ETSI TS 129 586 V18.0.0 (2024-05)

5G;
5G System;
SideLink Positioning Key Management Services;
Stage 3
(3GPP TS 29.586 version 18.0.0 Release 18)

Reference
DTS/TSGC-0429586vi00

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 the 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.1.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 stage 3 protocol and data model for the Nslpkmf Service Based Interface to support ranging based service and sidelink positioning in 5G system. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the SLPKMF as specified in 3GPP TS 33.533 [2].

The 5G System stage 2 architecture and procedures for ranging based service and sidelink positioning are specified in 3GPP TS 23.586 [3].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in 3GPP TS 29.500 [5] and 3GPP TS 29.501 [4].

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 33.533: "Security aspects of ranging based services and sidelink positioning".

[3] 3GPP TR 23.586: " Ranging based services and Sidelink Positioning ".

[4] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

[6] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[7] OpenAPI : "OpenAPI Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0.

[8] IETF RFC 9113: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[9] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[10] IETF RFC 9457: "Problem Details for HTTP APIs".

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

[12] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[13] 3GPP TS 29.510: "Network Function Repository Services; Stage 3".

[14] 3GPP TR 21.900: "Technical Specification Group working methods".

[15] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[16] 3GPP TS 24.554: "Proximity-services (ProSe) in 5G System (5GS) protocol aspects; Stage 3".

[17] 3GPP TS 24.514: "Ranging based services and sidelink positioning in 5G system(5GS); Stage 3".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

SLPKMF SideLink Positioning Key Management Function

4 Overview

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 and sidelink positioning services, including:

- the key management and the security material for the UE discovery for ranging and sidelink positioning.
- the key management for secure unicast direct link establishment between the UEs for ranging and sidelink positioning services provided by network.
- the key management for protection of SLPP signalling broadcast/groupcast.

Figure 4-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the SLPKMF:

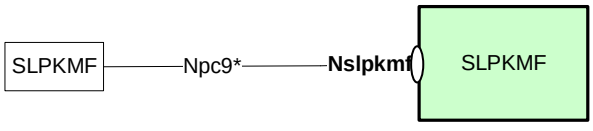

Figure 4-1: Reference model – SLPKMF

The functionalities supported by the SLPKMF are listed in clause 4.2 of 3GPP TS 33.533 [2].

5 Services offered by the SLPKMF

5.3 Introduction

The Table 5.3-1 shows the SLPKMF Services and SLPKMF Service Operations:

Table 5.31-1: 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

Table 5.31-2 summarizes the corresponding APIs defined for this specification.

Table 5.31-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Nslpkmf_Discovery	6.1	PKMF Discovery Service	TS29xxx_Nslpkmf_Discovery.yaml	Nslpkmf-disc	A.2
Nslpkmf_SLPKMFKeyRequest	6.2	SLPKMF Key Request Service	TS295xx_Nslpkmf_SLPKMFKeyRequest.yaml	nslpkmf-keyrequest	A.3

5.2 Nslpkmf_Discovery Service

5.2.1 Service Description

This service enables an NF (i.e. another SLPKMF in another PLMN) to request authorization information. The following are the key functionalities of this NF service.

- Provide the authorization from the SLPKMF for announcing in the PLMN
- Provide the discovery key from the SLPKMF for monitoring in the PLMN
- Provide the discovery key from the SLPKMF for a discoverer UE in the PLMN to operate Model B restricted discovery

5.2.2.1 Introduction

The Nslpkmf_Discovery service supports following service operations:

- AnnounceAuthorize
- MonitorAuthorize
- DiscoveryAuthorize

5.2.2.2 AnnounceAuthorize

5.2.2.2.1 General

The AnnounceAuthorize service operation is invoked by a NF Service Consumer, i.e. another SLPKMF in another PLMN, towards the SLPKMF to retrieve the authorization from the SLPKMF for announcing in the PLMN.

The NF Service Consumer (e.g., SLPKMF) shall request the SLPKMF to get authorization as shown in Figure 5.2.2.2.1-1

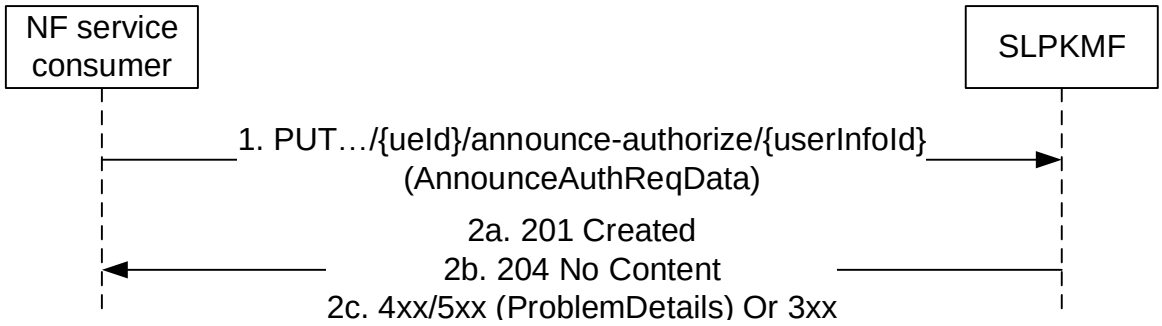

Figure 5.2.2.2.1-1: Announce Authorize

1. The NF service consumer (e.g., SLPKMF) sends a HTTP PUT request to the resource representing the announce-authorize custom operation. The request body shall contain the ranging and sidelink positioning application identifier and UE role.

2a. If the context indicated by the userInfoId doesn't exist, the SLPKMF shall create the new resource, and upon success of creation of the resource, "201 created" shall be returned.

2b. If the context indicated by the userInfoId already exists, the SLPKMF shall replace the stored data using the received data, and upon success of the update of the resource, "204 No Content" shall be returned.

2c. On failure or redirection, one of the HTTP status code listed in Table 6.1.3.2.3.1-3 may be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.2.3.1-3.

5.2.2.3 MonitorAuthorize

5.2.2.3.1 General

The MonitorAuthorize service operation is invoked by a NF Service Consumer, i.e. another SLPKMF in another PLMN, towards the SLPKMF to retrieve the discovery key from the SLPKMF for monitoring in the PLMN.

