|  |
| --- |
| 3GPP TS 33.533 V0.1.0 (2023-05) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;;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.© 2023, 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 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview of security architecture 6

4.1 General 6

4.2 Functional entities and reference points 7

4.2.1 Functional entities 7

4.2.2 Reference points 7

5 Security requirements and procedures 7

5.1 General 7

5.2 Common security 7

5.3 Security for Ranging/SL positioning discovery 7

5.4 Authorization for Ranging/SL positioning service 7

6 Security related services 7

Annex <X> (informative): Change history 8

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document specifies the security and privacy aspects of Ranging based services and Sidelink positioning in the 5G System (5GS) for commercial, V2X and public safety use cases, with the UE in coverage, partial coverage, and out-of-coverage of 5G network using 5G NR PC5 RAT, based on the architecture defined in TS 23.586 [2].

Security features for Ranging based services and Sidelink positioning include: authorization for Ranging/SL positioning service, security and privacy protection for Ranging/SL positioning UE discovery, security and privacy protection for unicast communication of Ranging/SL positioning control, and security and privacy protection for broadcast/groupcast communication of Ranging/SL positioning control.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.586: "Architectural Enhancements to support Ranging based services and Sidelink Positioning".

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

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

[5] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support 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 38.355: " NR; Sidelink Positioning Protocol (SLPP); Protocol Specification".

[8] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

# 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 Overview of security architecture

## 4.1 General

The overall architecture for Ranging/SL Positioning is specified in clause 4.2 of TS 23.586 [2], which involves the LCS architecture specified in TS 23.273 [3] and 5G Prose architecture specified in TS 23.304 [4]. The reference architecture also supports roaming scenario and inter-PLMN scenario.

Based on the architecture specified in TS 23.586 [2], the security architecture for Ranging/SL Positioning also supports roaming and inter-PLMN scenario, and reuses the security architecture of 5G ProSe services and security architecture of LCS services with necessary enhancements or adaptations.

## 4.2 Functional entities and reference points

### 4.2.1 Functional entities

Editor's Note: This sub-clause describes the functional requirements supported by the security related entities involved in the architecture.

### 4.2.2 Reference points

In addition to the reference points specified in clause 4.2 of TS 23.586 [2], the following reference points are added or enhanced for supporting Ranging/SL positioning security architecture:

**NL6:** The reference point between the UDM and the GMLC. It is used to transport the UE privacy profile to GMLC for authorization of Ranging/SL Positioning service exposure.

Editor's Note: more reference points supporting Ranging/SL positioning security architecture are FFS.

# 5 Common security

Editor's Note: This clause introduces the new clause and the specific contents to be included in next sub-clauses. The list of contents to be included in the normative text is not closed yet, so the current outline can be extended with new sub-clauses.

# 6 Security for Ranging/SL positioning features

## 6.1 General

Editor's Note: This clause introduces the new clause and the specific contents to be included in next sub-clauses. The list of contents to be included in the normative text is not closed yet, so the current outline can be extended with new sub-clauses.

## 6.2 Security for Ranging/SL positioning discovery

### 6.2.1 General

For ProSe capable UEs, the discovery procedures of both Model A and Model B defined in clause 6.3.2 of TS 23.304 [4] are used for Ranging/SL Positioning discovery.

For V2X capable UEs, the procedure of integrated discovery during V2X communication defined in clause 6.3.3 of TS 23.287 [5] are used for Ranging/SL Positioning discovery.

### 6.2.2 Security requirements

The 5G system shall support integrity protection, confidentiality protection and anti-replay protection of discovery messages.

The SLPKMF or 5G PKMF shall be able to provision discovery security materials to ProSe capable UEs. The discovery security materials are used to protect the integrity of discovery messages and privacy sensitive information (e.g. UE identity) in the messages.

The ciphering algorithm for discovery message confidentiality shall be configured by the network during discovery key request procedure.

Editor’s Note: Whether a new network function (SLPKMF) or an existing network function (5G PKMF) is used is FFS.

### 6.2.3 Security procedures for ProSe capable UEs

The security mechanisms for both models of restricted 5G ProSe Direct Discovery defined in clause 6.1.3.2 of TS 33.503 [6] are reused for ProSe capable UEs to provide protection for Ranging/SL positioning UE discovery.

The main difference is that SLPKMF or 5G PKMF rather than 5G DDNMF is used to provision discovery security materials for Ranging/SL positioning UE discovery.

## 6.3 Authorization for Ranging/SL positioning service

Editor's Note: This sub-clause introduces the security requirements and procedures for authorizing the elements (including the UE, application server, network functions) involved in Ranging/SL positioning services. The list of contents to be included in the normative text is not closed yet, so the current outline can be extended with further sub-clauses.

