ETSI TS 133 533 V18.4.0 (2024-10)

5G;
Security aspects of ranging based services and sidelink positioning
(3GPP TS 33.533 version 18.4.0 Release 18)

Reference
RTS/TSGS-0333533vi40

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

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".

[9] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[10] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[11] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[12] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[13] 3GPP TS 24.080: "Mobile radio interface layer 3 supplementary services specification; Formats and coding".

[14] 3GPP TS 24.514: "Ranging based services and sidelink positioning in 5G system(5GS); Stage 3".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and TS 23.586 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Located UE

Network-based Operation

Positioning

Ranging

Ranging/SL Positioning Application Identifier

SL Reference UE

Sidelink Positioning

SL Positioning Client UE

SL Positioning Server UE

Target UE

UE-only Operation

User Info ID

Application Layer ID

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

AKMA	Authentication and Key Management for Applications
DCR	Direct Communication Request
GBA	Generic Bootstrapping Architecture
LCS	Location Service
LMF	Location Management Function
ProSe	Proximity based Service
RSPP	Ranging/SL Positioning Protocol
SLP	Sidelink Positioning
SLPEK	Sidelink Positioning Encryption Key
SLPGK	Sidelink Positioning Group Key
SLPIK	Sidelink Positioning Integrity Key
SLPK	SideLink Positioning Key
SLPKMF	SideLink Positioning Key Management Function
SLPP	SideLink Positioning Protocol
SLPTK	Sidelink Positioning Traffic Key
UTC	Universal Time Coordinated
V2X	Vehicle-to-Everything

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

4.2.1.1 SideLink Positioning Key Management Function

The SideLink Positioning Key Management Function (SLPKMF) is the logical function handling network related operations required for generation and provisioning of security materials used for Ranging/SL positioning services. The SLPKMF has the similar functionalities as those of 5G Prose Key Management Function (PKMF) specified in TS 33.503 [6] and can be a standalone entity or collocated with 5G PKMF. In addition to the functionalities supported by 5G PKMF, the SLPKMF shall support the following functions:

- Support key management for secure unicast direct link establishment between the UEs for Ranging/SL Positioning services provided by network.
- Support UE role authorization via the UDM.
- Support key management for protection of SLPP signalling broadcast/groupcast.

The address of SLPKMF can be preconfigured on the UE or provisioned by the PCF to the UE.

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:

NL3: The reference point between the GMLCs in different PLMNs. It is used to transport the UE authorization result for authorization of Ranging/SL Positioning service exposure.

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.

PC8*: The reference point between the UE and the SLPKMF, which relies on 5GC user plane for transport (i.e. an "over IP" reference point). It is used to transport security materials to UEs for Ranging/SL Positioning discovery and communication.

Npc9*: The reference point between the SLPKMFs of the UEs subscribed in different PLMNs. It is used to transport security materials between SLPKMFs to support Ranging/SL Positioning services in inter-PLMN scenarios.

Npc10*: The reference point between the UDM and the SLPKMF. It is used to request subscription information related to Ranging/SL Positioning service from the UDM for UE authorization.

5 Common security

5.1 General

This clause describes the security requirements and procedures commonly applied to different features of Ranging/SL positioning services, including Ranging/SL positioning discovery, Ranging/SL positioning communication with unicast mode, broadcast/groupcast mode, etc.

5.2 Security for PC8* interface

5.2.1 General

The security requirements on PC8* interface between ProSe capable UE and SLPKMF are derived based on the definition of the SLPKMF described in clause 4.2.1.1 and the definition of PC8* interface described in clause 4.2.2.

5.2.2 Security requirements

The 5G System shall support mutual authentication between the ProSe capable UE and the SLPKMF.

The 5G System shall support integrity protection for the transmission between the ProSe capable UE and the SLPKMF.

The 5G System shall support confidentiality protection for the transmission between the ProSe capable UE and the SLPKMF.

The 5G System shall support anti-replay protection for the transmission between the ProSe capable UE and the SLPKMF.

5.2.3 Security procedures for PC8* using GBA

When using GBA for the security procedures on PC8* interface, the use of either TLS v1.2 or TLS v. 1.3 as described in clause 5.3.3.2 of TS 33.303 [9] applies with the following changes:

- The SLPKMF takes the role of ProSe function.
- Confidentiality protection shall be enabled.

5.2.4 Security procedures for PC8* using AKMA

When using AKMA for the security procedures on PC8* interface, the specification in clause B.1.3.2 of TS 33.535 [10] applies with the following changes:

- The SLPKMF takes the role of AF.
- Confidentiality protection shall be enabled.

5.3 Security of service-based interfaces used in Ranging/SL Positioning

Npc9* and Npc10* defined in clause 4.2.2 are realized by corresponding NF service-based interfaces. Security procedures specified in clause 13 of TS 33.501 [11] apply to these interfaces.

6 Security for Ranging/SL positioning features

6.1 Void

6.2 Security for Ranging/SL positioning UE 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 UE discovery.

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

6.2.2 Security requirements

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

The SLPKMF shall be able to provision discovery security materials to ProSe capable UEs. The discovery security materials are associated with the Ranging/SL Positioning application identifier defined in TS 23.586 [2] and 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.