The NF Service Consumer (e.g., SLPKMF) shall request the SLPKMF to get authorization as shown in Figure 5.2.2.3.1-1

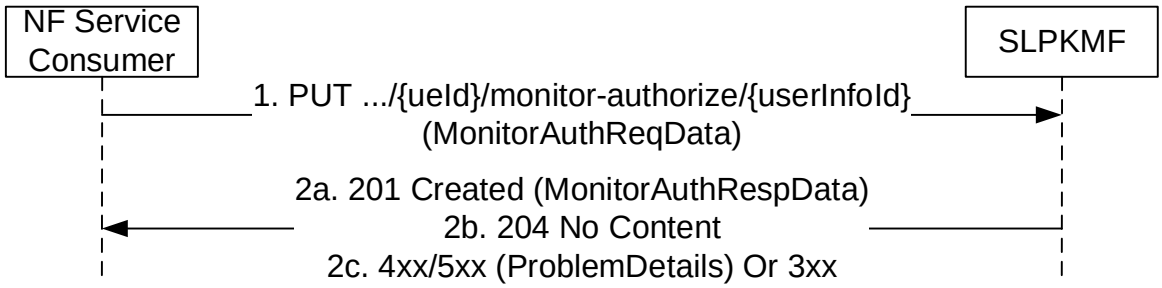

Figure 5.2.2.3.2-1: Monitor Authorize

1. The NF Service Consumer (e.g., SLPKMF) shall send an HTTP PUT request to the resource representing the monitor-authorize custom operation. The request body shall contain the ranging and sidelink positioning application identifier, UE role and PC5 UE security capability.

2a. If the context indicated by the userInfoId doesn't exist, the SLPKMF shall create the new resource, and upon success of creation of the resource, "201 created" shall be returned.

2b. If the context indicated by the userInfoId already exists, the SLPKMF shall replace the stored data using the received data, and upon success of the update of the resource, "204 No Content" shall be returned.

2c. On failure or redirection, one of the HTTP status code listed in Table 6.1.3.3.3.1-3 may be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.3.3.1-3.

5.2.2.4 DiscoveryAuthorize

5.2.2.4.1 General

The DiscoveryAuthorize service operation is invoked by a NF Service Consumer, i.e. another SLPKMF in another PLMN, towards the SLPKMF to retrieve the discovery key from the SLPKMF for a discoverer UE in the PLMN to operate Model B restricted discovery.

The NF Service Consumer (e.g., SLPKMF) shall request the SLPKMF to get authorization as shown in Figure 5.2.2.4.1-1

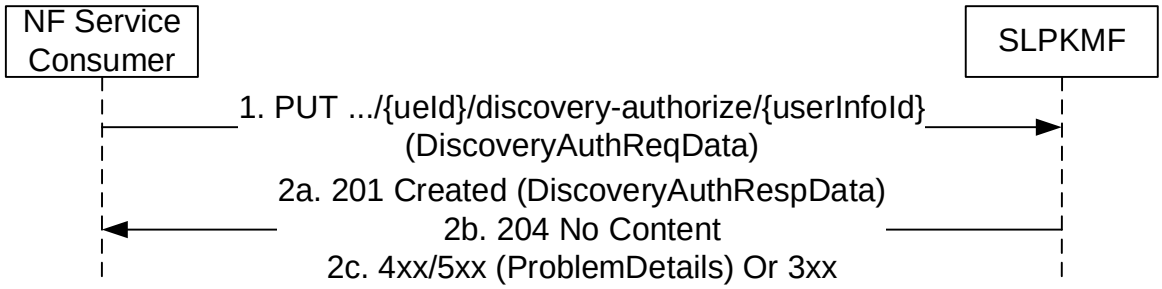

Figure 5.2.2.4.1-1: Discover Authorize

1. The NF Service Consumer (e.g., SLPKMF) shall send an HTTP PUT request to the resource representing the monitor-authorize custom operation. The request body shall contain the ranging and sidelink positioning application identifier, UE role and PC5 UE security capability.

2a. If the context indicated by the userInfoId doesn't exist, the SLPKMF shall create the new resource, and upon success of creation of the resource, "201 created" shall be returned.

2b. If the context indicated by the userInfoId already exists, the SLPKMF shall replace the stored data using the received data, and upon success of the update of the resource, "204 No Content" shall be returned.

2c. On failure or redirection, one of the HTTP status code listed in Table 6.1.3.3.3.1-3 may be returned. For a 4xx/5xx response, the message body may contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.3.3.3.1-3.

5.3 Nslpkmf_SLPKMFKeyRequest Service

5.3.1 Service Description

This service enables an NF (i.e. another SLPKMF in another PLMN) to request ranging related keying material. The following are the key functionalities of this NF service.

- Provide ranging related keying material for unicast communication

5.3.2 Service Operations

5.3.2.1 Introduction

5.3.2.2 UnicastKey

5.3.2.2.1 General

The UnicastKey service operation is invoked by a NF Service Consumer, i.e. another SLPKMF in another PLMN, towards the SLPKMF to retrieve the keying material related to ranging.

The UnicastKey service operation is used during the following procedure:

- Unicast direct communication for ranging and sidelink positioning services provided by network (see 3GPP TS 33.533 [4], clause 6.4.3.3)

The NF Service Consumer (i.e. another SLPKMF in another PLMN) shall retrieve the ranging related keying material by invoking the "request " custom method on the resource URI of "Ranging Keys Collection" resource, see clause 6.2.3.2.4. See also Figure 5.3.2.2.1-1.

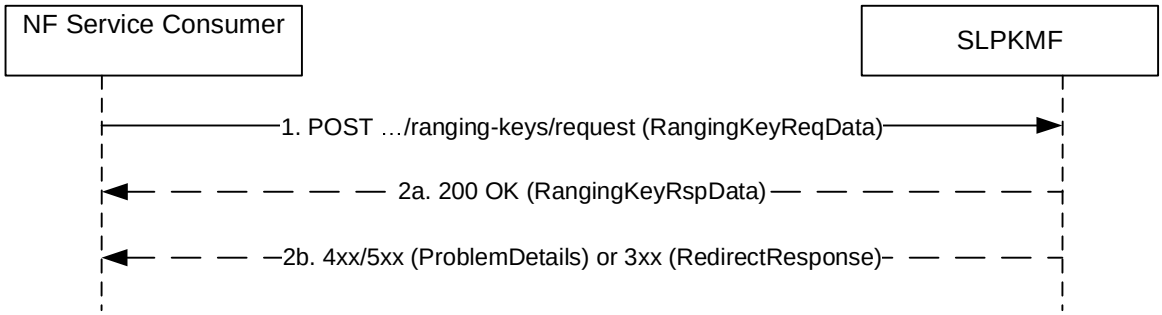

Figure 5.3.2.2.1-1 UnicastKey service operation

1. The NF Service Consumer shall send a HTTP POST request to invoke "request" custom method. The payload of the request shall be an object of "UnicastKeyReqData" data type. The payload shall include the ranging and sidelink positioning application identifier, the KSLP freshness parameter 1, and the SLPK ID.

2a. On success, the SLPKMF shall respond with the status code "200 OK". The payload of the response shall be an object of "UnicastKeyRspData" data type. They payload shall include the KSLP and the KSLP freshness parameter 2.

