|  |  |
| --- | --- |
| 3GPP TR 33.893 V0.2.0 (2022-08) | |
| 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 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Architecture assumptions 7

4.1 Reference architecture 7

4.2 Reference points 8

5 Key issues 8

5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Authorization for Ranging/Sidelink Positioning Service 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

5.3 Key issue #3: Protection of discovery procedure 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key issue #4: Protection of direct communication 10

5.4.1 Key issue details 10

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.X Key issue #X: <Title> 11

5.X.1 Key issue details 11

5.X.2 Security threats 11

5.X.3 Potential security requirements 11

6 Solutions 12

6.1 Mapping of solutions to key issues 12

6.Y Solution #Y: <Title> 12

6.Y.1 Introduction 12

6.Y.2 Solution details 12

6.Y.3 Evaluation 12

7 Conclusions 12

Annex X: Change history 13

# 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".

# 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].

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

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

<ABBREVIATION> <Expansion>

# 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

The reference architecture for Ranging/SL Positioning is shown in Figure 4.1-1. The UE A and UE B involved in Ranging/SL Positioning can be subscribed to the same 5G network or subscribed to different 5G networks. The reference architecture also supports the case where UE-A or UE-B or both are not registered to the network or not in coverage. UE C and UE D may be out of network coverage, or with partial network coverage.

NOTE 1: For simplicity, the figure only shows target UE and reference UE (i.e. UE-A, UE-B, UE-C and UE-D), and there could also be Assistant UE, Located UE and Location Server UE in the architecture.

NOTE 2: Other 5GC entities not marked with the SL positioning/Ranging label may also need to be involved in SL positioning/Ranging.

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 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. 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 reference UE and invalidate the charging mechanism.

An unauthorized UE can claim the role of the 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 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.

## 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. 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 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 reference UE connects with a 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 PC5 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 PC5 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 PC5 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 PC5 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 PC5 direct communication of Ranging/SL Positioning service.

The 5G system shall support a means to protect the integrity of the information transferred during PC5 direct communication for the Ranging/SL Positioning service.

The 5G system shall support a means to protect the confidentiality of the information transferred during PC5 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 PC5 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.

## 6.1 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.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 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |