ETSI TS 129 559 V18.3.0 (2024-07)

5G;
5G System;
5G ProSe Key Management Services;
Stage 3
(3GPP TS 29.559 version 18.3.0 Release 18)

Reference
RTS/TSGC-0429559vi30

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 stage 3 protocol and data model for the Npkmf Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the 5G PKMF as specified in 3GPP TS 33.503 [4].

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [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 [6].

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 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

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

[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: "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 29.503: "5G System; Unified Data Management Services; Stage 3".

[18] 3GPP TS 29.509: "5G System; Authentication Server Services; Stage 3".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

Void

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].

5G PKMF	5G ProSe Key Management Function
5G ProSe	5G Proximity based Services
RPAUID	Restricted ProSe Application User ID
PDUID	ProSe Discovery UE ID
UP-PRUK	User Plane ProSe Remote User Key

4 Overview

The 5G ProSe Key Management Function (5G PKMF) is the logical function handling network related actions required for the key management and the security material for discovery of a 5G ProSe UE-to-Network Relay by a 5G ProSe Remote UE, for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay, for discovery of a 5G ProSe UE-to-UE Relay by a 5G ProSe End UE, and for establishing a secure PC5 communication link between a 5G ProSe End UE and a 5G ProSe UE-to-UE Relay (see 3GPP TS 33.503 [4]).

Figure 4-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the 5G PKMF:

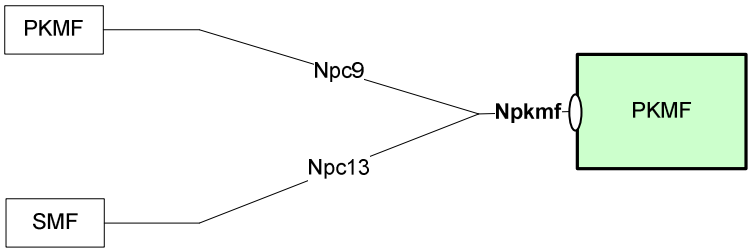

Figure 4-1: Reference model – 5G PKMF

The functionalities supported by the 5G PKMF are listed in clause 4.2.1.2 of 3GPP TS 33.503 [4].

5 Services offered by the 5G PKMF

5.1 Introduction

The table 5.1-1 shows the 5G PKMF Services and 5G PKMF Service Operations:

Table 5.1-1: List of 5G PKMF Services

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Npkmf_PKMFKeyRequest	ProseKey	Request/Response	5G PKMF
Npkmf_ResolveRemoteUserId	Retrieve	Request/Response	SMF, 5G PKMF
Npkmf_Discovery	AnnounceAuthorize	Request/Response	5G PKMF
	MonitorKey	Request/Response	5G PKMF
	DiscoveryKey	Request/Response	5G PKMF

Table 5.1-2 summarizes the corresponding APIs defined for this specification.

Table 5.1-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Npkmf_PKMFKeyRequest	6.1	PKMF Key Request Service	TS29559_Npkmf_PKMFKeyRequest.yaml	npkmf-keyrequest	A.2
Npkmf_ResolveRemoteUserId	6.2	PKMF Resolve Remote User ID Service	TS29559_Npkmf_UserId.yaml	npkmf-userid	A.3
Npkmf_Discovery	6.3	PKMF Discovery Service	TS29559_Npkmf_Discovery.yaml	npkmf-disc	A.4

5.2 Npkmf_PKMFKeyRequest Service

5.2.1 Service Description

This service enables an NF (i.e. another 5G PKMF in another PLMN) to request information related to 5G ProSe keying. The following are the key functionalities of this NF service.

- Provide 5G ProSe related keying material

5.2.2 Service Operations

5.2.2.1 Introduction

5.2.2.2 ProseKey

5.2.2.2.1 General

The ProseKey service operation is invoked by a NF Service Consumer, i.e. another 5G PKMF in another PLMN, towards the 5G PKMF to retrieve the keying material related to 5G ProSe.

The ProseKey service operation is used during the following procedure:

- PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane (see 3GPP TS 33.503 [4], clause 6.3.3.2.2)

The NF Service Consumer (i.e. another 5G PKMF in another PLMN) shall retrieve the 5G ProSe related keying material by invoking the "request " custom method on the resource URI of "Prose Keys Collection" resource, see clause 6.1.3.2.4. See also Figure 5.2.2.2.1-1.

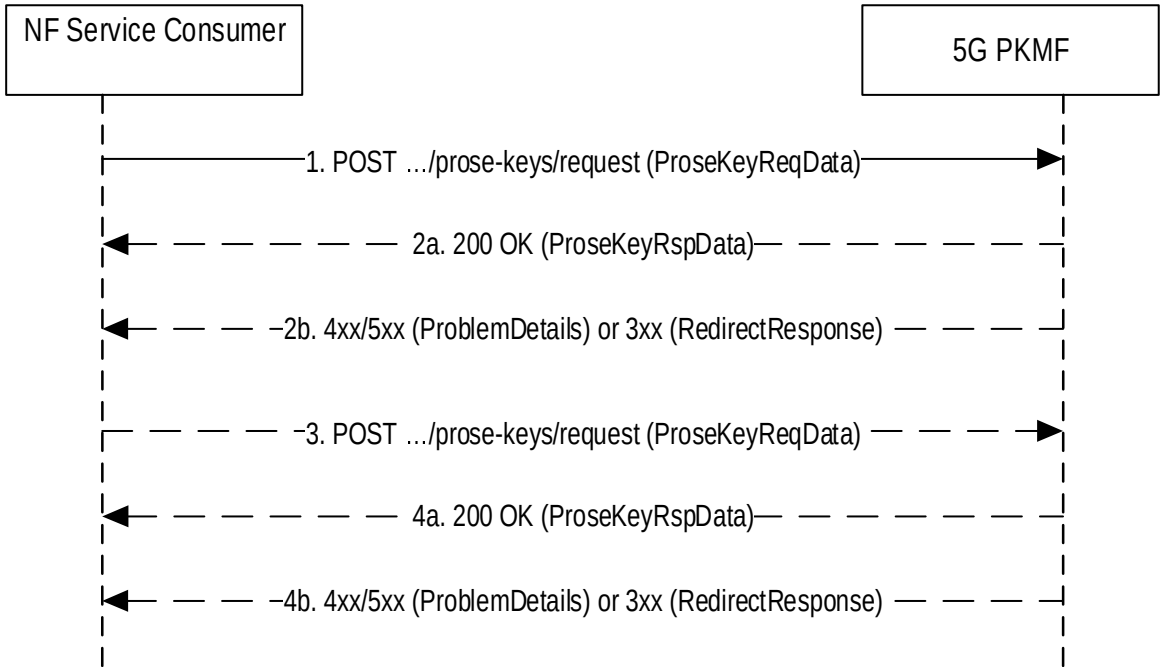

Figure 5.2.2.2.1-1 ProseKey service operation

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 "ProseKeyReqData" data type. The payload shall include the Relay Service Code, the KNRP freshness parameter 1, and either the SUCI of the 5G ProSe UE (Remote UE or End UE) or the UP-PRUK ID.