2b. On failure or redirection, one of the HTTP status codes listed in Table 6.2.3.2.4.2.2-2 shall be returned. For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application errors listed in Table 6.2.3.2.4.2.2-2.

6 API Definitions

6.1 Nslpkmf_Discovery Service API

6.1.1 Introduction

The Nslpkmf_Discovery shall use the Nslpkmf_Discovery API.

The API URI of the Nslpkmf_Discovery API shall be:

{apiRoot}/<apiName>/<apiVersion>

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [6], i.e.:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The <apiName> shall be "Nslpkmf-discovery".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.1.3.

6.1.2 Usage of HTTP

6.1.2.1 General

HTTP/2, IETF RFC 9113 [8], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [7] specification of HTTP messages and content bodies for the Nslpkmf_Discovery API is contained in Annex A.

6.1.2.2 HTTP standard headers

6.1.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

6.1.2.2.2 Content type

JSON, IETF RFC 8259 [9], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 9457 [10].

6.1.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be applicable, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

6.1.3 Resources

6.1.3.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 6.1.3.1-1 describes the resource URI structure of the Nslpkmf_Discovery API.

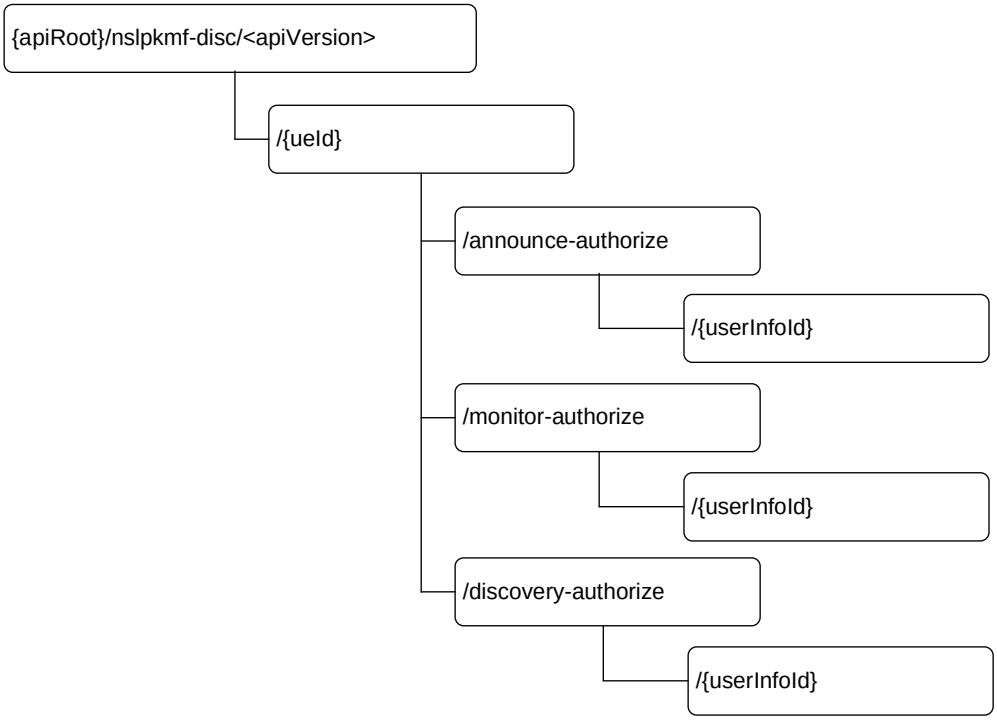

Figure 6.1.3.1-1: Resource URI structure of the Nslpkmf_Discovery API

Table 6.1.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.1.3.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
AnnounceAuthorize	/{ueId}/announce-authorize/{userInfoId}	PUT	Obtain the authorization from the SLPKMF for announcing in the PLMN
MonitorAuthorize	/{ueId}/monitor-authorize/{userInfoId}	PUT	Obtain the discovery key from the SLPKMF for monitoring in the PLMN
DiscoveryAuthorize	/{ueId}/discovery-authorize/{userInfoId}	PUT	Obtain the discovery key from the SLPKMF for a discoverer UE in the PLMN to operate Model B restricted discovery

6.1.3.2 Resource: AnnounceAuthorize

6.1.3.2.1 Description

6.1.3.2.2 Resource Definition

Resource URI: **{apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/announce-authorize/{userInfoId}**

This resource shall support the resource URI variables defined in Table 6.1.3.2.2-1.

Table 6.1.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1
ueId	VarUeId	Represents the Subscription Identifier SUPI or GPSI (see 3GPP TS 23.501 [2] clause 5.9.2) pattern: See pattern of type VarUeId in 3GPP TS 29.571 [15]
userInfoId	UserInfoId	Represents User Info Id.

6.1.3.2.3 Resource Standard Methods

6.1.3.2.3.1 PUT

This method shall support the URI query parameters specified in Table 6.1.3.2.3.1-1.

Table 6.1.3.2.3.1-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in Table 6.1.3.2.3.1-2 and the response data structures and response codes specified in Table 6.1.3.2.3.1-3.

Table 6.1.3.2.3.1-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
AnnounceAuthData	M	1	Contains the Announce Authorization Data for the indicated UE and indicated user info id.

Table 6.1.3.2.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AnnounceAuthData	M	1	201 Created	Upon success of creation of the resource, a response body shall be returned. The HTTP response shall include a "Location" HTTP header that contains the resource URI of the created resource.
n/a			204 No Content	Upon success of the update of the resource, an empty response body shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 1)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	The "cause" attribute may be used to indicate one of the following application errors: - RANGINGSL_SERVICE_UNAUTHORIZED See Table 6.1.7.3-1 for the description of these errors.
NOTE 1: The manadatory HTTP error status code for the PUT method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/announce-authorize/{userInfoId}

Table 6.1.3.2.3.1-5: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

Table 6.1.3.2.3.1-6: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

6.1.3.3 Resource: MonitorAuthorize

6.1.3.3.1 Description

This resource represents the Monitor Key.

6.1.3.3.2 Resource Definition

Resource URI: **{apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/monitor-authorize/{userInfoId}**

This resource shall support the resource URI variables defined in Table 6.1.3.3.2-1.

Table 6.1.3.3.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1
ueId	VarUeId	Represents the Subscription Identifier SUPI or GPSI (see 3GPP TS 23.501 [2] clause 5.9.2) pattern: See pattern of type VarUeId in 3GPP TS 29.571 [15]
userInfoId	UserInfoId	Represents User Info Id.

6.1.3.3.3 Resource Standard Methods

6.1.3.3.3.1 PUT

This method shall support the URI query parameters specified in Table 6.1.3.3.3.1-1.

Table 6.1.3.3.3.1-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in Table 6.1.3.3.3.1-2 and the response data structures and response codes specified in Table 6.1.3.3.3.1-3.