6.2.3 Security procedures for ProSe capable UEs

The security mechanisms for both models of restricted 5G ProSe UE-to-Network Relay 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 with the following changes:

- SLPKMF rather than 5G DDNMF/5G PKMF is used to provision discovery security materials for Ranging/SL positioning UE discovery.
- Ranging/SL Positioning application identifier (as defined in clause 3.1 of TS 23.586 [2]) instead of the Relay Service Code (RSC) is included in the Discovery Key Request/Response messages.
- The SLPKMF of the monitoring/discoverer UE discovers the SLPKMF(s) of potential announcing/discoveree UE(s) supporting the Ranging/SL Positioning application identifier based on a configured list of PLMNs supporting the corresponding Ranging/SL Positioning application.

6.2.4 Security procedures for V2X capable UEs

Based on clause 5.3.3.1 of TS 33.536 [8], the Direct Communication Request (DCR) message is not protected for V2X capable UEs.

NOTE: Any information that needs security protection for Ranging/SL Positioning UE discovery needs to be sent in the Direct Security Mode Complete message.

6.3 Authorization for Ranging/SL positioning service

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 or LCS client 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 or privacy check 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 authorization of the UE for Ranging/SL positioning communication in unicast mode, broadcast/groupcast mode.

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

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

6.3.3 Procedures of UE role authorization for discovery

For ProSe capable UEs, the role of the UE shall be authorized by the network during the procedure of discovery security materials provisioning. The UE role authorization shall be performed via the SLPKMF through Discovery Key Request/Response messages during the security procedure for Ranging/SL positioning discovery as defined in clause 6.2.3 when the UE role is included in the Discovery Key Request. The authorization information used to check whether the UE is allowed to act the announced role in a Ranging/SL positioning service is included in UE subscription data or provisioned to the UE based on TS 23.586 [2]. The SLPKMF may retrieve subscription information from the UDM or use locally configured information for authorizing the role of the UE. After UE role authorization check, the SLPKMF provisions discovery security materials to the UE, which indicates the successful authorization of the UE role.

If the UE announces its role to the peer UE(s) in DCR and DCA messages, the UE role authorization may be performed by the peer UE against its locally configured information, which can be provisioned by the application. If the UE role is not acceptable, the peer UE shall discard or reject the request directly.

6.3.4 Procedures of UE authorization for Ranging/SL positioning communication

The details of UE authorization for Ranging/SL positioning communication in unicast mode are specified in clause 6.4.3.

The details of UE authorization for Ranging/SL positioning communication in broadcast/groupcast mode are specified in clause 6.4.4.

6.3.5 Procedures for authorization of AF/5GC NF/LCS Client for Ranging/SL positioning service exposure

6.3.5.0 General

For the authorization of the AF, 5GC NF or LCS client for Ranging/SL Positioning service exposure, the SL-MT-LR procedure specified in TS 23.273 [3] is taken as the baseline. The authorization shall be performed towards all the n UEs ($n \geq 2$), i.e. UE1, UE2, ..., UEn in the request message. If all of the UEs grant permission for Ranging/SL Positioning exposure, the GMLC shall forward the service request from the AF,5GC NF or LCS client to the AMF. If none of the UEs grants permission for Ranging/SL Positioning exposure, the GMLC shall reject the service request. If part of the UEs grant and part of the UEs don't grant permission for Ranging/SL Positioning exposure, the GMLC shall decide to proceed with or reject the service request from the AF, 5GC NF or LCS client based on the privacy check results of the n UEs and a criterion up to implementation, e.g. a local rule configured by the network operator. If the GMLC decides to accept the service request, it shall only include the identities of the UEs granting permission in the service request forwarded to the AMF.

When receiving the Ranging/SL Positioning service request from the AF,5GC NF or LCS client, the GMLC (i.e. anchor GMLC) interacts with the UDM to check the UE privacy profile. for Ranging/SL Positioning service as specified in Annex B for the UEs belonging to the same PLMN If any of n UEs belong to different PLMNs, then the anchor GMLC sends a request to the Home GMLC of each of those UEs to check the Ranging/SL positioning privacy profiles of the UEs.

NOTE: The address of the Home GMLC of the UE(s) in a different PLMN is determined by the anchor GMLC based on local configuration or by the NRF query.

6.3.5.1 Authorization for the home GMLCs

The Home GMLCs of each of those UEs queries the UDM in its own PLMN to check the UE privacy profile and sends back the privacy check result to the anchor GMLC. When the Home GMLC of each of those UE checks UE Ranging/SL Positioning privacy profile and if privacy check related action (e.g. notification, verification) towards the UE is required, the Home GMLC of each of those UEs shall retrieve the serving AMF from the UDM of each of the UEs and trigger privacy check of the UE towards the serving AMF of each of these UEs via VGMLC, using Ngmlc_Location_ProvideLocation and Namf_Location_ProvidePositioningInfo message which include the indicator of privacy related action for the UE and location type indicating "notification only". The serving AMF shall respond to the Home GMLC of each of the UEs with privacy check results of the UE. If the Ranging/SL Positioning service exposure is disallowed by the UE, or signalling connection establishment fails for UE notification (including UE notification with privacy verification), the serving AMF shall also include failure cause for the UE in the response message to the Home GMLC.

