioning capability, SL positioning assistance data and Location information should not be leaked to other UEs not participating in the SLPP procedure. Therefore the UEs responding to the broadcast request from an Initiator UE will form an ad-hoc temporary group only for the requested action, which will be protected with a group key. All UEs participating in the procedure are assumed to be registered successfully in the network.



Figure 6.28.2-1: Ad-Hoc Group creation for Broadcast SL Positioning

1. UE1 wants to initiate SL broadcast authorization request and sends a broadcast authorization request message to the SL Positioning Key Management Function (SLPKMF) including its UE Identity (UE ID) and the Zone ID where it is located. The Zone ID is defined by RAN2 as indicator of UE1’s coarse location information. The message is protected by the NAS protocol.

2. The SLPKMF sends an Authorization Request of the UE1 for broadcast requests to the Ranging Server function including the UE1 ID and its Zone ID.

3. The Ranging Application Server authorizes the request e.g. based on the UE1 subscription and stores the Zone ID corresponding to the UE1.

4. The Ranging Application Server provides the authorization result to the SLPKMF.

5. The SLPKMF assigns a temporary group ID and Option A: generates a group broadcast key KB for the broadcast communication. The SLPKMF sets a validity time for the broadcast procedure, i.e. UEs responding to the broadcast request of UE1 in step 7 have to respond within the validity time, further the group broadcast key KB in the participating UEs should be removed after expiration of the validity time. The validity time should be therefore set carefully to allow the procedure to complete.

Editor’s Note: the need of Ad-Hoc Group for broadcast is FFS

6. The SLPKMF provides the group ID, Group Broadcast Key KB and validity time to the UE1 in the broadcast authorization response message. UE1 deletes the Group Broadcast Key KB after expiration of the validity time. The message is protected by the NAS protocol.

7. The UE1 sends a SL broadcast message with a requested positioning/ranging action, the UE1 ID and the temporary group ID.

Editor’s Note: the broadcast messages in step7 are not protected. Security and privacy threats of unprotected broadcast message is FFS

8. UE2, UE3, UE4 receive the SL broadcast message and send a Broadcast Key Request to the SLPKMF containing the temporary group ID, UE1 ID and the respective UEx ID as well as the Zone ID, indicating the local area where they are located.

9. The SLPKMF checks whether the UEs respond within the validity time of the broadcast request.

10. The SLPKMF sends an authorization request to the Ranging Server for the received responses with respect to temporary groupd ID. The request contains the UE1 ID, responder UEx ID and respective Zone ID.

11. The Ranging Server authorizes the request of the participating UEs and may check whether all participating UEs are located in the same Zone (proximity check), i.e. it compares the Zone ID provided by UE1 in step 2 with the ones from UEx. If the Zones of the UE1 and a responding UEx are different, the authorization may be rejected.

12. The Ranging Server provides the authorization result to the SLPKMF.

13. The SLPKMF provides the Group Broadcast Key KB generated in step 5 to all responding UEx.

14. All UEs participate in the requested SL Ranging/Positioning action according to the request in step 7.

15. If SLPP Session-based operation is used, the UE1 establishes an SLPP session with the participating UEs. The SLPP Session may use the Broadcast Key KB for authentication and establishment. This step may be skipped if SLPP Session-less operation is used.

16. The participating UEs provide their results from the performed action in step 14, e.g. Assistance Data/Configuration/Location Information to the UE1, protected with the common group broadcast key KB.

If SLPP Session-less operation is used, each participating UE broadcasts the information.

If SLPP Session-based operation is used, each participating UE sends the information within the established SLPP session.

17. If SLPP Session-based operation is used, the UE1 terminates the SLPP session with the participating UEs when the SL Ranging/Positioning action has been completed. All UEs delete the Broadcast Key KB.

Editor’s Note: how broadcast messages are confidentiality and integrity protected are FFS

Editor’s Note: Whether the solution is aligned with RAN2 broadcast scenarios is FFS

### 6.28.3 Evaluation

The solution applies for in-coverage scenario, all UEs involved in the communication must be able to communicate with the network.

Depending on RAN2 decision, the responses may be sent in an SLPP Session-less or SLPP Session-based operation.

Editor’s Note: Further evaluation is FFS

## 6.29 Solution #29: Discovery security material and SL session root key provisioning for Ranging/SL positioning UE discovery

### 6.29.1 Introduction

This solution addresses Key issue #3: Protection of discovery procedure and Key issue #4: Protection of unicast direct communication.

TS 23.586 [11] defines the use cases that the LMF may obtain the UE IDs of Located UE(s), Reference UE(s) and provides the UE ID list to the Target UE to assist Ranging/SL positioning UE discovery and/or Ranging/Sidelink Positioning.

E.g., for selection of Located UE for Network based SL Positioning (e.g. 5GC-MO-LR or 5GC-MT-LR), the LMF may be pre-configured with the list of candidate Located UEs including e.g. the capability, stationary information, and location information of the Located UE(s), e.g. RSU or the operator deployed Located UE. The LMF may provide to the Target UE a list of candidate Located UE(s) as assistance data. For Ranging/SL Positioning service exposure, the request from AF includes one or multiple target UEs and optionally it may include additional information such as the SL reference UE for relative distance/direction. Then LMF triggers a Ranging/Sidelink Positioning session for involved UE accordingly.

This solution proposes that security material used for discovery security between Target UE and Located UE/Reference UE are provisioned by the network as part of DL Positioning procedure. Hence, the Target UE and Located/Reference UE can use the provisioned discovery security material to protect the discovery messages.

This solution also proposes that security material used for establishing a secure PC5 link for PC5 communication (called SL session Root Key in this document, which is used as root to derive PC5 session keys) between Target UE and Located UE/Reference UE can also be provisioned by the network as part of DL Positioning procedure. Hence, the Target UE and Located UE/Reference UE can use the provisioned SL session root key to derive PC5 session keys to protect the PC5 link.

This solution assumes both Target UE and Located/Reference UE have connectiontivity to the network, e.g. to retrieve security materials.

Editor’s Note: For mobile terminated operation, UE may not be always in coverage and have connection. How to solve this issue is FFS.

### 6.29.2 Solution details

Figure 6.29.2-1 illustrates the high-level procedure of the proposed solution.



Figure 6.29.2-1: High-level procedure for security material provisioning for Ranging UE1. In case the AMF receives request for SL Ranging/Positioning (e.g. MO-LR, MT-LR), the AMF triggers positioning of Target UE with the LMF and includes Target UE ID in the message. If the received request includes one or multiple SL reference UE ID(s) (e.g. from original request from AF for Ranging/SL Positioning service exposure), the AMF forwards SL reference UE ID(s) in the LCS service request towards LMF.

Editor’s Note: How AMF can trigger the SL positioning or ranging request is FFS.

2. LMF determines to trigger the SL positioning or Ranging to the Target UE. If LMF receives SL positioning request from the Target UE/GMLC/AF via AMF, LMF may determine to trigger SL positioning and provide to the Target UE a list of candidate Located UE(s) as assistance data. If LMF receives Ranging request from GMLC/AF via AMF, LMF may get the Target UE information and the Reference UE(s) information from the request.

NOTE: How LMF obtains and determines the candicate Located UEs is up to SA2 design.

3. The LMF obtains the security materials of discovery security for each pair of Target UE and Located/Reference UE from 5G PKMF. The LMF can also generate the discovery security material by itself.

The security material for discovery security includes e.g. ProSe Restricted Code, ProSe Query Code, ProSe Response Code, Code-Receiving Security Parameters, Code-Sending Security Parameters, Discovery Query Filter(s), CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm etc.

The LMF obtains the security materials of PC5 communication security for each pair of Target UE and Located UE/Reference UE from 5G PKMF. The security material for PC5 communication security includes e.g. secrets that can be used as long term credentials as specified in TS 33.536 for the Target UE and Located UE/Reference UE. The LMF can also generate the security material e.g. SL session root key by itself.

Editor’s Note: How a LMF can interact with 5G PKMF to get the security materials of Target UE/Reference UE/Located UE is FFS.

Editor’s Note: The reason for LMF providing the security materials is FFS.

4. The LMF maintains a session ID of positioning requests for each pair of Target UE and Located/Reference UE which is associated with the corresponding security material for discovery security and security material for PC5 communication security.

The LMF sends the Ranging/Sidelink positioning requests to Target UE and Located/Reference UE to trigger the Ranging/Sidelink positioning procedure via downlink NAS message. The LMF includes in the message with container for discovery security material and/or the container for SL session root key for PC5 communication security and the associated Session ID.