2a. On success, the 5G PKMF shall respond with the status code "200 OK". The payload of the response shall be an object of "ProseKeyRspData" data type. They payload shall include the KNRP, the KNRP freshness parameter 2 and optionally the GPI.

2b. On failure or redirection, one of the HTTP status codes listed in table 6.1.3.2.4.2.2-2 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 6.1.3.2.4.2.2-2.

3. [conditional] If synchronization failed when UE processes the authentication challenge in the GPI and a subsequent Key Request is send for resynchronization, 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 "ProseKeyReqData" data type. The payload shall include the Relay Service Code, the KNRP freshness parameter 1, the information for resynchronization (RAND and AUTS).

4a. On success, the 5G PKMF shall respond with the status code "200 OK". The payload of the response shall be an object of "ProseKeyRspData" data type. They payload shall include the KNRP, the KNRP freshness parameter 2 and the GPI.

4b. On failure or redirection, one of the HTTP status codes listed in table 6.1.3.2.4.2.2-2 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 6.1.3.2.4.2.2-2.

5.3 Npkmf_ResolveRemoteUserId Service

5.3.1 Service Description

The Npkmf_ResolveRemoteUserId service enables a NF to request the 5G PKMF to resolve Remote User ID (i.e., UP-PRUK ID) to SUPI.

5.3.2 Service Operations

5.3.2.1 Introduction

The service operation defined for the Npkmf_ResolveRemoteUserId service is as follows:

- Retrieve: It allows a consumer NF to get an user's SUPI from Remote User ID.

5.3.2.2 Retrieve

5.3.2.2.1 General

The Retrieve service operation is used during the following procedure:

- PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane (see 3GPP TS 33.503 [4], clause 6.3.3.2.2)

The NF Service Consumer (e.g., SMF, 5G PKMF) shall request the 5G PKMF to get the SUPI of a 5G ProSe Remote UE as shown in Figure 5.3.2.2.1-1

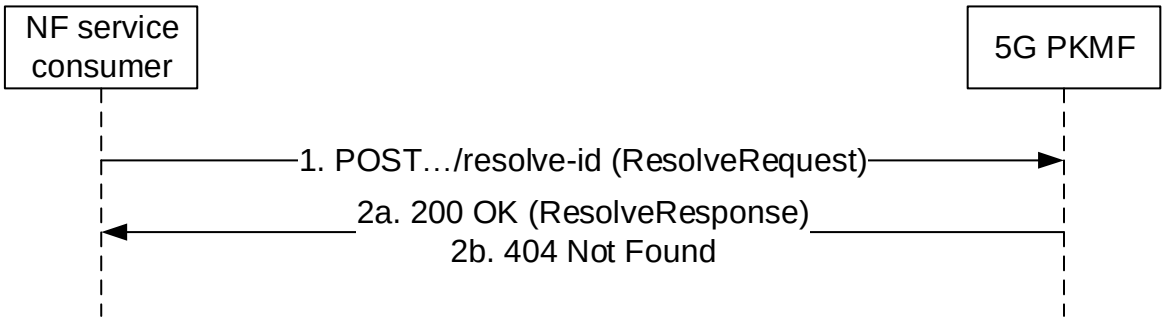

Figure 5.3.2.2.1-1: Requesting the SUPI of a ProSe Remote UE

1. The NF service consumer (e.g., SMF, 5G PKMF) sends a POST request to the resource representing the resolve-id custom operation. The request body shall contain the UP-PRUK ID.

2a. On success, the 5G PKMF responds with "200 OK" with the message body containing the corresponding SUPI.

2b. If there is no valid data, HTTP status code "404 Not Found" shall be returned including additional error information in the response body (in the "ProblemDetails" element).

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the POST response body.

5.4 Npkmf_ Discovery Service

5.4.1 Service Description

This service enables an NF (i.e. another 5G PKMF in another PLMN) to request authorization information. The following are the key functionalities of this NF service.

- Provide the authorization from the 5G PKMF for announcing in the PLMN
- Provide the discovery key from the 5G PKMF for monitoring in the PLMN
- Provide the discovery key from the 5G PKMF for a discoverer UE in the PLMN to operate Model B restricted discovery

5.4.2 Service Operations

5.4.2.1 Introduction

The Npkmf_Discovery service supports following service operations:

- AnnounceAuthorize
- MonitorKey
- DiscoveryKey

5.4.2.2 AnnounceAuthorize

5.4.2.2.1 General

The AnnounceAuthorize service operation is invoked by a NF Service Consumer, i.e. another 5G PKMF in another PLMN, towards the 5G PKMF to retrieve the authorization from the 5G PKMF for announcing in the PLMN.

The NF Service Consumer (e.g., 5G PKMF) shall request the 5G PKMF to get authorization as shown in Figure 5.4.2.2.1-1

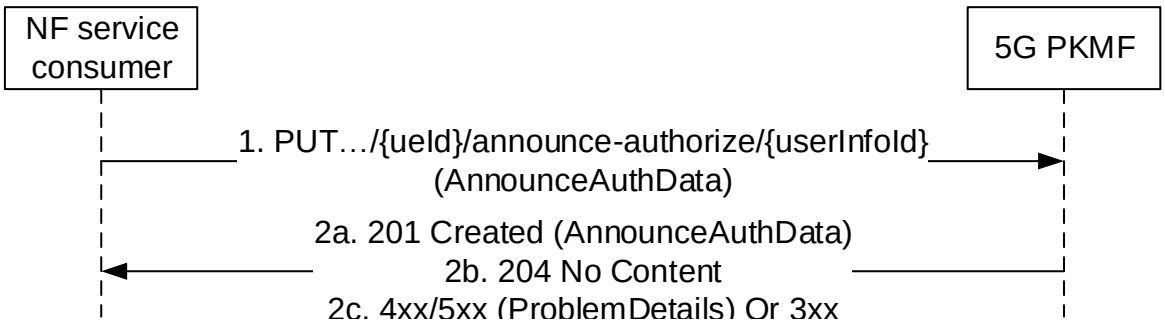

Figure 5.4.2.2.1-1: Announce Authorize

1. The NF service consumer (e.g., 5G PKMF) sends a HTTP PUT request to the resource representing the announce-authorize custom operation. The request body shall contain the RSC.

2a. If the context indicated by the userInfoId doesn't exist, the 5G PKMF 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 5G PKMF 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 6.3.3.2.3.1-3 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 6.3.3.2.3.1-3.

5.4.2.3 MonitorKey

5.4.2.3.1 General

The MonitorKey service operation is invoked by a NF Service Consumer, i.e. another 5G PKMF in another PLMN, towards the 5G PKMF to retrieve the discovery key from the 5G PKMF for monitoring in the PLMN.