6.3.5.2 Authorization for the anchor GMLCs

The anchor GMLC interacts with the AMF of the target UE (which is treated as UE1 in clause 6.20.3 in TS 23.273 [3]) to request the ranging/SL positioning result of UEs based on the SL-MT-LR procedure as specified in clause 6.20.3 in TS 23.273 [3], which may include an indication of a privacy related action, for each of the UEs if privacy related action is required by the UEs based on privacy profile check result from UDM and if the UEs belonging to the same PLMNand served by the same AMF as the target UE.

If one or more UEs are served by different AMF(s) and privacy related action is required, the anchor GMLC triggers privacy check of these UEs towards the serving AMF(s) of these UEs via VGMLC, using Ngmlc_Location_ProvideLocation and Namf_Location_ProvidePositioningInfo message which include the indicator of privacy related action for each of the UEs and location type indicating "notification only". If the indicator of privacy check related action for each of the UEs indicates that the UEs shall either be notified or notified with privacy verification, a notification invoke message is sent to each of the UEs by the serving AMF(s) if the NAS connection is established. The serving AMF(s) shall respond to the anchor GMLC with privacy check results of the UEs. If the Ranging/SL Positioning service exposure is disallowed by the UE, or NAS connection establishment fails for UE notification (including UE notification with privacy verification), the serving AMF(s) shall also include failure cause for each of the UE(s) in the response message to the anchor GMLC.

6.3.6 Procedures for authorization of UE for Ranging/SL positioning service exposure

6.3.6.1 General

According to TS 23.586 [2], clause 5.6.2, Ranging/SL Positioning service can be exposed to the SL Positioning Client UE through PC5. The SL Positioning Client UE shall be authorized for Ranging/SL Positioning service exposure.

6.3.6.2 Void

6.3.6.3 Authorization procedure for Ranging/SL positioning service exposure through PC5

For Ranging/SL Positioning service exposure through PC5 (i.e. clause 6.7.1.1 of TS 23.586 [2]), the SL Positioning Client UE authorization is triggered by the Target UE during PC5 link establishment. The authorization for service access can be performed by the network via the SLPKMF for ProSe capable UEs according to clause 6.4.3.3or by the Target UE if the authorization information is available in the UE.

If the Client UE is not authorized to access Ranging/SL Positioning service, the PC5 link between the Client UE and the Target UE shall not be established.

For UE-only operation or before triggering SL-MO-LR for Network based operation, the UE1 (i.e. Target UE receiving the Ranging/SL positioning request as in clause 6.8 of TS 23.586 [2]) shall be able to trigger privacy check for Ranging/SL positioning service exposure through PC5.

For exposure of absolute location of the Target UE, UE1 shall perform privacy check using locally configured privacy verification information against the received user info of SL Positioning Client UE.

For exposure of relative locations between Target UE and Reference UEs, UE1 shall trigger privacy check by sending a supplementary RSPP signalling message to UE2/../UEn respectively. The supplementary RSPP signalling message shall include Client UE's user info ID that is received by UE1 from the Client UE. The UE1 and UE2/../UEn shall perform UE privacy check as described in clause 6.3.7 to determine whether their location related information can be exposed to Client UE.

If the Client UE is authorized as per UE privacy check, UE1 shall send the Ranging/SL positioning request to the selected LMF or SL Positioning Server UE by including only the identities of UE2/../UEn returning positive privacy check results (step #6 of TS 23.586 [2] clauses 6.7.1.1 and 6.8). If the Client UE is not authorized as per UE privacy check, the Ranging/SL Positioning service request shall be rejected by UE1.

6.3.7 Procedure of UE privacy verification for UE-only operation

For UE-only Operation in which the network is not involved in Ranging/Sidelink positioning, the authorization for UE privacy is based on the local configured privacy verification information to determine whether its location related information can be exposed to the UE(s) indicated in the supplementary RSPP signalling message. To enable privacy check of exposure to a SL Positioning Client UE via the peer UE, the peer UE shall include the user info ID of the SL Positioning Client UE, and the user info ID of the SL Positioning Server UE if selected by the Target UE, in the supplementary RSPP signalling message to the UE from which the location information or related results are to be exposed.

In case of n UEs involved in UE-only operation as in TS 23.586 [2] clause 6.8, if none of the n UEs grants permission for exposure, the UE1 shall reject the Ranging/SL Positioning service request. If all of the n UEs grant permission for exposure, the UE1 shall proceed with the Ranging/SL positioning service request. If part of the n UEs return positive privacy check results and part of the n UEs return negative privacy check results, UE1 shall determine to accept or reject the service request based on the privacy check results of the n UEs and a criterion up to UE implementation (e.g. a rule from application layer).

UE privacy check against SL Positioning Server UE only applies to UE-only operation, and is performed only when the Server UE is selected by the Target UE (as per clause 6.8 step 5 in TS 23.586 [2]). The SL Positioning Server UE may be reselected based on the privacy check results of the Target/Reference UEs.

If the privacy verification information allows location exposure, the UE (e.g. Located UE) accepts the request to expose its location related information and proceeds. If the privacy verification information disallows location exposure, the UE shall return privacy check reject message.

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) between the UEs and between the UE and LMF for Ranging/SL Positioning.

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 6.20 of TS 23.273 [3].

NOTE: The Ranging/SL Positioning Protocol (RSPP) includes Sidelink Positioning Protocol (SLPP) defined in TS 38.355 [7], Supplementary Service messages defined in TS 24.080 [13] and Supplementary RSPP signalling messages defined in TS 24.514 [14].