Table 6.1.3.3.3.1-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
MonitorAuthReqData	M	1	Contains the Monitor Key Data for the indicated UE and indicated user info id.

Table 6.1.3.3.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MonitorAuthRespData	M	1	201 Created	Upon success of creation of the resource, a response body containing a representation of the discovery key data to monitor for the UE shall be returned. The HTTP response shall include a "Location" HTTP header that contains the resource URI of the created resource.
n/a			204 No Content	Upon success of the update of the resource, an empty response body shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 1)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	The "cause" attribute may be used to indicate one of the following application errors: - RANGINGSL_SERVICE_UNAUTHORIZED See Ttable 6.1.7.3-1 for the description of these errors.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - APPLICATION_NOT_FOUND See Table 6.1.7.3-1 for the description of these errors.
NOTE 1: The manadatory HTTP error status code for the PUT method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.3.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/monitor-authorize/{userInfoId}

Table 6.1.3.3.3.1-5: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

Table 6.1.3.3.3.1-6: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

6.1.3.4 Resource: DiscoveryAuthorize

6.1.3.4.1 Description

This resource represents the Discovery Key.

6.1.3.4.2 Resource Definition

Resource URI: **{apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/discovery-authorize/{userInfoId}**

This resource shall support the resource URI variables defined in Table 6.1.3.4.2-1.

Table 6.1.3.4.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1
ueId	VarUeId	Represents the Subscription Identifier SUPI or GPSI (see 3GPP TS 23.501 [2] clause 5.9.2) pattern: See pattern of type VarUeId in 3GPP TS 29.571 [15]
userInfoId	UserInfoId	Represents User Info Id.

6.1.3.4.3 Resource Standard Methods

6.1.3.4.3.1 PUT

This method shall support the URI query parameters specified in Table 6.1.3.4.3.1-1.

Table 6.1.3.4.3.1-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in Table 6.1.3.4.3.1-2 and the response data structures and response codes specified in Table 6.1.3.4.3.1-3.

Table 6.1.3.4.3.1-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
DiscoveryAuthReqData	M	1	Contains the Discovery Key Data for the indicated UE and indicated user info id.

Table 6.1.3.4.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
DiscoveryAuthRespData	M	1	201 Created	Upon success of creation of the resource, a response body containing a representation of the discovery key data for the discoverer UE in the PLMN to operate Model B restricted discovery shall be returned. The HTTP response shall include a "Location" HTTP header that contains the resource URI of the created resource.
n/a			204 No Content	Upon success of the update of the resource, an empty response body shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	The "cause" attribute may be used to indicate one of the following application errors: - RANGINGSL_SERVICE_UNAUTHORIZED See Table 6.1.7.3-1 for the description of these errors.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - APPLICATION_NOT_FOUND See Table 6.1.7.3-1 for the description of these errors.
NOTE 1: The manadatory HTTP error status code for the PUT method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.4.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/Nslpkmf-disc/<apiVersion>/{ueId}/discovery-authorize/{userInfoId}

Table 6.1.3.4.3.1-5: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

Table 6.1.3.4.3.1-6: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

6.1.4 Custom Operations without associated resources

There is no custom operation without associated resources supported in Nslpkmf_Discovery Service.

6.1.5 Notifications

There is no notification defined for Nslpkmf_Discovery service.

6.1.6 Data Model

6.1.6.1 General

This clause specifies the application data model supported by the API.

Table 6.1.6.1-1 specifies the data types defined for the Nslpkmf_Discovery service based interface protocol.

Table 6.1.6.1-1: Nslpkmf_Discovery specific Data Types

Data type	Clause defined		Description	Applicability
AnnounceAuthData	6.1.6.2.2		Represents Data used to request the authorization to announce for a UE	
MonitorAuthReqData	6.1.6.2.3		Represents Data used to request the discovery key data to monitor for a UE	
MonitorAuthRespData	6.1.6.2.4		Represents the obtained Monitor discovery key data for a UE	
DiscoveryAuthReqData	6.1.6.2.5		Represents Data used to request the discovery key data for a discoverer UE	
DiscoveryAuthRespData	6.1.6.2.6		Represents the obtained the discovery key data for a discoverer UE.	
DiscSecMaterials	6.1.6.2.7		Represents the discovery security materials	
UeSecurityCapability	6.1.6.3		Ranging and sidelink positioning UE security capability	
ChosenPc5CipheringAlgorithm	6.1.6.3		The chosen PC5 ciphering algorithm	
UeRole	6.1.6.3		Represents ranging and sidelink positioning UE role	

Table 6.1.6.1-2 specifies data types re-used by the Nslpkmf_Discovery service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nslpkmf_Discovery service based interface.

Table 6.1.6.1-2: Nslpkmf_Discovery re-used Data Types

Data type	Reference	Comments	Applicability
VarUeId	3GPP TS 29.571 [15]	String represents the SUPI or GPSI.	
ApplicationId	3GPP TS 29.571 [15]	Represents the identifier of an application.	

6.1.6.2 Structured data types

6.1.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

6.1.6.2.2 Type: AnnounceAuthData

Table 6.1.6.2.2-1: Definition of type AnnounceAuthData

Attribute name	Data type	P	Cardinality	Description	Applicability
rangingSlAppId	ApplicationId	M	1	This IE shall indicate the application identifier for ranging and sidelink positioning service.	
ueRole	UeRole	M	1	This IE shall indicate the role of the UE for ranging and sidelink positioning service.	

6.1.6.2.3 Type: MonitorAuthReqData

Table 6.1.6.2.3-1: Definition of type MonitorAuthReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
rangingSlAppId	ApplicationId	M	1	This IE shall indicate the application identifier for ranging and sidelink positioning service.	
ueRole	UeRole	M	1	This IE shall indicate the role of the UE for ranging and sidelink positioning service.	
ueSecurityCapability	UeSecurityCapability	M	1	This IE shall indicate the PC5 UE security capability for ranging and sidelink positioning sevice.	

6.1.6.2.4 Type: MonitorAuthRespData

Table 6.1.6.2.4-1: Definition of type MonitorAuthRespData

Attribute name	Data type	P	Cardinality	Description	Applicability
chosenPc5CipheringAlgorithm	ChosenPc5CipheringAlgorithm	M	1	This IE shall indicate the chosen PC5 ciphering algorithm for ranging and sidelink positioning sevice	
discSecMaterials	DiscSecMaterials	M	1	This IE shall indicate the discovery security materials	

6.1.6.2.5 Type: DiscoveryAuthReqData

Table 6.1.6.2.5-1: Definition of type DiscoveryAuthReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
rangingSlAppId	ApplicationId	M	1	This IE shall indicate the application identifier for ranging and sidelink positioning service.	
ueRole	UeRole	M	1	This IE shall indicate the role of the UE for ranging and sidelink positioning service.	
ueSecurityCapability	UeSecurityCapability	M	1	This IE shall indicate the PC5 UE security capability for ranging and sidelink positioning sevice.	