The NF Service Consumer (e.g., 5G PKMF) shall request the 5G PKMF to get authorization as shown in Figure 5.4.2.3.1-1

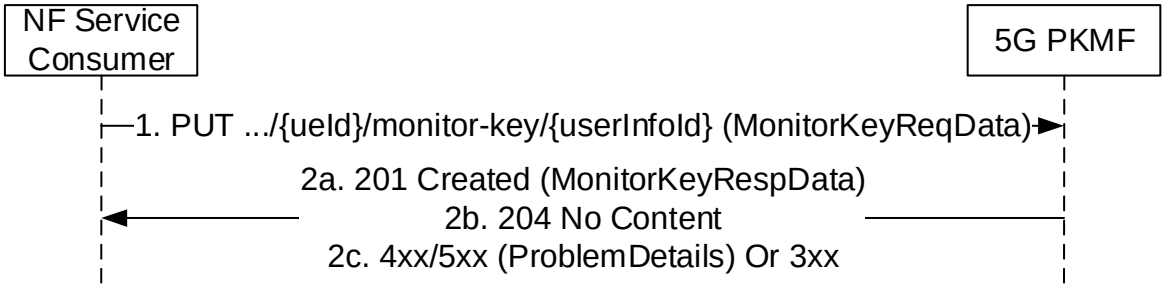

Figure 5.4.2.3.2-1: Monitor Key

1. The NF Service Consumer (e.g., 5G PKMF) shall send an HTTP PUT request to the resource representing the monitor-key custom operation. The request body shall contain the RSC and PC5 UE security capability.

2a. If the context indicated by the userInfoId doesn't exist, the 5G PKMF 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 5G PKMF 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 6.3.3.3.3.1-3 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 6.3.3.3.3.1-3.

5.4.2.4 DiscoverKey

5.4.2.4.1 General

The DiscoverKey service operation is invoked by a NF Service Consumer, i.e. another 5G PKMF in another PLMN, towards the 5G PKMF to retrieve the discovery key from the 5G PKMF for a discoverer UE in the PLMN to operate Model B restricted discovery.

The NF Service Consumer (e.g., 5G PKMF) shall request the 5G PKMF to get authorization as shown in Figure 5.4.2.4.1-1

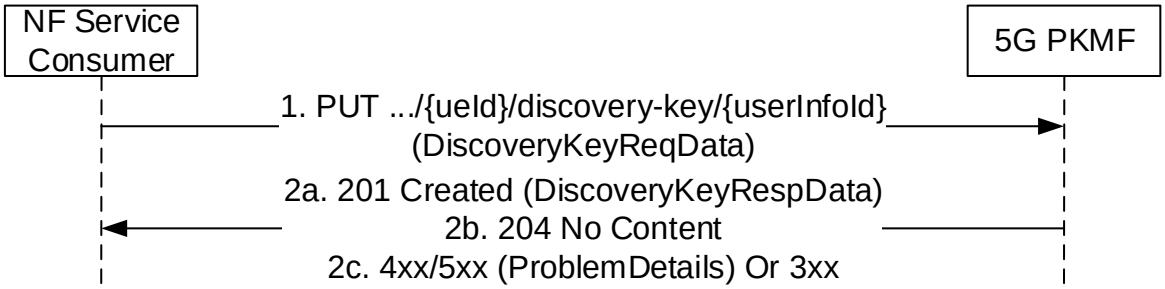

Figure 5.4.2.4.2-1: Discover Key

1. The NF Service Consumer (e.g., 5G PKMF) shall send an HTTP PUT request to the resource representing the monitor-key custom operation. The request body shall contain the RSC and PC5 UE security capability.

2a. If the context indicated by the userInfoId doesn't exist, the 5G PKMF 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 5G PKMF 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 6.3.3.3.3.1-3 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 6.3.3.3.3.1-3.

6 API Definitions

6.1 Npkmf_PKMFKeyRequest Service API

6.1.1 Introduction

The Npkmf_PKMFKeyRequest shall use the Npkmf_PKMFKeyRequest API.

The API URI of the Npkmf_PKMFKeyRequest 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 "npkmf-keyrequest ".
- 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 [5].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [5].

The OpenAPI [7] specification of HTTP messages and content bodies for the Npkmf_PKMFKeyRequest 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 [5] 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 [5]. 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 [5] shall be applicable, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [5] 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 Npkmf_PKMFKeyRequest API.

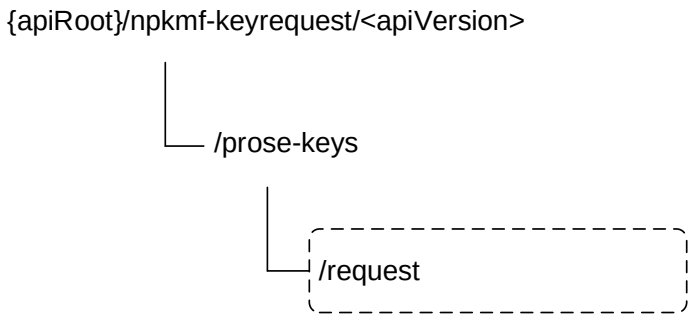

Figure 6.1.3.1-1: Resource URI structure of the Npkmf_PKMFKeyRequest API

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
ProSe Keys Collection	/prose-keys	request (POST)	ProseKey service operation

6.1.3.2 Resource: ProSe Keys Collection

6.1.3.2.1 Description

This resource represents the collection of the ProSe Keys managed by the 5G PKMF.

This resource is modelled with the Collection resource archetype (see clause C.2 of 3GPP TS 29.501 [5]).

6.1.3.2.2 Resource Definition

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

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

6.1.3.2.3 Resource Standard Methods

There is no standard method supported by the resource.

6.1.3.2.4 Resource Custom Operations

6.1.3.2.4.1 Overview

Table 6.1.3.2.4.1-1: Custom operations

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

6.1.3.2.4.2 Operation: request

6.1.3.2.4.2.1 Description

This custom operation requests the keying material related to 5G ProSe in the 5G PKMF.

6.1.3.2.4.2.2 Operation Definition

This operation shall support the request data structures specified in table 6.1.3.2.4.2.2-1 and the response data structure and response codes specified in table 6.1.3.2.4.2.2-2.

Table 6.1.3.2.4.2.2-1: Data structures supported by the POST Request Body on this resource

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

Table 6.1.3.2.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ProseKeyRspData	M	1	200 OK	Representation of the successfully requested keying material.
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 Not Found	The "cause" attribute shall be set to one of the following application error: - UE_NOT_AUTHORIZED See table 6.1.7.3-1 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 6.1.7.3-1 for the description of these errors.
NOTE1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.2.4.2.2-3: 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 5G PKMF or 5G PKMF (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 5G PKMF (service) instance ID towards which the request is redirected

Table 6.1.3.2.4.2.2-4: 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 5G PKMF or 5G PKMF (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 5G PKMF (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 Npkmf_PKMFKeyRequest Service.

6.1.5 Notifications

There is no notification defined for Npkmf_PKMFKeyRequest 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 Npkmf_PKMFKeyRequest service based interface protocol.