6.4.2 Security requirements

The 5G system shall support mutually authentication between the UEs during unicast direct communication establishment for Ranging/SL Positioning control over RSPP.

The 5G 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 5G 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 5G 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.

The 5G system shall support a means to configure PC5 security policies to the UE for Ranging/SL positioning services.

SR5 signalling integrity protection policy is configured to "REQUIRED" for Ranging/SL positioning services.

The 5G system shall support a means to provide confidentiality, integrity and anti-replay protection of SL positioning broadcast/groupcast signalling.

The 5G system shall provide a means to mitigate trackability and linkability attacks of the UE during SL Positioning broadcast/ groupcast signalling procedures.

NOTE: SL Positioning broadcast/groupcast signalling procedures are not supported.

6.4.3 Security procedures 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 (e.g. 5GC-MO-LR and 5GC-MT-LR services using SL positioning as defined in TS 23.586 [2] and TS 23.273 [3]), there are no long-term credentials provided by applications on the UE (e.g. Located UE). The security procedures for unicast communication for Ranging/SL Positioning services provided by application and for Ranging/SL Positioning services provided by network are specified separately in subclauses 6.4.3.2 and 6.4.3.3.

6.4.3.2 Unicast direct communication for Ranging/SL Positioning services provided application

If long-term credentials provided by application 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.

6.4.3.3 Unicast direct communication for Ranging/SL Positioning services provided by network

For Ranging/SL Positioning services provided by network operators, the network shall support key provisioning and management for unicast direct communication. The security procedures defined for 5G ProSe UE-to-Network Relay communication in clause 6.3.3.2 of TS 33.503 [6] are reused with the following modifications:

- The SLPKMF instead of 5G PKMF is used to generate and provision the key materials for secure unicast direct communication of Ranging/SL Positioning services.
- UE SLP Key Request/Response are used instead of ProSe Remote User Key Request/Response.
- Ranging/SL Positioning Application Identifier is used instead of RSC.
- SLPK and SLPK ID are used instead of UP-PRUK and UP-PRUK ID.
- SLP Key Request/Response are used instead of Key Request/Response.
- K_{SLP} is used instead of K_{NRP}.
- KDF of K_{SLP} as defined in clause A.2 uses Ranging/SL Positioning Application Identifier as input instead of RSC.

NOTE: This procedure does not apply to V2X capable UEs.

6.4.4 Security procedure for broadcast/groupcast communication over RSPP

6.4.4.1 General

This clause describes the security mechanism for broadcast/groupcast communication over RSPP. The RSPP messages for broadcast/groupcast communication are protected at the RSPP layer.

6.4.4.2 Security flows for broadcast/groupcast communication

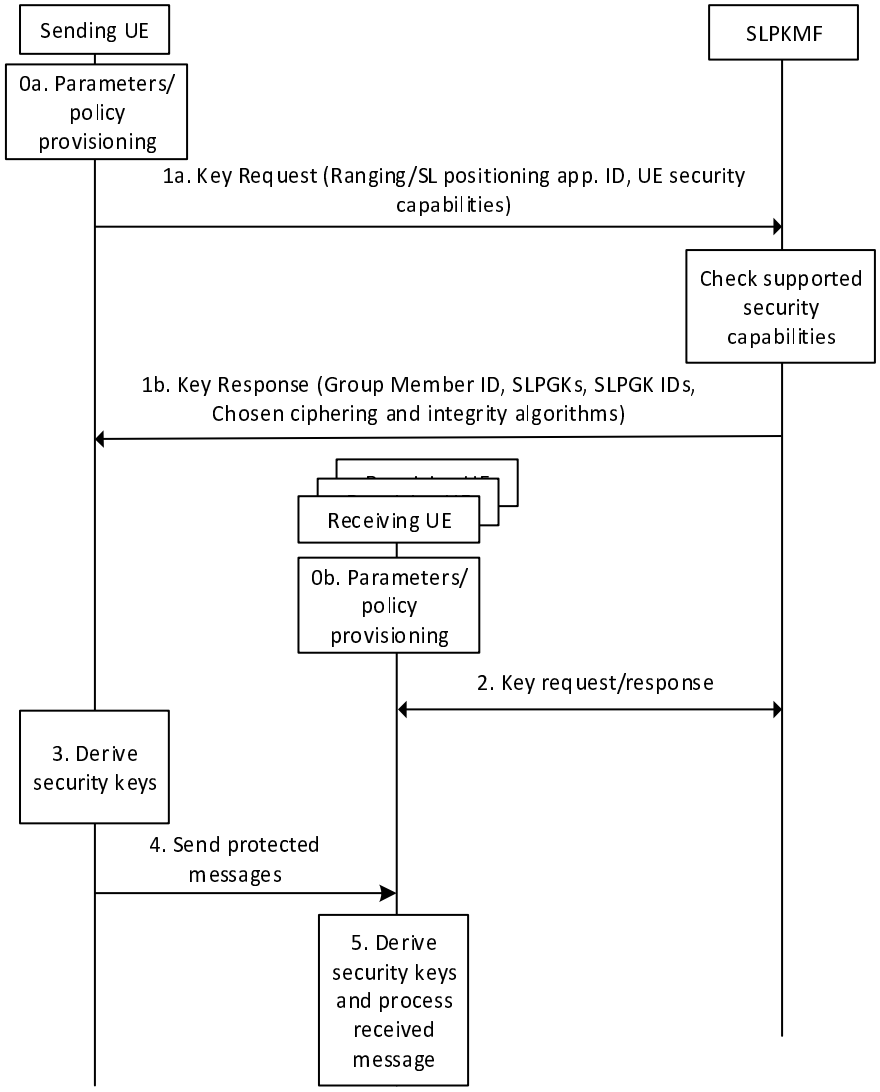

Figure 6.4.4.2-1: Security flows for broadcast/groupcast communication

0a and 0b. Both sending and receiving UEs shall be provisioned with the parameters/policy for Ranging/SL positioning service as specified in clause 5.1 of TS 23.586 [2].