6.1.6.2.6 Type: DiscoveryAuthRespData

Table 6.1.6.2.6-1: Definition of type DiscoveryAuthRespData

Attribute name	Data type	P	Cardinality	Description	Applicability
chosenPc5CipheringAlgorithm	ChosenPc5CipheringAlgorithm	M	1	This IE shall indicate the chosen PC5 ciphering algorithm for ranging and sidelink positioning service.	
discSecMaterials	DiscSecMaterials	M	1	This IE shall indicate the discovery security materials for ranging and sidelink positioning service.	

6.1.6.2.7 Type: DiscSecMaterials

Table 6.1.6.2.7-1: Definition of type DiscSecMaterials

Attribute name	Data type	P	Cardinality	Description	Applicability
duik	Duik	O	0..1	Discovery User Integrity Key	
duck	Duck	O	0..1	Discovery User Confidentility Key	
dusk	Dusk	O	0..1	Discovery User Scrambling Key	

6.1.6.3 Simple data types and enumerations

6.1.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

6.1.6.3.2 Simple data types

The simple data types defined in Table 6.1.6.3.2-1 shall be supported.

Table 6.1.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
UserInfoId	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "User Info ID" IE as specified in 3GPP TS 24.514 [17] (starting from octet 1)	
UeSecurityCapability	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "UE security capability" IE as specified in 3GPP TS 24.514 [17] (starting from octet 1).	
ChosenPc5CipheringAlgorithm	integer	This IE shall indicate the chosen PC5 ciphering algorithm as specified in 3GPP TS 24.514 [17]	
Seckey	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUIK" IE, or "DUCK", or "DUSK" as specified in 3GPP TS 24.514 [17]	
Duik	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUIK" IE as specified in 3GPP TS 24.514 [17]	
Duck	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUCK" IE as specified in 3GPP TS 24.514 [17]	
Dusk	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUSK" IE as specified in 3GPP TS 24.514 [17]	

6.1.6.3.3 Enumeration: UeRole

The enumeration UeRole represents the different roles of UE for ranging and sidelink positioning service.

Table 6.1.6.3.28-1: Enumeration UeRole

Enumeration value	Description
"TARGET_UE"	UE as target UE for the ranging and sidelink positioning service
"REFERENCE_UE"	UE as sidelink reference UE for the ranging and sidelink positioning service
"LOCATED_UE"	UE as located UE for the ranging and sidelink positioning service
"CLIENT_UE"	UE as sidelink positioning client UE for the ranging and sidelink positioning service
"SERVER_UE"	UE as sidelink positioning server UE for the ranging and sidelink positioning service

6.1.6.4 Data types describing alternative data types or combinations of data types

There is no data type describing alternative data types or combinations of data types in Nslpkmf_Discovery Service.

6.1.6.5 Binary data

There is no binary data type in Nslpkmf_Discovery Service.

6.1.7 Error Handling

6.1.7.1 General

For the Nslpkmf_Discovery API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [6]. Protocol errors and application errors specified in Table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in Table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Nslpkmf_Discovery API.

6.1.7.2 Protocol Errors

Protocol errors handling shall be supported as specified in clause 5.2.7 of 3GPP TS 29.500 [4].

6.1.7.3 Application Errors

The application errors defined for the Nslpkmf_Discovery service are listed in Table 6.1.7.3-1.

Table 6.1.7.3-1: Application errors

Application Error	HTTP status code	Description
RANGINGSL_SERVICE_UNAUTHORIZED	403 Forbidden	It is used when the requested ProSe service, which is a ranging and sidelink positioning service, is not authorized for this UE Identity.
APPLICATION_NOT_FOUND	404 Not Found	It is used when the requested application doesn't exist

6.1.8 Feature negotiation

The optional features in Table 6.1.8-1 are defined for the Nslpkmf_Discovery API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.1.8-1: Supported Features

Feature number	Feature Name	Description
N/A		

6.1.9 Security

As indicated in 3GPP TS 33.501 [11] and 3GPP TS 29.500 [4], the access to the Nslpkmf_Discovery API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [12]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [13]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Nslpkmf_Discovery API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [13], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Nslpkmf_Discovery service.

The Nslpkmf_Discovery API defines the following scopes "Nslpkmf-keyrequest" for OAuth2 authorization as specified in 3GPP TS 33.501 [11]:

Table 6.1.9-1: OAuth2 scopes defined in Npanf_ProseKey API

Scope	Description
"Nslpkmf-disc"	Access to the Nslpkmf_Discovery API
"Nslpkmf-disc:announce-authorize:modify"	Access to modify the authorization to announce for a UE in the PLMN
"Nslpkmf-disc:monitor-authorize:modify"	Access to modify the authorization for monitoring for an UE in the PLMN
"Nslpkmf-disc:discovery-authorize:modify"	Access to modify the authorization from the 5G DDNMF for a discoverer UE in the PLMN to operate Model B restricted discovery

6.1.10 HTTP redirection

An HTTP request may be redirected to a different SLPKMF service instance, within the same SLPKMF or a different SLPKMF of an SLPKMF set, e.g. when an SLPKMF service instance is part of an SLPKMF (service) set or when using indirect communications (see 3GPP TS 29.500 [4]).

An SCP that reselects a different SLPKMF producer instance will return the NF Instance ID of the new SLPKMF producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [4].

If an SLPKMF within an SLPKMF set redirects a service request to a different SLPKMF of the set using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new SLPKMF towards which the service request is redirected shall be indicated in the 3gpp-Sbi-Target-Nf-Id header of the 307 Temporary Redirect or 308 Permanent Redirect response as specified in clause 6.10.9.1 of 3GPP TS 29.500 [4].

6.2 Nslpkmf_SLPKMFKeyRequest Service API

6.2.1 Introduction

The Nslpkmf_SLPKMFKeyRequest shall use the Nslpkmf_SLPKMFKeyRequest API.

The API URI of the Nslpkmf_SLPKMFKeyRequest API shall be:

{apiRoot}/<apiName>/<apiVersion>

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [6], i.e.:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The <apiName> shall be "nslpkmf-keyrequest ".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.2.3.

6.2.2 Usage of HTTP

6.2.2.1 General

HTTP/2, IETF RFC 9113 [8], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [7] specification of HTTP messages and content bodies for the Nslpkmf_SLPKMFKeyRequest API is contained in Annex A.

6.2.2.2 HTTP standard headers

6.2.2.2.1 General

See clause 5.3.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

6.2.2.2.2 Content type

JSON, IETF RFC 8259 [9], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 9457 [10].

6.2.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.3.3.2 of 3GPP TS 29.500 [4] shall be applicable, and the optional HTTP custom header fields specified in clause 5.3.3.3 of 3GPP TS 29.500 [4] may be supported.