Table 6.1.6.1-1: Npkmf_PKMFKeyRequest specific Data Types

Data type	Clause defined	Description	Applicability
ProseKeyReqData	6.1.6.2.2	Representation of the input to request the keying material.	
ProseKeyRspData	6.1.6.2.3	Representation of the successfully requested keying material.	
PrukId	6.1.6.3	User Plane Prose Remote User Key ID	
Knrp	6.1.6.3	Key for NR PC5	
KnrpFreshnessParameter1	6.1.6.3	K_{NRP} Freshness Parameter 1	
KnrpFreshnessParameter2	6.1.6.3	K_{NRP} Freshness Parameter 2	
Gpi	6.1.6.3	GBA Push Information	

Table 6.1.6.1-2 specifies data types re-used by the Npkmf_PKMFKeyRequest 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 Npkmf_PKMFKeyRequest service based interface.

Table 6.1.6.1-2: Npkmf_PKMFKeyRequest re-used Data Types

Data type	Reference	Comments	Applicability
RelayServiceCode	3GPP TS 29.571 [15]	Relay Service Code	
ResynchronizationInfo	3GPP TS 29.503 [17]	Resynchronization Information	
Suci	3GPP TS 29.509 [18]	String contains the SUCI	

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: ProseKeyReqData

Table 6.1.6.2.2-1: Definition of type ProseKeyReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
relayServCode	RelayServiceCode	M	1	This IE shall indicate the Relay Service Code from the 5G ProSe Remote UE or the 5G ProSe End UE.	
knrpFreshness1	KnrpFreshnessParameter1	M	1	This IE shall carry the K_{NRP} Freshness Parameter 1 in the 5G ProSe Remote UE or the 5G ProSe End UE.	
resyncInfo	ResynchronizationInfo	C	0..1	This IE shall be present in service request for subsequent key request handling synchronization failure. When present, this IE shall carry information (RAND, AUTS) from the 5G ProSe Remote UE or the 5G ProSe End UE related to the synchronization Failure.	
prukId	PrukId	C	0..1	This IE may be present in service request for initial key request. When present, this IE shall indicate the UP-PRUK ID from the 5G ProSe Remote UE or the 5G ProSe End UE. (See NOTE)	
suci	Suci	C	0..1	This IE may be present in service request for initial key request. When present, this IE shall carry the SUCI of the 5G ProSe Remote UE or the 5G ProSe End UE (See NOTE).	
NOTE: Either prukId IE or suci IE shall be present in service request for initial key request.					

6.1.6.2.3 Type: ProseKeyRspData

Table 6.1.6.2.3-1: Definition of type ProseKeyRspData

Attribute name	Data type	P	Cardinality	Description	Applicability
knrp	Knrp	M	1	This IE shall carry the K_{NRP} derived by the 5G PKMF.	
knrpFreshness2	KnrpFreshness Parameter2	M	1	This IE shall carry the K_{NRP} Freshness Parameter 2 generated by the 5G PKMF.	
gpi	Gpi	C	0..1	This IE shall be present if GPI is generated or requested. When present, this IE shall carry the GPI.	

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
PrukId	string	User Plane Prose Remote User Key ID String type as defined in OpenAPI Specification [7], carrying the value of the "UP-PRUK ID" parameter via PC8 (with "xs:string" type in XML schema) as specified in clause 11.6.2.3 of 3GPP TS 24.554 [16].	
Knrp	string	Key for NR PC5 String type as defined in OpenAPI Specification [7], carrying the value of the "KNRP" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in clause 11.6.2.25 of 3GPP TS 24.554 [16].	
KnrpFreshnessParameter1	string	K_{NRP} Freshness Parameter 1 String type as defined in OpenAPI Specification [7], carrying the value of the "KNRP freshness parameter 1" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in clause 11.6.2.22 of 3GPP TS 24.554 [16].	
KnrpFreshnessParameter2	string	K_{NRP} Freshness Parameter 2 String type as defined in OpenAPI Specification [7], carrying the value of the "KNRP freshness parameter 2" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in clause 11.6.2.26 of 3GPP TS 24.554 [16].	
Gpi	string	GBA Push Information String type as defined in OpenAPI Specification [7], carrying the value of the "GPI" parameter via PC8 (with "xs:hexBinary" type in XML schema) as specified in clause 11.6.2.16 of 3GPP TS 24.554 [16].	

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 Npkmf_PKMFKeyRequest Service.

6.1.6.5 Binary data

There is no binary data type in Npkmf_PKMFKeyRequest Service.

6.1.7 Error Handling

6.1.7.1 General

For the Npkmf_PKMFKeyRequest 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 [5] 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 [5].

In addition, the requirements in the following clauses are applicable for the Npkmf_PKMFKeyRequest 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 [5].

6.1.7.3 Application Errors

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

Table 6.1.7.3-1: 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 indicated by the SUCI or related to the UP-PRUK ID is not found in the 5G PKMF.

6.1.8 Feature negotiation

The optional features in table 6.1.8-1 are defined for the Npkmf_PKMFKeyRequest API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [5].

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 [5], the access to the Npkmf_PKMFKeyRequest 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 Npkmf_PKMFKeyRequest 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 Npkmf_PKMFKeyRequest service.

The Npkmf_PKMFKeyRequest API defines a single scope "npkmf-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.

6.1.10 HTTP redirection

An HTTP request may be redirected to a different 5G PKMF service instance, within the same 5G PKMF or a different 5G PKMF of an 5G PKMF set, e.g. when an 5G PKMF service instance is part of an 5G PKMF (service) set or when using indirect communications (see 3GPP TS 29.500 [5]).

An SCP that reselects a different 5G PKMF producer instance will return the NF Instance ID of the new 5G PKMF producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [5].

If an 5G PKMF within an 5G PKMF set redirects a service request to a different 5G PKMF of the set using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new 5G PKMF 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 [5].

6.2 Npkmf_ResolveRemoteUserId Service API

6.2.1 Introduction

The Npkmf_ResolveRemoteUserId service shall use the Npkmf_ResolveRemoteUserId API.

The API URI of the Npkmf_ResolveRemoteUserId 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 "npkmf-userid".
- 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 [5].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [5].

The OpenAPI [7] specification of HTTP messages and content bodies for the Npkmf_ResolveRemoteUserId API is contained in Annex A.3.

6.2.2.2 HTTP standard headers

6.2.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [5] 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 [5]. 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 5.2.3.2 of 3GPP TS 29.500 [5] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [5] 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 depicts the resource URIs structure for the Npkmf_ResolveRemoteUserId API.

Figure 6.2.3.1-1: Resource URI structure of the Npkmf_ResolveRemoteUserId 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

6.2.4 Custom Operations without associated resources

6.2.4.1 Overview

The URI structure for Custom Operations without associated resources is included as part of the Figure 6.2.3.1-1

Table 6.2.4.1-1: Custom operations without associated resources

Custom operation URI	Mapped HTTP method	Description
resolve-id	POST	Resolve ProSe Remote User ID (i.e., UP-PRUK ID) to SUPI

6.2.4.2 Operation: resolve-id

6.2.4.2.1 Description

This custom operation is used by the NF service consumer (e.g., SMF, 5G PKMF) to request to resolve ProSe Remote User ID (i.e., UP-PRUK) to SUPI.