5. The Target UE and Located/Reference UE initiates either Model A or Model B discovery procedures over PC5 using the discovery key and the associated discovery codes e.g. ProSe Restricted/Query/Response Code provided by the LMF.

6. If the container for SL session root key for PC5 link establishment is provisioned, then the Target UE and Located UE/Reference UE initiates PC5 link establishment using the security procedure as specified in TS 33.536. The Target UE and Located UE/Reference UE authenticate each other based on the provisioned PC5 communication security material from the LMF, e.g. using the secrets in PC5 communication security material as long term credentials as specified in TS 33.536 [5].

### 6.29.3 Evaluation

Editor’s Note: Further evaluation is FFS.

# 7 Conclusions

## 7.1 Conclusions on Key Issue #1

To protect UE privacy of Ranging/SL Positioning services, the following conclusions are made:

- For privacy protection during discovery:

- The discovery security materials provisioned during the Discovery Key Request procedure are used to protect the privacy sensitive information (e.g. UE identity) in the discovery messages.

NOTE 1: The privacy protection of the integrated discovery message for V2X capable UEs is to be aligned with the conclusions on key issue #3.

- For privacy protection during communication:

- For unicast direct communication over SR5 reference point, security policy configuration for confidentiality protection is used as the basis for normative work. The security procedures defined in clause 5.3.3.2 of TS 33.536 [5] are reused for non-trackability protection.

- For Ranging/SL positioning result exposure to a Client UE over PC5, the method of PC5-U security policy setting for confidentiality protection (as defined for ProSe/V2X services) is used.

- For Ranging/SL positioning result exposure to a Client UE over Uu using enhanced MO-LR procedure, NAS security for confidentiality protection is used.

- For broadcast communication over SR5 reference point, the broadcast mode security mechanism to randomise the UE’s source Layer-2 ID and source IP address including IP prefix (if used), as defined in clause 5.5 of TS 33.536 [5], is reused for non-trackability protection.

- For groupcast communication over SR5 reference point, the groupcast mode security mechanism to randomise the UE’s source Layer-2 ID and source IP address including IP prefix (if used), as defined in clause 5.5 of TS 33.536 [5], is reused for non-trackability protection.

NOTE 2: The conclusions on broadcast and groupcast communication as above should be aligned with the conclusions on key issue #5.

## 7.2 Conclusions on Key Issue #2

The following conclusions are made on Key Issue #2:

- To authorize an application server or a 5GC NF for Ranging/SL Positioning service exposure, the MT-LR procedure specified in TS 23.273 [9] is taken as the baseline. The GMLC interacts with the UDM to check the UE privacy profile and interacts with the AMF for UE privacy verification.

- For Ranging/SL Positioning service exposure through the network via control plane (i.e. clause 6.7.1.2.3, TS 23.586 [11]), the SL Positioning Client UE authorization is reusing the MO-LR authorization as specified in TS 23.273 [9].

- For Ranging/SL Positioning service exposure through PC5, the SL Positioning Client UE authorization is triggered by the Reference/Target UE during PC5 link establishment. The authorization can be performed by the network via the PKMF for ProSe capable UEs or by the Reference/Target UE if the authorization information is available in the UE.

NOTE: Whether the authorization is based on the existing UE LCS privacy profile in UDM or whether it’s new data or profile is to be decided in normative work, and needs to be coordinated with SA2.

- To authorize the UE in its role (e.g. as a Target UE/Reference UE/Located UE/SL Positioning Server UE) in a Ranging/Sidelink Positioning service, the authorization is performed as the following:

- When the UE role is claimed towards the network, the authorization of UE role is performed through the interaction with the UDM (via e.g. DDNMF/PKMF/PCF or GMLC) by checking the subscription information on the allowed role(s) of the UE as defined in clause 5.8 of TS 23.586 [11]. Only when the role of the UE is successfully authorized, the subsequent procedure (e.g. generating and provisioning discovery security materials to the UE, Ranging/SL positioning procedure) can proceed.

- When the UE role is claimed towards the peer UE, the authorization of UE role is performed by the peer UE via checking the locally pre-configured authorization/privacy verification information, which is provisioned either from the application or from the network.

## 7.3 Conclusions on Key Issue #3

For protection of discovery procedure, the following conclusions are made:

- For ProSe capable UEs, the 5G ProSe Restricted Discovery security procedure defined in clause 6.1.3.2 of TS 33.503 [6] is taken as the baseline for discovery security with the following changes:

- The discovery security materials are provisioned by 5G PKMF or PCF.