6.2.3 Resources

6.2.3.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 6.2.3.1-1 describes the resource URI structure of the Nslpkmf_SLPKMFKeyRequest API.

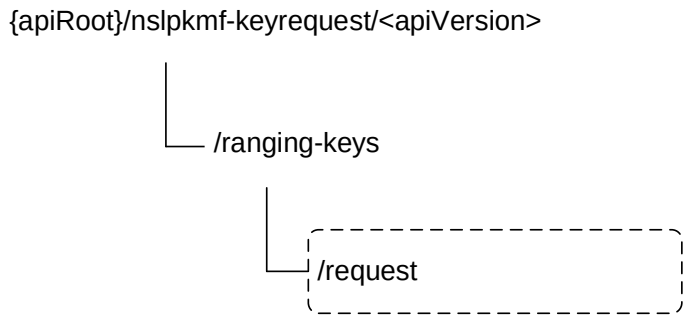

Figure 6.2.3.1-1: Resource URI structure of the Nslpkmf_SLPKMFKeyRequest API

Table 6.2.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.2.3.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Ranging Keys Collection	/ranging-keys	request (POST)	UnicastKey service operation

6.2.3.2 Resource: Ranging Keys Collection

6.2.3.2.1 Description

This resource represents the collection of the ranging keys managed by the SLPKMF.

This resource is modelled with the Collection resource archetype (see clause C.2 of 3GPP TS 29.501 [6]).

6.2.3.2.2 Resource Definition

Resource URI: **{apiRoot}/<apiName>/<apiVersion>/ranging-keys**

This resource shall support the resource URI variables defined in Table 6.2.3.2.2-1.

Table 6.2.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.2.1

6.2.3.2.3 Resource Standard Methods

There is no standard method supported by the resource.

6.2.3.2.4 Resource Custom Operations

6.2.3.2.4.1 Overview

Table 6.2.3.2.4.1-1: Custom operations

Operation name	Custom operaration URI	Mapped HTTP method	Description
request	{resourceUri}/request	POST	UnicastKey service operation

6.2.3.2.4.2 Operation: request

6.2.3.2.4.2.1 Description

This custom operation requests the keying material related to ranging in the SLPKMF.

6.2.3.2.4.2.2 Operation Definition

This operation shall support the request data structures specified in Table 6.2.3.2.4.2.2-1 and the response data structure and response codes specified in Table 6.2.3.2.4.2.2-2.

Table 6.2.3.2.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
UnicastKeyReqData	M	1	Representation of the input to request the keying material.

Table 6.2.3.2.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
UnicastKeyRspData	M	1	200 OK	Representation of the successfully requested keying material.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 1)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	The "cause" attribute shall be set to one of the following application error: - UE_NOT_AUTHORIZED See Table 6.2.7.3-1 for the description of these errors.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute shall be set to one of the following application error: - UE_NOT_FOUND See Table 6.2.7.3-1 for the description of these errors.
NOTE 1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.2.3.2.4.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

Table 6.2.3.2.4.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SLPKMF or SLPKMF (service) set. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target SLPKMF (service) instance ID towards which the request is redirected

6.2.4 Custom Operations without associated resources

There is no custom operation without associated resources supported in Nslpkmf_SLPKMFKeyRequest Service.

6.2.5 Notifications

There is no notification defined for Nslpkmf_SLPKMFKeyRequest service.

6.2.6 Data Model

6.2.6.1 General

This clause specifies the application data model supported by the API.

Table 6.2.6.1-1 specifies the data types defined for the Nslpkmf_SLPKMFKeyRequest service based interface protocol.

Table 6.2.6.1-1: Nslpkmf_SLPKMFKeyRequest specific Data Types

Data type	Clause defined	Description	Applicability
UnicastKeyReqData	6.2.6.2.2	Representation of the input to request the keying material.	
UnicastKeyRspData	6.2.6.2.3	Representation of the successfully requested keying material.	
SlpkId	6.2.6.3	Sidelink positioning Key ID for user	
Kslp	6.2.6.3	Key for Sidelink positioning	
KslpFreshnessParameter1	6.2.6.3	KSLP Freshness Parameter 1	
KslpFreshnessParameter2	6.2.6.3	KSLP Freshness Parameter 2	

Table 6.2.6.1-2 specifies data types re-used by the Nslpkmf_SLPKMFKeyRequest service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nslpkmf_SLPKMFKeyRequest service based interface.

Table 6.2.6.1-2: Nslpkmf_SLPKMFKeyRequest re-used Data Types

Data type	Reference	Comments	Applicability
ApplicationId	3GPP TS 29.571 [15]	Represents the identifier of an application.	

6.2.6.2 Structured data types

6.2.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

6.2.6.2.2 Type: UnicastKeyReqData

Table 6.2.6.2.2-1: Definition of type UnicastKeyReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
rangingSlAppId	ApplicationId	M	1	This IE shall indicate the application identifier for ranging and sidelink positioning service.	
kslpFreshness1	KslpFreshness Parameter1	M	1	This IE shall carry the KSLP Freshness Parameter 1 in the ranging UE.	
slpkId	SlpkId	M	1	This IE shall indicate the SLPK ID from the ranging UE.	

6.2.6.2.3 Type: UnicastKeyRspData

Table 6.2.6.2.3-1: Definition of type UnicastKeyRspData

Attribute name	Data type	P	Cardinality	Description	Applicability
kslp	Kslp	M	1	This IE shall carry the KSLP derived by the SLPKMF.	
kslpFreshness2	KslpFreshness Parameter2	M	1	This IE shall carry the KSLP Freshness Parameter 2 generated by the SLPKMF.	

6.2.6.3 Simple data types and enumerations

6.2.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

6.2.6.3.2 Simple data types

The simple data types defined in Table 6.2.6.3.2-1 shall be supported.

Table 6.2.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
SlpkId	string	Ranging User Key ID String type as defined in OpenAPI Specification [7], carrying the value of the "SLPK ID" parameter via PC8* (with "xs:string" type in XML schema) as specified in 3GPP TS 24.554 [16].	
Kslp	string	Key for RANGING AND SIDELINK POSITIONING String type as defined in OpenAPI Specification [7], carrying the value of the "KSLP" parameter via PC8* (with "xs:hexBinary" type in XML schema) as specified in 3GPP TS 24.554 [16].	
KslpFreshnessParameter1	string	KSLP Freshness Parameter 1 String type as defined in OpenAPI Specification [7], carrying the value of the "KSLP freshness parameter 1" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in 3GPP TS 24.554 [16].	
KslpFreshnessParameter2	string	KSLP Freshness Parameter 2 String type as defined in OpenAPI Specification [7], carrying the value of the "KSLP freshness parameter 2" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in 3GPP TS 24.554 [16].	