Editor's Note: This sub-clause may be subject to adjustment of the document structure pending on procedure discussion.

### 6.3.1 General

According to clause 4.1 of TS 23.586 [2], a UE capable of Ranging/SL Positioning may take different roles in various Ranging/SL Positioning operations. Each of the UEs in a Ranging/SL Positioning service acts in its own authorized role. The UE shall follow the policy/parameters defined in clause 5.1 of TS 23.586 [2] for authorization with the network. TS 23.586 [2] clause 5.6 also specifies that Ranging/SL Positioning service can be exposed to an authorized SL Positioning Client UE, 5GC NF or AF to obtain the relative or absolution distance/direction result between two UEs capable of Ranging/SL positioning.

This clause specifies the authorization requirements and procedures for the operations in Ranging/SL positioning services wherever authorization is required.

### 6.3.2 Authorization requirements

The 5G system shall support the authorization of the role of the UE (e.g. as a Target UE/SL Reference UE/SL Positioning Server UE/Located UE) in a Ranging/Sidelink Positioning service.

The 5G system shall support the authorization of the AF/5GC NF/SL Positioning Client UE for Ranging/SL Positioning service exposure.

Editor’s Note: The authorization requirement on SL Positioning Client UE is to be aligned with the specification in SA2.

The 5G system shall support privacy protection of the to-be-measured UEs for Ranging/SL Positioning service exposure.

## 6.4 Security for communication of Ranging/SL positioning control

### 6.4.1 General

Ranging/SL Positioning control is defined in TS 23.586 [2], which is supported by the Ranging/SL Positioning layer above the AS layer. The Ranging/SL Positioning layer provides the support of Ranging/SL Positioning Protocol (RSPP) (i.e. Sidelink Positioning Protocol (SLPP) defined in TS 38.355 [7]) and the protocol between the UE and LMF for Ranging/SL Positioning.

Editor's note: The protocol used between the UE and LMF is FFS in RAN2.

Ranging/SL Positioning control over RSPP is performed on SR5 reference point between UEs. PC5-U is used as the transport layer for RSPP as specified in clause 5.3.2 of TS 23.586 [2]. Depending on type of the UE (V2X capable or 5G ProSe capable), V2X Communication procedures defined in TS 23.287 [5] or 5G ProSe Direct Communication procedures defined in TS 23.304 [4] are used for RSPP transport between UEs.

Ranging/SL Positioning control over the protocol between the UE and LMF is specified in clauses 6.x and 6.y of TS 23.273 [3].

### 6.4.2 Security requirements

The Ranging/SL Positioning system shall support mutually authentication between the UEs during unicast direct communication establishement for Ranging/SL Positioning control over RSPP.

The Ranging/SL Positioning system shall support integrity, confidentiality and anti-replay protection for the information transferred during unicast direct communication for Ranging/SL Positioning control over RSPP.

The Ranging/SL Positioning system shall support cryptographic separation for each SR5 interface and for each peer UE during unicast direct communication for Ranging/SL Positioning control over RSPP.

The Ranging/SL Positioning system shall support integrity, confidentiality and anti-replay protection for the information transferred during unicast communication for Ranging/SL Positioning control over the protocol between the UE and LMF.

### 6.4.3 Security procedure for unicast direct communication over RSPP between the UEs

#### 6.4.3.1 General

Ranging/SL Positioning services could be provided by an application provider (i.e. the services requested by a Ranging/SL positioning application server) or by a network operator (i.e. the services requested by a 5GC NF). For Ranging/SL Positioning services provided by application providers, long term credentials provided by applications are assumed available on the UE. For Ranging/SL Positioning services provided by network operators, there are no long term credentials provided by applications on the UE.

#### 6.4.3.2 Unicast direct communication with long term credentials

If long term credentials are available on the UE, the security procedures defined for V2X unicast mode communication in clause 5.3 of TS 33.536 [8] are reused on V2X capable UEs. The security procedures defined for 5G ProSe unicast mode Direct Communication in clause 6.2.3 of TS 33.503 [6] are reused on ProSe capable UEs.

### 6.4.4 Security procedure for communication between the UE and LMF

Editor’s Note: whether NAS security is sufficient for security protection of unicast communication between the UE and LMF is FFS depending on the specification in RAN2.

# 7 Security related services

Editor's Note: This clause describes the new network services if they are identified to be introduced based on the security procedures described in clause 5. The clause can be removed if no new security related services are identified.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2023-04 | SA3#110-adhoc-e | S3-232195 |  |  |  | Implementation of S3-232028, S3-232194 | 0.0.0 |
| 2023-05 | SA3#111 | S3-233311 |  |  |  | Implementation of S3-233309, S3-233310, S3-233312, S3-233313, S3-233314, S3-233315, S3-233398 | 0.1.0 |