- For V2X capable UEs, the security procedures defined in clause 5.3.3 of TS 33.536 [5] is reused.

NOTE: Whether the DCR message of V2X capable UEs needs to be protected is to be determined during normative work based on the DCR information defined by SA2 and RAN2.

## 7.4 Conclusions on Key Issue #4

For protection of unicast direct communication, the following conclusions are made:

- For security of SR5 direct communication for Ranging/SL Positioning services provided by application providers, the security mechanisms defined for V2X unicast mode communication in TS 33.536 [5] and for 5G ProSe unicast mode Direct Communication in TS 33.503 [6] are reused.

- For security of SR5 direct communication for network assisted SL positioning services provided by operators, the security mechanisms defined for 5G ProSe UE-to-Network Relay communication in TS 33.503 [6] can be reused.

- To protect RSPP unicast messages on SR5 reference point, security policies for the Ranging/SL Positioning service are to be enforced on PDCP layer.

- During the establishment of the direct communication for the Ranging/SL positioning service, the UEs reuses the security policy negotiation to decide the security protection status of the direct communication for the Ranging/SL positioning servic, as defined in 5G ProSe in TS 33.503 [6] and/or in 5G V2X in TS 33.536 [5].

- Security policies for PC5-S integrity and confidentiality and PC5-U confidentiality follow the configurations defined in TS 33.536 [5] for V2X capable UEs and TS 33.503 [6] for ProSe capable UEs. Whether the security policy for PC5-U integrity is configured as "REQUIRED" is to be determined during normative work.

Annex X:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107e-AdHoc | S3-221537 |  |  |  | Skeleton (approved at SA3#107e-AdHoc) | 0.0.1 |
| 2022-07 | SA3#107e-AdHoc | S3-221627 |  |  |  | Inclusion of the documents approved at SA3#107e-AdHoc: S3-221538, S3-221622, S3-221623, S3-221624, S3-221647 | 0.1.0 |
| 2022-08 | SA3#108e | S3-222406 |  |  |  | Inclusion of the documents approved at SA3#108e: S3-222071, S3-222206, S3-222348, S3-222349 | 0.2.0 |
| 2022-10 | SA3#108Adhoc-e | S3-223038 |  |  |  | Inclusion of the documents approved at SA3#108Adhoc-e: S3-223034, S3-223035, S3-223036, S3-223037, S3-223094, S3-223112, S3-223113 | 0.3.0 |
| 2022-11 | SA3#109 | S3-224129 |  |  |  | Inclusion of the documents approved at SA3#109: S3-223747, S3-223748, S3-223982, S3-224128, S3-224130, S3-224131 | 0.4.0 |
| 2023-01 | SA3#109Adhoc-e | S3-230564 |  |  |  | Inclusion of the documents approved at SA3#109Adhoc-e: S3-230236, S3-230238, S3-230403, S3-230404, S3-230467, S3-230468, S3-230502, S3-230503, S3-230504, S3-230527, S3-230555, S3-230559, S3-230560, S3-230561, S3-230562, S3-230566 | 0.5.0 |
| 2023-02 | SA3#110 | S3-231519 |  |  |  | Inclusion of the documents approved at SA3#110: S3-231215, S3-231259, S3-231260, S3-231515, S3-231516, S3-231517, S3-231518, S3-231520, S3-231521, S3-231522, S3-231600, S3-231624, S3-231625, S3-231626, S3-231632 | 0.6.0 |
| 2023-04 | SA3#110Adhoc-e | S3-232197 |  |  |  | Inclusion of the documents approved at SA3#110Adhoc-e: S3-231824, S3-232035, S3-232036, S3-232037, S3-232059, S3-232124, S3-232127, S3-232138, S3-232139, S3-232148, S3-232149, S3-232150, S3-232157, S3-232158, S3-232165, S3-232166, S3-232179, S3-232180, S3-232181, S3-232182, S3-232183, S3-232184, S3-232185, S3-232187, S3-232188, S3-232190, S3-232201, S3-232233 | 0.7.0 |
| 2023-05 | SA3#111 | S3-233210 |  |  |  | Inclusion of the documents approved at SA3#111: S3-232578, S3-233225, S3-233226, S3-233227, S3-233228, S3-233229, S3-233230, S3-233394, S3-233395, S3-233396, S3-233397 | 1.0.0 |