The URI of this custom operation is: {apiRoot}/npkmf-userid/<apiVersion>/resolve-id

6.2.4.2.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 6.2.4.2.2-1 and 6.2.4.2.2-2.

Table 6.2.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
ResolveRequest	M	1	Resolve Request data.

Table 6.2.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ResolveResponse	M	1	200 OK	Upon success, the response data contain the SUPI of the ProSe Remote UE.
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	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - USER_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 [5] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [5].				

Table 6.2.4.2.2-3: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

Table 6.2.4.2.2-4: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

6.2.5 Notifications

There is no notification defined for Npkmf_ResolveRemoteUserId 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 Npkmf_ResolveRemoteUserId service based interface protocol.

Table 6.2.6.1-1: Npkmf_ResolveRemoteUserId specific Data Types

Data type	Clause defined	Description	Applicability
ResolveRequest	6.2.6.2.2	Request Data	
ResolveResponse	6.2.6.2.3	Response Data	

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

Table 6.2.6.1-2: Npkmf_ResolveRemoteUserId re-used Data Types

Data type	Reference	Comments	Applicability
PrukId	Clause 6.1.6.3.2	Defined in Npkmf_PKMFKeyRequest API.	
PlmnId	3GPP TS 29.571 [15]	PLMN ID	
Supi	3GPP TS 29.571 [15]	Subscription Permanent Identifier	

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: ResolveRequest

Table 6.2.6.2.2-1: Definition of type ResolveRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
upPrukId	PrukId	M	1	UP-PRUK ID of the ProSe Remote UE	
plmnId	PlmnId	O	0..1	HPLMN ID of the 5G ProSe Remote UE	

6.2.6.2.3 Type: ResolveResponse

Table 6.2.6.2.2-1: Definition of type ResolveResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi	M	1	The SUPI of the UE	

6.2.6.3 Simple data types and enumerations

There are no simply data types and enumerations defined in Npkmf_ResolveRemoteUserId Service.

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 Npkmf_ResolveRemoteUserId Service.

6.2.6.5 Binary data

There is no binary data type in Npkmf_ResolveRemoteUserId Service.

6.2.7 Error Handling

6.2.7.1 General

For the Npkmf_ResolveRemoteUserId 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 [5] 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 [5].

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

6.2.7.2 Protocol Errors

No specific procedures for the Npkmf_ResolveRemoteUserId service are specified.

6.2.7.3 Application Errors

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

Table 6.2.7.3-1: Application errors

Application Error	HTTP status code	Description
USER_NOT_FOUND	404 Not Found	The provided subscriber identifier is not found.

6.2.8 Feature negotiation

The optional features in table 6.2.8-1 are defined for the Npkmf_ResolveRemoteUserId API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [5].

Table 6.2.8-1: Supported Features

Feature number	Feature Name	Description

6.2.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [5], the access to the Npkmf_ResolveRemoteUserId API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), 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 Npkmf_ResolveRemoteUserId 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 Npkmf_ResolveRemoteUserId service.

The Npkmf_ResolveRemoteUserId API defines a single scope "npkmf-userid" 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 5G PKMF service instance, within the same 5G PKMF or a different 5G PKMF of an 5G PKMF set, e.g. when an 5G PKMF service instance is part of an 5G PKMF (service) set or when using indirect communications (see 3GPP TS 29.500 [5]).

An SCP that reselects a different 5G PKMF producer instance will return the NF Instance ID of the new 5G PKMF producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [5].

If an 5G PKMF within an 5G PKMF set redirects a service request to a different 5G PKMF of the set using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new 5G PKMF 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 [5].

6.3 Npkmf_Discovery Service API

6.3.1 Introduction

The Npkmf_Discovery shall use the Npkmf_Discovery API.

The API URI of the Npkmf_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 "npkmf-discovery".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.3.3.

6.3.2 Usage of HTTP

6.3.2.1 General

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

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [5].

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

6.3.2.2 HTTP standard headers

6.3.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [5] for the usage of HTTP standard headers.

6.3.2.2.2 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 [5]. 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 7807 [10].

6.3.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [5] shall be applicable, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [5] may be supported.

6.3.3 Resources

6.3.3.1 Overview

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

Figure 6.3.3.1-1 describes the resource URI structure of the Npkmf_Discovery API.

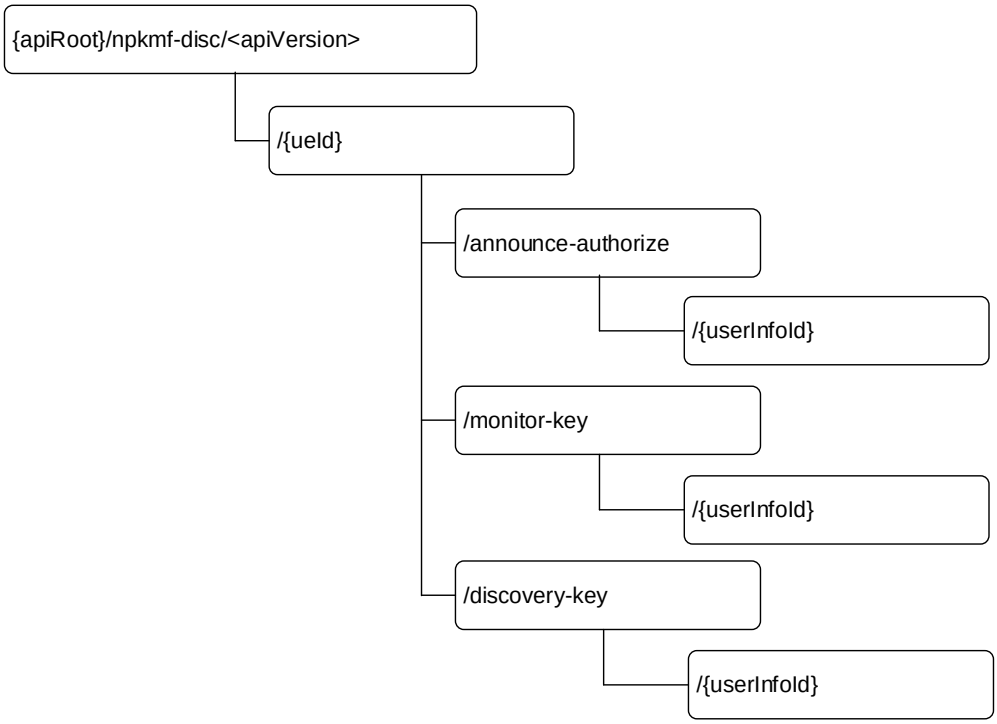

Figure 6.3.3.1-1: Resource URI structure of the Npkmf_Discovery API

Table 6.3.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.3.3.1-1: 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 5G PKMF for announcing in the PLMN
MonitorKey	/{ueId}/monitor-key/{userInfoId}	PUT	Obtain the discovery key from the 5G PKMF for monitoring in the PLMN
DiscoveryKey	/{ueId}/discovery-key/{userInfoId}	PUT	Obtain the discovery key from the 5G PKMF for a discoverer UE in the PLMN to operate Model B restricted discovery

NOTE: The Custom operation URI above are deviating from the URI Path Segment Naming Conventions defined in clause 5.1.3.2 of 3GPP TS 29.501 [5], but they are not changed to maintain backwards compatibility.