1a. The sending UE shall establish a secure connection with the Sidelink Positioning Key Management Function (SLPKMF) based on the security procedures specified in clause 5.2.5 of TS 33.503 [6]. The sending UE sends a Key Request message to Sidelink Positioning Key Management Function (SLPKMF) including the Ranging/SL positioning application identifier provisioned in step 0a, and UE security capabilities.

1b. The SLPKMF shall reply with the Key Response message containing the Sidelink Positioning Group Key (SLPGK), the Sidelink Positioning Group Key ID (SLPGK ID), the validity time, and the chosen ciphering and integrity algorithms. The SLPKMF may be locally configured with the UE's authorization information. Otherwise, the SLPKMF interacts with the UDM of the UE to retrieve the UE's authorization information. The chosen ciphering and integrity algorithms are determined by SLPKMF based on the received UE security capabilities in step 1a. The Key Response message may include multiple SLPGK and SLPGK ID pairs with different validity times. Group member ID shall be assigned by the SLPKMF which is included in the Key Response message. As an alternative, the sending UE may generate a Group member ID randomly.

NOTE 1: For V2X capable UEs, the security materials (e.g. SLPGK, SLPGK ID, validity time) and the ciphering and integrity algorithms used for broadcast/groupcast communication are provisioned at the application, which is out of the scope of the present document.

NOTE 2: In case the SLPKMF of a receiving UE is different from the SLPKMF of a sending UE, the provisioning of security materials as specified in clause 6.1.3.2 in TS 33.503 [6] is reused.

NOTE 3: Sidelink Positioning Group refers to a specific Ranging/SL positioning service. Accordingly, Group member ID refers to the identifier of the UE that is authorized to use the Ranging/SL positioning service.

2. The receiving UE shall perform a Key Request procedure to get security materials from the SLPKMF as described in step 1. This may happen any time before step 5.

3. The sending UE shall derive the Sidelink Positioning Traffic Key (SLPTK) from SLPGK using Group member ID, and SLPTK ID as specified in Annex A.3 of present document. SLPTK ID is a counter set to a unique value in the sending UE that has not been previously used together with the same SLPGK and the associated SLPGK ID. The UE shall use a new SLPGK and SLPGK ID pair based on step 1 before the SLPTK ID wraps around. The UE shall calculate the Sidelink Positioning Encryption Key (SLPEK) and Sidelink Positioning Integrity Key (SLPIK) from SLPTK using the chosen ciphering and integrity algorithms, respectively as specified in Annex A.4 of present document.

4. The sending UE shall protect the message as described in clause 6.4.4.3.1 and send the message.

5. Upon receiving the message matching the SLPGK ID, the receiving UE shall calculate SLPTK, SLPEK and SLPIK if it has not calculated them. The receiving UE derives security keys as in step 3 using the SLPGK ID, SLPTK ID and Group member ID (if it is included) in the received message. Then, the UE shall decrypt the message and verifies the integrity of the message as described in clause 6.4.4.3.2.

6.4.4.3 Protection of messages between UEs

6.4.4.3.1 Message processing in the sending UE

The UE sending a message shall construct the message as follows:

1) Form RSPP message header that contains Group member ID, SLPGK ID, SLPTK ID, and a counter. Then, append the Payload to it as illustrated in figure 6.4.4.3.1-1. The counter is used in combination with the selected ciphering algorithm and integrity algorithm.

NOTE 1: The counter can be a time counter.

2. If the chosen integrity algorithm is not the NULL algorithm, calculate MAC of the message header and the Payload based on the chosen integrity algorithm. If the chosen algorithm is the NULL algorithm, then the sending UE shall set the MAC to a 32-bit random string or all zeros in the message header. The use and mode of operation of the chosen integrity algorithm are specified in Annex D of TS 33.501 [11].

3. If the chosen ciphering algorithm is not the NULL algorithm, encrypt the Payload and MAC based on the chosen ciphering algorithm. The use and mode of operation of the chosen ciphering algorithm are specified in Annex D of TS 33.501 [11].

In case the Group member ID is provided by the SLPKMF, multiple Group member IDs can be provisioned for privacy. If multiple Group member IDs are provisioned by the SLPKMF or Group member IDs are self-generated, the sending UE shall change its Group member ID according to its policy.

NOTE 2: Additional procedures to mitigate trackability/linkability attacks may apply to Group member ID, SLPGK ID, SLPTK ID, and Counter.

