|  |
| --- |
| 3GPP TR 33.893 V0.4.0 (2022-11) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Architecture assumptions 8

4.1 Reference architecture 8

4.2 Reference points 9

5 Key issues 9

5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services 9

5.1.1 Key issue details 9

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Authorization for Ranging/Sidelink Positioning Service 10

5.2.1 Key issue details 10

5.2.2 Security threats 11

5.2.3 Potential security requirements 11

5.3 Key issue #3: Protection of discovery procedure 11

5.3.1 Key issue details 11

5.3.2 Security threats 11

5.3.3 Potential security requirements 12

5.4 Key issue #4: Protection of direct communication 12

5.4.1 Key issue details 12

5.4.2 Security threats 12

5.4.3 Potential security requirements 12

5.X Key issue #X: <Title> 13

5.X.1 Key issue details 13

5.X.2 Security threats 13

5.X.3 Potential security requirements 13

6 Solutions 13

6.0 Mapping of solutions to key issues 13

6.1 Solution #1: Privacy protection for UEs in Ranging 13

6.1.1 Introduction 13

6.1.2 Solution details 13

6.1.3 Evaluation 15

6.2 Solution #2: Authorization of 5GC NF for Ranging/SL positioning service exposure 15

6.2.1 Introduction 15

6.2.2 Solution details 15

6.2.3 Evaluation 17

6.3 Solution #3: Authorization of Application Server for Ranging/SL positioning service exposure 17

6.3.1 Introduction 17

6.3.2 Solution details 17

6.3.3 Evaluation 19

6.4 Solution #4: Subscription-based authorization of the role of the UE during discovery 19

6.4.1 Introduction 19

6.4.2 Solution details 20

6.4.3 Evaluation 23

6.5 Solution #5: Use of authorization tokens at PC5 security establishment 24

6.5.1 Introduction 24

6.5.2 Solution details 24

6.5.2.1 Token based authorization for scenario of SL positioning services 24

6.5.2.1.1 Security for network assisted Sidelink Positioning with full network coverage 24

6.5.2.1.2 Security for network assisted Sidelink Positioning with partial network coverage 25

6.5.2.2 Token based authorization for scenario of Ranging services 26

6.5.2.2.1 Security for Ranging procedure between Reference UE and Target UE 26

6.5.2.2.2 Security for Ranging procedure between Reference UE/Target UE and Assistant UE 27

6.5.3 Evaluation 29

6.6 Solution #6: Protection of direct communication for Sidelink Positioning service 29

6.6.1 Introduction 29

6.6.2 Solution details 29

6.6.3 Evaluation 30

6.7 Solution #7: Security policy based protection for Ranging/SL positioning service operation 31

6.7.1 Introduction 31

6.7.2 Solution details 31

6.7.3 Evaluation 32

6.8 Solution #8: Security policy based protection for ranging result sent to SL Positioning Client UE 32

6.8.1 Introduction 32

6.8.2 Solution details 33

6.8.2.1 Security policy configuration for ranging result sent via PC5 33

6.8.2.2 Security policy configuration for ranging result sent via 5GC 33

6.8.3 Evaluation 34

6.Y Solution #Y: <Title> 34

6.Y.1 Introduction 34

6.Y.2 Solution details 34

6.Y.3 Evaluation 34

7 Conclusions 35

Annex X: Change history 36

# 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".

# 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.

Editor's Note: Whether exposing positioning signals for ranging/sidelink positioning after discovery requires privacy protection is FFS.

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. Based on the authorization checking, the access to 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 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.

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.

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.

## 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 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, if the UE cannot authenticate the peer UE to be the entity it intends to communicate with, it may lead to the disclosure of privacy-sensitive information to the peer UE.

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 Ranging results.

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 direct communication of Ranging/SL Positioning service.

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

The 5G system shall support a means to protect the confidentiality 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.X Key issue #X: <Title>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 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.

NOTE 1: The solution assumes that Ranging authorization is not performed during discovery and communication establishment procedures.

3. UE1 sends the ranging request in the Ranging/SL Positioning layer to the UE2 to check the authorization and negotiate the ranging parameters. The ranging request includes the ranging parameters, e.g. the Ranging role (Reference UE or Target UE), 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”. If it is implied by the ranging role, the result calculation entity is not needed.

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. UE2 decides whether to accept the ranging role as assigned by UE1. 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 the Ranging role or result calculation entity, for example due to its privacy consideration, a new Ranging role or result calculation entity is included.

NOTE 2: 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 accordingly 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. Ranging authorization on consumer info, purpose or result calculation entity is performed in the Ranging/SL Positioning layer based on configuration, which may be provided from application layer. The UE determines whether to continue the ranging process according to the authorization and negotiation result.

Editor’s Note: Further evaluation is FFS.