6.3.3.2 Resource: AnnounceAuthorize

6.3.3.2.1 Description

6.3.3.2.2 Resource Definition

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

This resource shall support the resource URI variables defined in table 6.3.3.2.2-1.

Table 6.3.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.3.1
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 [16]
userInfoId	UserInfoId	Represents User Info Id.

6.3.3.2.3 Resource Standard Methods

6.3.3.2.3.1 PUT

This method shall support the URI query parameters specified in table 6.3.3.2.3.1-1.

Table 6.3.3.2.3.1-1: 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 6.3.3.2.3.1-2 and the response data structures and response codes specified in table 6.3.3.2.3.1-3.

Table 6.3.3.2.3.1-2: 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 6.3.3.2.3.1-3: 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 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: - PROSE_SERVICE_UNAUTHORIZED See table 6.3.7.3-1 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 [5] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [5].				

Table 6.3.3.2.3.1-4: 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}/npkmf-disc/<apiVersion>/{ueId}/announce-authorize/{userInfoId}

Table 6.3.3.2.3.1-5: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

Table 6.3.3.2.3.1-6: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

6.3.3.3 Resource: MonitorKey

6.3.3.3.1 Description

This resource represents the Monitor Key.

6.3.3.3.2 Resource Definition

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

This resource shall support the resource URI variables defined in table 6.3.3.3.2-1.

Table 6.3.3.3.2-1: 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 [16]
userInfoId	UserInfoId	Represents User Info Id.

6.3.3.3.3 Resource Standard Methods

6.3.3.3.3.1 PUT

This method shall support the URI query parameters specified in table 6.3.3.3.3.1-1.

Table 6.3.3.3.3.1-1: 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 6.3.3.3.3.1-2 and the response data structures and response codes specified in table 6.3.3.3.3.1-3.

Table 6.3.3.3.3.1-2: Data structures supported by the PUT Request Body on this resource

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

Table 6.3.3.3.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MonitorKeyRespData	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 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: - PROSE_SERVICE_UNAUTHORIZED See table 6.3.7.3-1 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 6.3.7.3-1 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 [5] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [5].				

Table 6.3.3.3.3.1-4: 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}/npkmf-disc/<apiVersion>/{ueId}/monitor-key/{userInfoId}

Table 6.3.3.3.3.1-5: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

Table 6.3.3.3.3.1-6: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

6.3.3.4 Resource: DiscoveryKey

6.3.3.4.1 Description

This resource represents the Discovery Key.

6.3.3.4.2 Resource Definition

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

This resource shall support the resource URI variables defined in table 6.3.3.4.2-1.

Table 6.3.3.4.2-1: 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 [16]
userInfoId	UserInfoId	Represents User Info Id.

6.3.3.4.3 Resource Standard Methods

6.3.3.4.3.1 PUT

This method shall support the URI query parameters specified in table 6.3.3.4.3.1-1.

Table 6.3.3.4.3.1-1: 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 6.3.3.4.3.1-2 and the response data structures and response codes specified in table 6.3.3.4.3.1-3.

Table 6.3.3.4.3.1-2: Data structures supported by the PUT Request Body on this resource

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

Table 6.3.3.4.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
DiscoveryKeyRespData	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: - PROSE_SERVICE_UNAUTHORIZED See table 6.3.7.3-1 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 6.3.7.3-1 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 [5] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [5].				

Table 6.3.3.4.3.1-4: 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}/npkmf-disc/<apiVersion>/{ueId}/discovery-key/{userInfoId}

Table 6.3.3.4.3.1-5: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

Table 6.3.3.4.3.1-6: 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 5G PKMF or 5G PKMF (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 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 5G PKMF (service) instance ID towards which the request is redirected

6.3.4 Custom Operations without associated resources

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

6.3.5 Notifications

There is no notification defined for Npkmf_Discovery service.

6.3.6 Data Model

6.3.6.1 General

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

Table 6.3.6.1-1 specifies the data types defined for the Npkmf_Discovery service based interface protocol.

Table 6.3.6.1-1: Npkmf_Discovery specific Data Types

Data type	Clause defined	Description	Applicability
AnnounceAuthData	6.3.6.2.2	Represents Data used to request the authorization to announce for a UE	
MonitorKeyReqData	6.3.6.2.3	Represents Data used to request the discovery key data to monitor for a UE	
MonitorKeyRespData	6.3.6.2.4	Represents the obtained Monitor discovery key data for a UE	
DiscoveryKeyReqData	6.3.6.2.5	Represents Data used to request the discovery key data for a discoverer UE	
DiscoveryKeyRespData	6.3.6.2.6	Represents the obtained the discovery key data for a discoverer UE.	
DiscSecMaterials	6.3.6.2.7	Represents the discovery security materials	
UeSecurityCapability	6.3.6.3	PC5 UE security capability	
ChosenPc5CipheringAlgorithm	6.3.6.3	The chosen PC5 ciphering algorithm	
Duik	6.3.6.3	Discovery User Integrity Key	
Duck	6.3.6.3	Discovery User Confidentility Key	
Dusk	6.3.6.3	Discovery User Scrambling Key	
UserInfoId	6.3.6.3	User Info ID	

Table 6.3.6.1-2 specifies data types re-used by the Npkmf_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 Npkmf_Discovery service based interface.

Table 6.3.6.1-2: Npkmf_Discovery re-used Data Types

Data type	Reference	Comments	Applicability
VarUeId	3GPP TS 29.571 [15]	String represents the SUPI or GPSI.	
RelayServiceCode	3GPP TS 29.571 [15]	Relay Service Code	

6.3.6.2 Structured data types

6.3.6.2.1 Introduction

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

6.3.6.2.2 Type: AnnounceAuthData

Table 6.3.6.2.2-1: Definition of type AnnounceAuthData

Attribute name	Data type	P	Cardinality	Description	Applicability
relayServCode	RelayServiceCode	M	1	This IE shall indicate the Relay Service Code.	