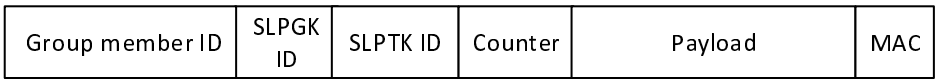

Figure 6.4.4.3.1-1: RSPP message format for Sidelink Positioning broadcast/groupcast communication

6.4.4.3.2 Protected message processing in the receiving UE

The UE receiving a message shall do the following steps:

1. If the chosen ciphering algorithm is not the NULL algorithm, undo confidentiality protection based on the chosen ciphering algorithm.

2. If the chosen integrity algorithm is not the NULL algorithm, verify the integrity of the received message by checking MAC based on the chosen integrity algorithm. The message with MAC part filled with all zeroes is discarded.

NOTE: Freshness verification may be required.

6.4.4.4 Key hierarchy for broadcast/groupcast protection communication over RSPP

The key hierarchy for broadcast/groupcast communication over RSPP follows the key hierarchy for one-to-many ProSe direct communication as specified in TS 33.303 [9]. The different layers of keys (see figure 6.4.4.4-1) are the following:

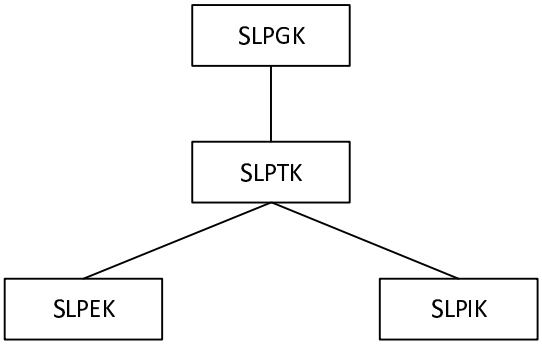

Figure 6.4.4.4-1: Key hierarchy for broadcast/groupcast communication over RSPP

- SLPGK: SL Positioning Group Key is a 256-bit root key specific to a Ranging/SL positioning application (for broadcast) or group (for groupcast) provisioned with an expiry time. Each SLPGK has an SLPGK ID to identify it. This allows several SLPGKs to be held simultaneously for one Ranging/SL positioning application (for broadcast) or Ranging/SL positioning group (for groupcast). SLPGK may either be provisioned by the SLPKMF to the UE or be derived by the UE from locally configured long-term credentials.

- SLPTK: SL Positioning Traffic Key is a 256-bit intermediate key derived by the UE from SLPGK. It is unique per UE to ensure that each UE generates unique SLPTKs for protecting the messages it sends. Each SLPTK has a 16-bit SLPTK ID to identify it. SLPTK ID is a counter in the UE set to a unique value that has not been previously used together with the same SLPGK and associated SLPGK ID. Every time a new SLPTK needs to be derived, the SLPTK ID counter is incremented.

- SLPEK and SLPIK: The SL Positioning Encryption Key (SLPEK) and SL Positioning Integrity Key (SLPIK) are derived by the UE from SLPTK and used as broadcast/groupcast keys to protect the integrity and confidentiality of RSPP messages for Sidelink Positioning broadcast/groupcast communication respectively.

6.4.5 Security procedure for communication between the UE and LMF

The communication for Ranging/SL Positioning control between the UE and LMF is protected by using NAS security context created for the UE.

7 Security related services

7.1 General

This clause defines the network services required to support the security procedures described in clause 6.

7.2 SLPKMF services

7.2.1 General

The following table illustrates the SLPKMF Services and Service Operations.

Table 7.2.1-1: List of SLPKMF Services

Service	Service Operations	Operation Semantics	Example Consumer(s)
Nslpkmf_Discovery	AnnounceAuthorize	Request/Response	SLPKMF
	MonitorAuthorize	Request/Response	SLPKMF
	DiscoveryAuthorize	Request/Response	SLPKMF
Nslpkmf_SLPKMFKeyRequest	UnicastKey	Request/Response	SLPKMF
	GroupcastKey	Request/Response	SLPKMF

7.2.2 Nslpkmf_Discovery service

7.2.2.1 Nslpkmf_Discovery_AnnounceAuthorize service operation

Service operation name: Nslpkmf_Discovery_AnnounceAuthorize.

Description: The consumer NF obtains the authorization from the SLPKMF for announcing in the PLMN.

Input, Required: User Info ID, Ranging/SL Positioning Application Identifier, UE Role.

Input, Optional: None.

Output, Required: Authorization result.

Output, Optional: None.

7.2.2.2 Nslpkmf_Discovery_MonitorAuthorize service operation

Service operation name: Nslpkmf_Discovery_MonitorAuthorize.

Description: The consumer NF obtains the authorization from the SLPKMF for monitoring in the PLMN.

Input, Required: User Info ID, Ranging/SL Positioning Application Identifier, UE Role, PC5 UE security capability.

Input, Optional: None.

Output, Required: The chosen PC5 ciphering algorithm, discovery security materials.

Output, Optional: Discovery User Integrity Key (DUIK).

7.2.2.3 Nslpkmf_Discovery_DiscoveryAuthorize service operation

Service operation name: Nslpkmf_Discovery_DiscoveryAuthorize.

Description: The consumer NF obtains the authorization from the SLPKMF for a discoverer UE in the PLMN to operate Model B restricted discovery.

Input, Required: User info ID, Ranging/SL Positioning Application Identifier, UE Role, PC5 UE security capability.

Input, Optional: None.

Output, Required: The chosen PC5 ciphering algorithm, discovery security materials.