## 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 unauthorized SL positioning information could be exposed to the 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, assuming the SL positioning service procedure does not rely on the existing procedure for enhanced location service.

### 6.2.2 Solution details

The solution proposes that, when the 5GC NF checks with the UDM to discover the serving AMF(s) of the UEs, it also needs 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.

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

2. The 5GC NF interacts with the UDM to check the authorization info of UE1/UE2 via Nudm\_SDM\_Get service operation.

NOTE: If UE1 and UE2 are managed by different UDMs, the 5GC NF sends the Nudm\_SDM\_Get message to the corresponding UDMs respectively.

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 5GC NF.

5. The 5GC NF 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 5GC NF aborts the Ranging/SL positioning service.

If both UEs grant authorization without location restriction, the 5GC NF proceeds to step #11.

Conditionally, if both UEs grant authorization which is restricted in a certain area, the 5GC NF proceeds to step #6.

If the 5GC NF is the AMF of the UEs, the 5GC NF skips the steps #6~#9 and proceeds to step #10.



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

6. [Conditional] The 5GC NF sends the Nudm\_ParameterProvision\_Get Request to the UDM for requesting the coarse location of UE1/UE2 (e.g. TAI or Cell-ID of UE1/UE2).

7. [Conditional] The UDM sends the Namf\_Location\_ProvideLocationInfo Request to the AMF.

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

9. [Conditional] The UDM returns the Nudm\_ParameterProvision\_Get Response to the 5GC NF which contains the coarse location of UE1/UE2 (e.g. TAI or Cell-ID of UE1/UE2).

10. [Conditional] Based on the coarse location of UE1/UE2, the 5GC NF checks whether the UE1/UE2 is within the area for requesting SL Positioning service.

11. If both UEs grant authorization in their current locations, the 5GC NF sends the SL Positioning service request to the AMF of one of the UEs (e.g. UE1). If the 5GC NF is the AMF, this step can be skipped.

12~15. The rest of the SL Positioning procedure is performed between the network and the UE.

Alternatively, after the 5GC NF checks the authorization info of both UEs in step #5, if both UEs grant authorization which is however restricted in a certain area, the 5GC NF sends the Namf\_Location\_ProvideLocationInfo Request to the AMF directly rather than through the UDM. Then the AMF responds the Namf\_Location\_ProvideLocationInfo Response to the 5GC NF directly rather than through the UDM.

NOTE: 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 of all involved UEs in a service, as Ranging/SL Positioning services request UE location information which is privacy sensitive.

This solution does no assume the availability of the architecture supporting location based services, and relies on the requesting 5GC NF itself to check with the UDM for the authorization information of the involved UEs. Therefore, only the requesting 5GC NF is impacted in this solution, which is anyway impacted by the requirement of triggering the SL Positioning services.

## 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: If UE1 and UE2 are managed by different UDMs, the GMLC/NEF sends the Nudm\_SDM\_Get message to the corresponding UDMs respectively.

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.

Editor's Note: In the Ranging Service, the need for privacy profile with area granularity is ffs

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 3: 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.

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.

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.

## 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 third 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.

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 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

Editor’s Note: Whether 5G DDNMF/PKMF/Application Server are involved in Ranging/SL positioning discovery is FFS.

### 6.4.3 Evaluation

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

## 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].

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: The details and necessity of the token are FFS.

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 its token in the discovery message. Once receiving the discovery messages, the Target UE verifies the discovery message and 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 its token to the Target UE. Once receiving the discovery messages, the Target UE verifies the integrity of discovery message and 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: 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 if UE-1 does not have a valid SLPK, SL Positioning Code (SLPC) of the SL Positioning Service and KSLP nonce 1.

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. If SLPK ID is received, 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

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

## 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 are carried between UEs over SR5 reference point, SR5 security policies need to support the security requirements for protecting the key information, 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. Therefore, it is proposed that the SR5 security policies for integrity protection and confidentiality protection of Ranging/SL Positioning services should be set as “REQUIRED” only.

Alternatively, as SR5 security policies for Ranging/SL Positioning services 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.

Editor’s Note: whether both SR5 security and PC5 security need to be established is FFS.

### 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 services 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.

Editor’s Note: further evaluation is FFS.

## 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 communicate 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

If the ranging result is transmitted via Uu control plane from the UE to the 5GC and further to SL Positioning Client UE, the integrity and confidentiality protection of ranging result can be provided by the existing NAS security.

If the ranging result is transmitted via Uu user plane from the UE to the 5GC and further to SL Positioning Client UE, the integrity and confidentiality protection of ranging result 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 and Uu data by configuring proper PC5/Uu UP security policies on the involved UEs, hence has minimum impact on the network and the UE.

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 polices.

Editor’s Note: further evaluation is FFS.

## 6.Y Solution #Y: <Title>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any 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 |
|  |  |  |  |  |  |  |  |