6.3.6.2.3 Type: MonitorKeyReqData

Table 6.3.6.2.3-1: Definition of type MonitorKeyReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
relayServCode	RelayServiceCode	M	1	This IE shall indicate the Relay Service Code.	
ueSecurityCapability	UeSecurityCapability	M	1	This IE shall indicate the PC5 UE security capability	

6.3.6.2.4 Type: MonitorKeyRespData

Table 6.3.6.2.4-1: Definition of type MonitorKeyRespData

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

6.3.6.2.5 Type: DiscoveryKeyReqData

Table 6.3.6.2.5-1: Definition of type DiscoveryKeyReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
relayServCode	RelayServiceCode	M	1	This IE shall indicate the Relay Service Code.	
ueSecurityCapability	UeSecurityCapability	M	1	This IE shall indicate the PC5 UE security capability	

6.3.6.2.6 Type: DiscoveryKeyRespData

Table 6.3.6.2.6-1: Definition of type DiscoveryKeyRespData

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

6.3.6.2.7 Type: DiscSecMaterials

Table 6.3.6.2.7-1: 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	

6.3.6.3 Simple data types and enumerations

6.3.6.3.1 Introduction

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

6.3.6.3.2 Simple data types

The simple data types defined in table 6.3.6.3.2-1 shall be supported.

Table 6.3.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
UserInfoId	string	User Info ID is a string of hexadecimal characters, encoding the value of the user info ID parameter which is a 48-bit long bit string.	
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 clause 11.3.11 of 3GPP TS 24.554 [16] (starting from octet 1).	
ChosenPc5CipheringAlgorithm	integer	This IE shall indicate the chosen PC5 ciphering algorithm as specified in clause 11.4.2.51 of 3GPP TS 24.554 [16]	
Duik	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUIK" IE as specified in clause 11.6.2.13 of 3GPP TS 24.554 [16].	
Duck	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUCK" IE as specified in clause 11.6.2.14 of 3GPP TS 24.554 [16].	
Dusk	Bytes	String with format "byte" as defined in OpenAPI Specification [7], i.e. base64-encoded characters, encoding the "DUSK" IE as specified in clause 11.6.2.12 of 3GPP TS 24.554 [16].	

6.3.6.4 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 Npkmf_Discovery Service.

6.3.6.5 Binary data

There is no binary data type in Npkmf_Discovery Service.

6.3.7 Error Handling

6.3.7.1 General

For the Npkmf_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 [5] 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 [5].

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

6.3.7.2 Protocol Errors

Protocol errors handling shall be supported as specified in clause 5.2.7 of 3GPP TS 29.500 [5].

6.3.7.3 Application Errors

The application errors defined for the Npkmf_Discovery service are listed in Table 6.3.7.3-1.

Table 6.3.7.3-1: Application errors

Application Error	HTTP status code	Description
PROSE_SERVICE_UNAUTHORIZED	403 Forbidden	It is used when the requested ProSe service is not authorized for this UE Identity.
APPLICATION_NOT_FOUND	404 Not Found	It is used when the requested ProSe Application doesn't exist

6.3.8 Feature negotiation

The optional features in table 6.3.8-1 are defined for the Npkmf_Discovery API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [5].

Table 6.3.8-1: Supported Features

Feature number	Feature Name	Description
N/A		

6.3.9 Security

As indicated in 3GPP TS 33.501 [11] and 3GPP TS 29.500 [5], the access to the Npkmf_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 Npkmf_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 Npkmf_Discovery service.

The Npkmf_Discovery API defines the following scopes "npkmf-keyrequest" for OAuth2 authorization as specified in 3GPP TS 33.501 [8]:

Table 6.3.9-1: OAuth2 scopes defined in Npanf_ProseKey API

Scope	Description
"npkmf-disc"	Access to the Npkmf_Discovery API
"npkmf-disc:announce-authorize:modify"	Access to modify the authorization to announce for a UE in the PLMN
"npkmf-disc:monitor-key:modify"	Access to modify the authorization for monitoring for an UE in the PLMN
"npkmf-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

6.3.10 HTTP redirection

An HTTP request may be redirected to a different 5G PKMF service instance, within the same 5G PKMF or a different 5G PKMF of an 5G PKMF set, e.g. when an 5G PKMF service instance is part of an 5G PKMF (service) set or when using indirect communications (see 3GPP TS 29.500 [5]).

An SCP that reselects a different 5G PKMF producer instance will return the NF Instance ID of the new 5G PKMF producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [5].

If an 5G PKMF within an 5G PKMF set redirects a service request to a different 5G PKMF of the set using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new 5G PKMF 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 [5].

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 Npkmf_PKMFKeyRequest API

```
openapi: 3.0.0

info:
  title: Npkmf_PKMFKeyRequest
  version: 1.0.1
  description: |
    PKMF KeyRequest Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.559 V17.2.0; 5G System; 5G ProSe Key Management Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.559/

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

security:
  - {}
  - oAuth2ClientCredentials:
    - npkmf-keyrequest

paths:
  /prose-keys/request:
    post:
      summary: Request Keying Materials for 5G ProSe
      operationId: ProseKey
      tags:
        - ProSe Keys Collection (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ProseKeyReqData'
      responses:
        '200':
          description: Success
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ProseKeyRspData'
```

```
        '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:
            npkmf-keyrequest: Access to the Npkmf_PKMFKeyRequest API

  schemas:
#
#  Structured Data Types
#
    ProseKeyReqData:
      description: Representation of the input to request the keying material.
      type: object
      properties:
        relayServCode:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RelayServiceCode'
        knrpFreshness1:
          $ref: '#/components/schemas/KnrpFreshnessParameter1'
        resyncInfo:
          $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/ResynchronizationInfo'
        prukId:
          $ref: '#/components/schemas/PrukId'
        suci:
          $ref: 'TS29509_Nausf_UEAuthentication.yaml#/components/schemas/Suci'
      required:
        - relayServCode
        - knrpFreshness1

    ProseKeyRspData:
      description: Representation of the successfully requested keying material.
      type: object
      properties:
        knrp:
          $ref: '#/components/schemas/Knrp'
        knrpFreshness2:
          $ref: '#/components/schemas/KnrpFreshnessParameter2'
        gpi:
          $ref: '#/components/schemas/Gpi'
      required:
        - knrp
        - knrpFreshness2

#
#  Simple Data Types
#
```

```
    PrukId:
      description: User Plane Prose Remote User Key ID
      type: string

    Knrp:
      description: Key for NR PC5
      type: string

    KnrpFreshnessParameter1:
      description: KNRP Freshness Parameter 1
      type: string

    KnrpFreshnessParameter2:
      description: KNRP Freshness Parameter 2
      type: string

    Gpi:
      description: GBA Pushing Information
      type: string


#
#  Enumeration Data Types
#
```

A.3 Npkmf_ResolveRemoteUserId API

```
openapi: 3.0.0

info:
  title: Npkmf_ResolveRemoteUserId
  version: 1.0.0
  description: |
    PKMF Resolve Remote User Id Service.
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.559 V17.3.0; 5G System; 5G ProSe Anchor Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.559/

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

security:
  - {}
  - oAuth2ClientCredentials:
    - npkmf-userid

paths:
  /resolve-id:
    post:
      summary: Retrieve the SUPI of the ProSe Remote UE
      operationId: RetrieveSUPI
      tags:
        - SUPI Retrieval
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ResolveRequest'
        required: true
      responses:
        '200':
          description: Expected response to a valid request
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ResolveResponse'
        '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:
            npkmf-userid: Access to the Npkmf_ResolveRemoteUserId API

  schemas:
#
#  Structured Data Types
#

    ResolveRequest:
      description: Request Data
      type: object
      properties:
        upPrukId:
          $ref: 'TS29559_Npkmf_PKMFKeyRequest.yaml#/components/schemas/PrukId'
        plmnId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnId'
      required:
        - upPrukId

    ResolveResponse:
      description: Response Data
      type: object
      properties:
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
      required:
        - supi

#
#  Simple Data Types
#


#
#  Enumeration Data Types
#
```