Output, Optional: Discovery User Integrity Key (DUIK).

7.2.3 Nslpkmf_SLPKMFKeyRequest service

7.2.3.1 Nslpkmf_SLPKMFKeyRequest_UnicastKey service operation

Service operation name: Nslpkmf_SLPKMFKeyRequest_UnicastKey.

Description: Provides Ranging related keying material for unicast communication.

Input, Required: Ranging/SL Positioning Application Identifier, SLPK ID, K_{SLP} freshness parameter 1.

Input, Optional: None.

Output, Required: K_{SLP}, K_{SLP} freshness parameter 2.

Output, Optional: None.

7.2.3.2 Nslpkmf_SLPKMFKeyRequest_GroupcastKey service operation

Service operation name: Nslpkmf_SLPKMFKeyRequest_GroupcastKey.

Description: Provides Ranging related keying material for groupcast communication.

Input, Required: SLPGK ID, Group Identifier.

NOTE: For broadcast operation, Ranging/SL Positioning Application Identifier is used as the Group Identifier.

Input, Optional: None.

Output, Required: SLPGK.

Output, Optional: None.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

A.1.1 General

This annex specifies the use of the Key Derivation Function (KDF) specified in TS 33.220 [12] for the present document. This annex specifies how to construct the input string, S, and the input key KEY to the KDF. Note that "KEY" is denoted "Key" in TS 33.220 [12].

A.1.2 FC value allocations

The FC number space used is allocated as per B.2.2 of TS 33.220 [12].

A.2 Calculation of K_{SLP}

When calculating K_{SLP} from SLPK, the following parameters shall be used to form the input S to the KDF specified in Annex B of TS 33.220 [12]:

- FC = 0x8C
- P0 = Ranging/SL Positioning Application Identifier
- L0 = length of Ranging/SL Positioning Application Identifier (i.e. 0x00 0x03)
- P1 = K_{SLP} nonce 1
- L1 = length of K_{SLP} nonce 1 (i.e. 0x00 0x10)
- P2 = K_{SLP} nonce 2
- L2 = length of K_{SLP} nonce 2 (i.e. 0x00 0x10)

The input key to the KDF is the 256-bit SLPK.

A.3 Calculation of SLPTK

When calculating a SLPTK from SLPGK, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0x8D
- P0 = Group Member Identity
- L0 = length of Group Member Identity
- P1 = SLPTK Identity
- L1 = length of SLPTK Identity

The input key shall be the 256-bit SLPGK.

A.4 Calculation of keys from SLPTK

When calculating a SLPIK or SLPEK from SLPTK, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0x8E
- P0 = 0x00 if SLPEK is being derived or 0x01 if SLPIK is being derived
- L0 = length of P0 (i.e. 0x00 0x01)
- P1 = algorithm identity
- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm identity shall be set as described in TS 33.501 [11].

The input key shall be the 256-bit SLPTK.

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

Annex B (normative): UE privacy profile for Ranging/SL Positioning service

The UE LCS Privacy Profile defined in clause 5.4.2 of TS 23.273 [3] is taken as the baseline for the UE Ranging/SL Positioning privacy profile with the following modifications:

- UE Ranging/SL Positioning privacy profile is part of subscription data for UEs subscribed to use Ranging/SL positioning services.
- UE Ranging/SL Positioning privacy profile is used to indicate whether Ranging/SL positioning service exposure to 5GC NF, AF, LCS Client is allowed or disallowed.
- Privacy Override Indicator (POI) is used to determine whether the UE Ranging/SL positioning privacy profile of the subscriber to be positioned shall be overridden by the request for regulatory services. The assignment of a POI value is appliable to LCS client, same as specified in TS 23.273 [3].
- The list of external LCS client in UE LCS privacy profile is replaced by the list of zero or more AFs/LCS Clients.- The list of LCS client in UE LCS privacy profile is replaced by the list of zero or more 5GC NF or LCS client.
- The list of service type in UE LCS privacy profile is replaced by the list of Ranging/SL Positioning Application Identifier.

The UE Ranging/SL Positioning privacy profile data is defined in table B-1.

Table B-1: Ranging/SL Positioning privacy profile data stored in the UDM for a UE Subscriber

Privacy Profile Data Type	Presence	UDM data
Ranging/SL Positioning Privacy Indication	M O	Indication of one of the following mutually exclusive global settings: - Ranging/SL Positioning services is disallowed - Ranging/SL Positioning services is allowed (default) Time period when the Ranging/SL Positioning Privacy Indication is valid

Call/session Unrelated Class	M
	
	O
	
	O
	O
	O
	
	O
	
	O
	
	O
	O
	
	O
	
	O
	
	O
	O
	
	O
		For any AF or LCS Client not in the AF/LCS Client list or otherwise identified for the Call/session Unrelated Class, the following data may be present:
		- One of the following mutually exclusive options:
		  - Ranging/SL positioning result not allowed (default case)
		  - Ranging/SL positioning result allowed with notification
		  - Ranging/SL positioning result allowed without notification.
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning allowed if no response
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning restricted if no response
		- Time period when Ranging/SL positioning is allowed
		- Geographical area where Ranging/SL positioning is allowed
		- Indication that codeword shall be checked in UE or one or more codeword values to be checked in GMLC
		