6.2.6.4 Data types describing alternative data types or combinations of data types

There is no data type describing alternative data types or combinations of data types in Nslpkmf_SLPKMFKeyRequest Service.

6.2.6.5 Binary data

There is no binary data type in Nslpkmf_SLPKMFKeyRequest Service.

6.2.7 Error Handling

6.2.7.1 General

For the Nslpkmf_SLPKMFKeyRequest API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [6]. Protocol errors and application errors specified in Table 5.3.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in Table 5.3.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Nslpkmf_SLPKMFKeyRequest API.

6.2.7.2 Protocol Errors

Protocol errors handling shall be supported as specified in clause 5.3.7 of 3GPP TS 29.500 [4].

6.2.7.3 Application Errors

The application errors defined for the Nslpkmf_SLPKMFKeyRequest service are listed in Table 6.2.7.3-1.

Table 6.2.7.3-1: Application errors

Application Error	HTTP status code	Description
UE_NOT_AUTHORIZED	403 Forbidden	The UE is not authorized for the requested service.
UE_NOT_FOUND	404 Not Found	The UE related to the SLPK ID is not found in the SLPKMF.

6.2.8 Feature negotiation

The optional features in Table 6.2.8-1 are defined for the Nslpkmf_SLPKMFKeyRequest API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.2.8-1: Supported Features

Feature number	Feature Name	Description
N/A		

6.2.9 Security

As indicated in 3GPP TS 33.501 [11] and 3GPP TS 29.500 [4], the access to the Nslpkmf_SLPKMFKeyRequest API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [12]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [13]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Nslpkmf_SLPKMFKeyRequest API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [13], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Nslpkmf_SLPKMFKeyRequest service.

The Nslpkmf_SLPKMFKeyRequest API defines a single scope "nslpkmf-keyrequest" for OAuth2 authorization (as specified in 3GPP TS 33.501 [11]) for the entire service, and it does not define any additional scopes at resource or operation level.

6.2.10 HTTP redirection

An HTTP request may be redirected to a different SLPKMF service instance, within the same SLPKMF or a different SLPKMF of an SLPKMF set, e.g. when an SLPKMF service instance is part of an SLPKMF (service) set or when using indirect communications (see 3GPP TS 29.500 [4]).

An SCP that reselects a different SLPKMF producer instance will return the NF Instance ID of the new SLPKMF producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [4].

If an SLPKMF within an SLPKMF set redirects a service request to a different SLPKMF of the set using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new SLPKMF towards which the service request is redirected shall be indicated in the 3gpp-Sbi-Target-Nf-Id header of the 307 Temporary Redirect or 308 Permanent Redirect response as specified in clause 6.10.9.1 of 3GPP TS 29.500 [4].

Annex A (normative): OpenAPI specification

A.1 General

This Annex specifies the formal definition of the API(s) defined in the present specification. It consists of OpenAPI 3.0.0 specifications in YAML format.

This Annex takes precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API(s).

NOTE 1: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification files contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5.3.1 of 3GPP TS 29.501 [6] and clause 5B 3GPP TR 21.900 [14]).

A.2 Nslpkmf_Discovery API

```
openapi: 3.0.0

info:
  title: Nslpkmf_Discovery API
  version: '1.0.0-alpha.3'
  description: |
    Nslpkmf_Discovery Service.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.586 V18.0.0; 5G System; SideLink Positioning Key Management Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.586/

servers:
  - url: '{apiRoot}/Nslpkmf-discovery/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:
  - {}
  - oAuth2ClientCredentials:
    - Nslpkmf-discovery

paths:
  /{ueId}/announce-authorize/{userInfoId}:
    put:
      summary: Obtain the authorization from the SLPKMF for announcing in the PLMN
      operationId: ObtainAnnounceAuth
      tags:
        - Obtain the authorization from the SLPKMF for announcing in the PLMN
      security:
        - {}
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
          - Nslpkmf-disc:announce-authorize:modify
      parameters:
        - name: ueId
          in: path
          description: Identifier of the UE
          required: true
          schema:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/VarUeId'
        - name: userInfoId
          in: path
          description: User Info Id
          required: true
          schema:
            $ref: '#/components/schemas/UserInfoId'
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/AnnounceAuthData'
        required: true
      responses:
        '201':
          description: Successful creation of the resource
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AnnounceAuthData'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure:
                {apiRoot}/Nslpkmf-disc>/<apiVersion>/{ueId}/announce-authorize/{userInfoId}
              required: true
              schema:
                type: string
        '204':
          description: Successful update of the resource.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          description: Unexpected error

  /{ueId}/monitor-authorize/{userInfoId}:
    put:
      summary: Obtain the discovery key from the SLPKMF for monitoring in the PLMN
      operationId: ObtainMonitorAuthorize
      tags:
        - Obtain the discovery key from the SLPKMF for monitoring in the PLMN
      security:
        - {}
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
          - Nslpkmf-disc:monitor-authorize:modify
      parameters:
        - name: ueId
          in: path
          description: Identifier of the UE
          required: true
          schema:
```

```
            $ref: 'TS29571_CommonData.yaml#/components/schemas/VarUeId'
        - name: userInfoId
          in: path
          description: User Info Id
          required: true
          schema:
            $ref: '#/components/schemas/UserInfoId'
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MonitorAuthReqData'
        required: true
      responses:
        '201':
          description: Created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MonitorAuthRespData'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure:
                {apiRoot}/Nslpkmf-disc>/<apiVersion>/{ueId}/monitor-authorize/{userInfoId}
              required: true
              schema:
                type: string
        '204':
          description: Successful update of the resource.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          description: Unexpected error

  /{ueId}/discovery-authorize/{userInfoId}:
    put:
      summary: Obtain the discovery key from the SLPKMF for a discoverer UE
      operationId: ObtainDiscAuth
      tags:
        - Obtain the discovery key for a discoverer UE
      security:
        - {}
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
        - oAuth2ClientCredentials:
          - Nslpkmf-disc
          - Nslpkmf-disc:discovery-authorize:modify
      parameters:
        - name: ueId
          in: path
          description: Identifier of the UE
          required: true
          schema:
```

```
            $ref: 'TS29571_CommonData.yaml#/components/schemas/VarUeId'
        - name: userInfoId
          in: path
          description: User Info Id
          required: true
          schema:
            $ref: '#/components/schemas/UserInfoId'
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DiscoveryAuthReqData'
        required: true
      responses:
        '201':
          description: Created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/DiscoveryAuthRespData'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure:
                {apiRoot}/Nslpkmf-disc>/<apiVersion>/{ueId}/discovery-authorize/{userInfoId}
              required: true
              schema:
                type: string
        '204':
          description: Successful update of the resource.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          description: Unexpected error


components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            Nslpkmf-disc: Access to the Nslpkmf_Discovery API
            Nslpkmf-disc:announce-authorize:modify: >
              Access to modify the authorization to announce for a UE in the PLMN
            Nslpkmf-disc:monitor-authorize:modify: >
              Access to modify the authorization for monitoring for an UE in the PLMN
            Nslpkmf-disc:discovery-authorize:modify: >
              Access to modify the authorization from the SLPKMF for a discoverer UE
              in the PLMN to operate Model B restricted discovery

  schemas:
```

```
# COMPLEX TYPES:

    AnnounceAuthData:
      type: object
      description: Represents Data used to request the authorization to announce for a UE
      required:
        - rangingSlAppId
        - ueRole
      properties:
        rangingSlAppId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        ueRole:
          $ref: '#/components/schemas/UeRole'

    MonitorAuthReqData:
      type: object
      description: Data used to request the discovery key to monitor for a UE
      required:
        - rangingSlAppId
        - ueRole
        - ueSecurityCapability
      properties:
        rangingSlAppId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        ueRole:
          $ref: '#/components/schemas/UeRole'
        ueSecurityCapability:
          $ref: '#/components/schemas/UeSecurityCapability'

    MonitorAuthRespData:
      type: object
      description: Represents the obtained Monitor Discovery Key Data for a UE
      required:
        - chosenPc5CipheringAlgorithm
        - discSecMaterials
      properties:
        chosenPc5CipheringAlgorithm:
          $ref: '#/components/schemas/ChosenPc5CipheringAlgorithm'
        discSecMaterials:
          $ref: '#/components/schemas/DiscSecMaterials'

    DiscoveryAuthReqData:
      type: object
      description: Data used to request the discovery key to monitor for a discoverer UE
      required:
        - rangingSlAppId
        - ueRole
        - ueSecurityCapability
      properties:
        rangingSlAppId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        ueRole:
          $ref: '#/components/schemas/UeRole'
        ueSecurityCapability:
          $ref: '#/components/schemas/UeSecurityCapability'

    DiscoveryAuthRespData:
      type: object
      description: Represents the obtained Monitor Discovery Key Data for a discoverer UE
      required:
        - chosenPc5CipheringAlgorithm
        - discSecMaterials
      properties:
        chosenPc5CipheringAlgorithm:
          $ref: '#/components/schemas/ChosenPc5CipheringAlgorithm'
        discSecMaterials:
          $ref: '#/components/schemas/DiscSecMaterials'

    DiscSecMaterials:
      type: object
      description: Represents the discovery security materials
      properties:
        duik:
          $ref: '#/components/schemas/Duik'
        dusk:
          $ref: '#/components/schemas/Dusk'
        duck:
```

```
          $ref: '#/components/schemas/Duck'


# SIMPLE TYPES:
    UserInfoId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'

    UeSecurityCapability:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'

    ChosenPc5CipheringAlgorithm:
      description: Contains the chosen PC5 ciphering algorithm.
      type: integer

    Duik:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'

    Duck:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'

    Dusk:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'


    UeRole:
      description: Specifies the different roles of UE for ranging and sidelink positioning service.
      anyOf:
        - type: string
          enum:
            - TARGET_UE
            - REFERENCE_UE
            - LOCATED_UE
            - CLIENT_UE
            - SERVER_UE
        - type: string


# ENUMS:
```