A.4 Npkmf_Discovery API

```
openapi: 3.0.0

info:
```

```
  title: Npkmf_Discovery API
  version: '1.0.0'
  description: |
    Npkmf_Discovery Service.
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.559 V17.5.0; 5G System; 5G ProSe Key Management Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.559/

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

security:
  - {}
  - oAuth2ClientCredentials:
    - npkmf-discovery

paths:
  /{ueId}/announce-authorize/{userInfoId}:
    put:
      summary: Obtain the authorization from the 5G PKMF for announcing in the PLMN
      operationId: ObtainAnnounceAuth
      tags:
        - Obtain the authorization from the 5G PKMF for announcing in the PLMN
      security:
        - {}
        - oAuth2ClientCredentials:
          - npkmf-disc
        - oAuth2ClientCredentials:
          - npkmf-disc
          - npkmf-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}/npkmf-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-key/{userInfoId}:
  put:
    summary: Obtain the discovery key from the 5G PKMF for monitoring in the PLMN
    operationId: ObtainMonitorKey
    tags:
      - Obtain the discovery key from the 5G PKMF for monitoring in the PLMN
    security:
      - {}
      - oAuth2ClientCredentials:
        - npkmf-disc
      - oAuth2ClientCredentials:
        - npkmf-disc
        - npkmf-disc:monitor-key: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/MonitorKeyReqData'
      required: true
    responses:
      '201':
        description: Created
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MonitorKeyRespData'
        headers:
          Location:
            description: >
              Contains the URI of the newly created resource, according to the structure:
              {apiRoot}/npkmf-disc>/<apiVersion>/{ueId}/monitor-key/{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-key/{userInfoId}:
  put:
    summary: Obtain the discovery key from the 5G PKMF for a discoverer UE
    operationId: ObtainDiscKey
    tags:
      - Obtain the discovery key for a discoverer UE
    security:
      - {}
      - oAuth2ClientCredentials:
        - npkmf-disc
      - oAuth2ClientCredentials:
        - npkmf-disc
        - npkmf-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/DiscoveryKeyReqData'
      required: true
    responses:
      '201':
        description: Created
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DiscoveryKeyRespData'
        headers:
          Location:
            description: >
              Contains the URI of the newly created resource, according to the structure:
              {apiRoot}/npkmf-disc>/<apiVersion>/{ueId}/discovery-key/{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:
            npkmf-disc: Access to the Npkmf_Discovery API
            npkmf-disc:announce-authorize:modify: >
              Access to modify the authorization to announce for a UE in the PLMN
            npkmf-disc:monitor-key:modify: >
              Access to modify the authorization for monitoring for an UE in the PLMN
            npkmf-disc:discovery-key:modify: >
              Access to modify the authorization from the 5G DDNMF for a discoverer UE
              in the PLMN to operate Model B restricted discovery

  schemas:

# STRUCTURED TYPES:

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

    MonitorKeyReqData:
      type: object
      description: Data used to request the discovery key to monitor for a UE
      required:
        - relayServCode
        - ueSecurityCapability
      properties:
        relayServCode:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RelayServiceCode'
        ueSecurityCapability:
          $ref: '#/components/schemas/UeSecurityCapability'

    MonitorKeyRespData:
      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'
```

```
    DiscoveryKeyReqData:
      type: object
      description: Data used to request the discovery key to monitor for a discoverer UE
      required:
        - relayServCode
        - ueSecurityCapability
      properties:
        relayServCode:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RelayServiceCode'
        ueSecurityCapability:
          $ref: '#/components/schemas/UeSecurityCapability'

    DiscoveryKeyRespData:
      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:
      type: string

    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'

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

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

# ENUMS:
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-04	C4#109-e	C4-222345				Implementation of pCRs agreed in CT4#109-e including C4-222355, C4-222356, C4-222023, C4-222024, C4-222025, C4-222026, C4-222027, C4-222028, C4-222029, C4-222031, C4-222409, C4-222410, C4-222411, C4-222412, C4-222413, C4-222414	0.1.0
2022-05	C4#110-e	C4-223454				Implementation of pCRs agreed in CT4#110-e including C4-223135, C4-223157, C4-223158, C4-223160, C4-223351, C4-223352, C4-223416, C4-223417	0.2.0
2022-06	CT#96	CP-221082				TS presented for information and approval	1.0.0
2022-06	CT#96	CP-221082				TS approved in CT#96	17.0.0
2022-09	CT#97e	CP-222035	0001	-	F	Alignment on the service name used with template	17.1.0
2022-12	CT#98e	CP-223054	0003	2	F	PRUK Name Alignment	17.2.0
2022-12	CT#98e	CP-223054	0004	-	F	Correct the server url and some table styles	17.2.0
2022-12	CT#98e	CP-223054	0006	-	F	Update on the procedure title	17.2.0
2022-12	CT#98e	CP-223066	0007	-	F	29.559 Rel-17 API version and External doc update	17.2.0
2023-06	CT#100	CP-231202	0010	3	F	Add service Npkmf_ResolveRemoteUserId	18.0.0
2023-06	CT#100	CP-231026	0008	3	F	Location header description	18.0.0
2023-09	CT#101	CP-232071	0018	1	A	Remove the EN and add the missing reference point	18.1.0
2023-12	CT#102	CP-233069	0024	3	A	Npkmf_Discovery_AnnounceAuthorize service operation	18.2.0
2023-12	CT#102	CP-233069	0026	1	A	Npkmf_Discovery_MonitorKey service operation	18.2.0
2023-12	CT#102	CP-233069	0028	1	A	Npkmf_Discovery_DiscoveryKey service operation	18.2.0
2023-12	CT#102	CP-233055	0029	-	F	Align with the SBI template	18.2.0
2023-12	CT#102	CP-233055	0031	-	F	PKMF replace by 5G PKMF	18.2.0
2023-12	CT#102	CP-233028	0032	1	F	RFC7540 obsoleted by RFC9113	18.2.0
2023-12	CT#102	CP-233055	0033	1	B	Enhancement to support UE-to-UE relay	18.2.0
2023-12	CT#102	CP-233030	0035	-	F	ProblemDetails RFC 7807 obsoleted by 9457	18.2.0
2024-06	CT#104	CP-241050	0039	1	F	Clarification on URI Path Segment Naming Conventions	18.3.0
2024-06	CT#104	CP-241050	0040	1	F	Clarifying the self-references	18.3.0

History

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