		AF/LCS Client list: a list of zero or more AFs/LCS Clients with the following data for each entry:
		- One of the following mutually exclusive options:
		  - Ranging/SL positioning result allowed without notification (default case)
		  - Ranging/SL positioning result allowed with notification
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning allowed if no response
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning restricted if no response
		- Time period when Ranging/SL positioning is allowed
		- Geographical area where Ranging/SL positioning is allowed
		
		Ranging/SL Positioning Application Identifier list: a list of one or more Ranging/SL Positioning Application Identifiers for which the Ranging/SL Positioning application is allowed to range/locate the particular UE. The following data may be present for each Ranging/SL Positioning Application Identifier in the list:
		- One of the following mutually exclusive options:
		  - Ranging/SL positioning result allowed without notification (default case)- Ranging/SL positioning result allowed with notification
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning allowed if no response
		  - Ranging/SL positioning result with notification and privacy verification; Ranging/SL positioning restricted if no response
		- Time period when Ranging/SL positioning is allowed
		- Geographical area where Ranging/SL positioning is allowed
		- Indication that codeword shall be checked in UE or one or more codeword values to be checked in GMLC

PLMN Operator Class	O	NF/LCS Client list: a list of one or more generic classes of 5GC NF/LCS client that are allowed to perform Ranging/SL positioning on the particular UE. The following classes are distinguished: - LCS client broadcasting location related information - O&M LCS client in the HPLMN - O&M LCS client in the VPLMN - LCS client recording anonymous location information - LCS Client supporting a bearer service, teleservice or supplementary service to the target UE - NWDAF in the HPLMN (when the UE is currently being served by the HPLMN) - NWDAF in the VPLMN
Event report expected area	O	Presents a geographical area generated by UE, which is used by GMLC to determine event report allowed area for the UE

Annex C (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2023-09	SA#101	SP-230868				Presented for information and approval	1.0.0
2023-09	SA#101					EditHelp review and upgrade to change control version	18.0.0
2023-12	SA#102	SP-231336	0001	-	F	Update the FC Value in 33.533	18.1.0
2023-12	SA#102	SP-231336	0003	1	F	Resolve the issue when SLPTK ID is about to wrap around	18.1.0
2023-12	SA#102	SP-231336	0004	1	F	Update the abbreviations in 33.533	18.1.0
2023-12	SA#102	SP-231336	0009	-	F	Rel18 SL positioning - Updates on unicast direct communication security	18.1.0
2023-12	SA#102	SP-231336	0017	-	F	Update to the Reference Points in Clause 4.2.2	18.1.0
2023-12	SA#102	SP-231336	0018	-	F	Update to Common Security in Clause 5	18.1.0
2023-12	SA#102	SP-231336	0019	1	F	Add differences between Ranging discovery and ProSe discovery	18.1.0
2023-12	SA#102	SP-231336	0020	-	F	Update to failure handling for authorization of UE role included in DCR	18.1.0
2023-12	SA#102	SP-231336	0021	1	F	Update to AF authorization procedure for Ranging/SL positioning service exposure	18.1.0
2023-12	SA#102	SP-231336	0022	1	F	Add privacy handing for Ranging/SL positioning service exposure through 5GC CP	18.1.0
2023-12	SA#102	SP-231336	0025	1	F	Update to the title for unicast direct communication with long-term credential	18.1.0
2023-12	SA#102	SP-231336	0031	-	F	Clarification on the Ranging/SL Positioning service exposure	18.1.0
2024-03	SA#103	SP-240358	0051	1	F	Update on UE role authorization during discovery	18.2.0
2024-03	SA#103	SP-240498	0055	4	F	Clarification on the UE Ranging/SL Positioning privacy profile	18.2.0
2024-03	SA#103	SP-240358	0056	1	F	Clarification on the procedure of UE privacy check	18.2.0
2024-03	SA#103	SP-240358	0057	1	F	UE Privacy handling for service exposure through PC5	18.2.0
2024-03	SA#103	SP-240358	0064	1	F	PC5 security policy for Ranging/SL positioning service	18.2.0
2024-03	SA#103	SP-240358	0065	1	F	Adding notes for Ranging/SL positioning broadcast/groupcast communication	18.2.0
2024-03	SA#103	SP-240358	0066	1	F	Clean up of TS 33.533	18.2.0
2024-03	SA#103	SP-240472	0067	1	F	Remove authorization procedure for Ranging/SL Positioning service exposure through 5GC	18.2.0
2024-07	SA#104	SP-240671	0068	-	F	Implementing CR to TS 33.533 agreed in SA plenary in SP-240498	18.3.0
2024-07	SA#104	SP-240671	0071	1	F	Update to UE Privacy Verification for UE-only Operation	18.3.0
2024-07	SA#104	SP-240671	0072	1	F	PC5-U integrity protection policy for Ranging/SL positioning service	18.3.0
2024-07	SA#104	SP-240671	0073	1	F	Updating RSPP broadcast/groupcast to SLPP broadcast/groupcast	18.3.0
2024-07	SA#104	SP-240671	0074	1	F	Update on UE role authorization during discovery	18.3.0
2024-09	SA#105	SP-241101	0076	1	F	Completing the Privacy Check of n UEs for Service Exposure to Client UE	18.4.0

History

Document history		
V18.2.0	May 2024	Publication
V18.3.0	July 2024	Publication
V18.4.0	October 2024	Publication