A.3 Nslpkmf_SLPKMFKeyRequest API

```
openapi: 3.0.0

info:
  title: Nslpkmf_SLPKMFKeyRequest
  version: '1.0.0-alpha.3'
  description: |
    SLPKMF KeyRequest Service.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.586 V18.0.0; 5G System; SideLink Positioning Key Management Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.586/

servers:
  - url: '{apiRoot}/nslpkmf-keyrequest/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:
  - {}
  - oAuth2ClientCredentials:
    - nslpkmf-keyrequest

paths:
  /ranging-keys/request:
    post:
```

```
      summary: Request Keying Materials for ranging
      operationId: UnicastKey
      tags:
        - Ranging Keys Collection (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/UnicastKeyReqData'
      responses:
        '200':
          description: Success
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/UnicastKeyRspData'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nslpkmf-keyrequest: Access to the Nslpkmf_SLPKMFKeyRequest API

  schemas:
#
#  Structured Data Types
#
    UnicastKeyReqData:
      description: Representation of the input to request the keying material.
      type: object
      properties:
        rangingSlAppId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        kslpFreshness1:
          $ref: '#/components/schemas/KslpFreshnessParameter1'
        slpkId:
          $ref: '#/components/schemas/SlpkId'
      required:
        - rangingSlAppId
        - kslpFreshness1
        - slpkId


    UnicastKeyRspData:
      description: Representation of the successfully requested keying material.
```

```
      type: object
      properties:
        kslp:
          $ref: '#/components/schemas/Kslp'
        kslpFreshness2:
          $ref: '#/components/schemas/KslpFreshnessParameter2'
      required:
        - kslp
        - kslpFreshness2

#
#  Simple Data Types
#
    SlpkId:
      description: Ranging User Key ID
      type: string

    Kslp:
      description: Key for RANGING AND SIDELINK POSITIONING
      type: string

    KslpFreshnessParameter1:
      description: KSLP Freshness Parameter 1
      type: string

    KslpFreshnessParameter2:
      description: KSLP Freshness Parameter 2
      type: string


#
#  Enumeration Data Types
#
```

Annex B (informative): Withdrawn API versions

B.1 General

This Annex lists withdrawn API versions of the APIs defined in the present specification. 3GPP TS 29.501 [5] clause 4.3.1.6 describes the withdrawal of API versions.

Annex C (normative): ABNF grammar for 3GPP SBI HTTP custom headers

This Annex shall only be included if the TS defines 3GPP-specific custom HTTP headers.

C.1 General

This Annex contains a self-contained set of ABNF rules, comprising the re-used rules from IETF RFCs, and the rules defined by the 3GPP custom headers defined in this specification (see clause 6.x.1.z).

Where clause 6.x.1.z is to be replaced by the clause number(s) where the 3GPP custom headers are defined in the APIs defined in this TS.

This grammar may be used as input to existing tools to help implementations to parse 3GPP custom headers.

Annex D (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-11	CT4#119	C4-235487 C4-235690 C4-235691				Implementing the following p-CR agreed by CT4: C4-235487, C4-235690, and C4-235691; and Editorial change from the rapporteur.	0.1.0
2023-12	CT#102	CP-233170				TS presented for information	1.0.0
2024-03	CT4#121	C4-240751				Implementing the following p-CR agreed by CT4: C4-240751; and Editorial change from the rapporteur.	1.1.0
2024-03	CT#103	CP-240027				TS Presented for approval	2.0.0
2024-03	CT#103					TS approved in CT#103	18.0.0

History

Document history		
V18.0.0	May 2024	Publication