ETSI TS 129 559 V17.1.0 (2022-10)

5G;
5G System;
5G ProSe Key Management Services;
Stage 3
(3GPP TS 29.559 version 17.1.0 Release 17)

Reference
RTS/TSGC-0429559vh10

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 http://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 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

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

[10] IETF RFC 7807: "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].

5G PKMF: 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; and for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay.

PKMF Key Request: A procedure employed by the 5G PKMF of the 5G ProSe Remote UE to request the discovery security materials to the 5G PKMFs of the potential 5G ProSe UE-to-Network Relays from which the 5G ProSe Remote UE gets the relay services; or employed by the 5G PKMF of the 5G ProSe UE-to-Network Relay to request the security materials (e.g. PRUK key) for PC5 communication with the 5G ProSe Remote UE from the 5G PKMF of the 5G ProSe Remote UE.

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
PRUK	Prose Remote User Key
RPAUID	Restricted ProSe Application User ID
PDUID	ProSe Discovery UE ID

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; and for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network 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:

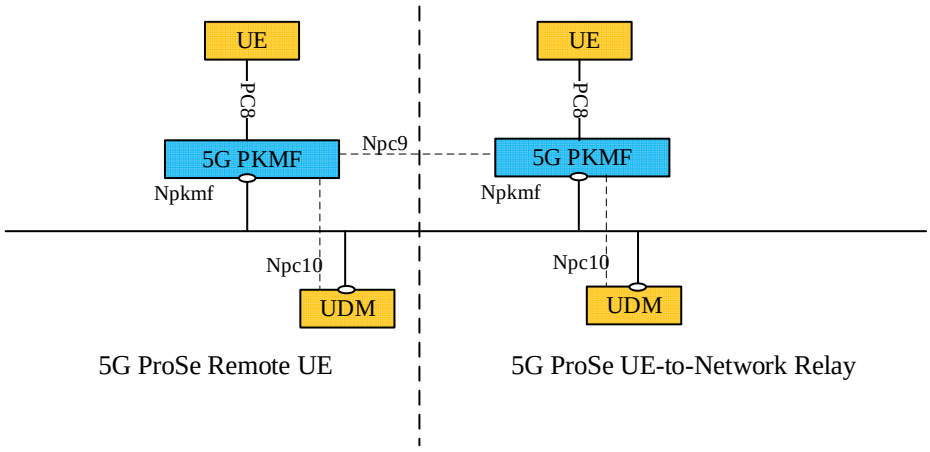

Figure 4-1: Reference model – 5G PKMF

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

NOTE: Only service based interfaces between 5G PKMFs will be covered in this TS, other interfaces won't be covered for the time being.

5 Services offered by the 5G PKMF

5.1 Introduction

The table 5.1-1 shows the PKMF Services and 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	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

5.2 Npkmf_PKMFKeyRequest Service

5.2.1 Service Description

This service enables an NF (i.e. another 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 PKMF in another PLMN, towards the PKMF to retrieve the keying material related to 5G ProSe.

The ProseKey service operation is used during the following procedure:

- 5G ProSe Remote UE attaching to a 5G ProSe UE-to-Network Relay (see 3GPP TS 33.503 [4], clause 6.3.3.2.2)

The NF Service Consumer (i.e. another 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.

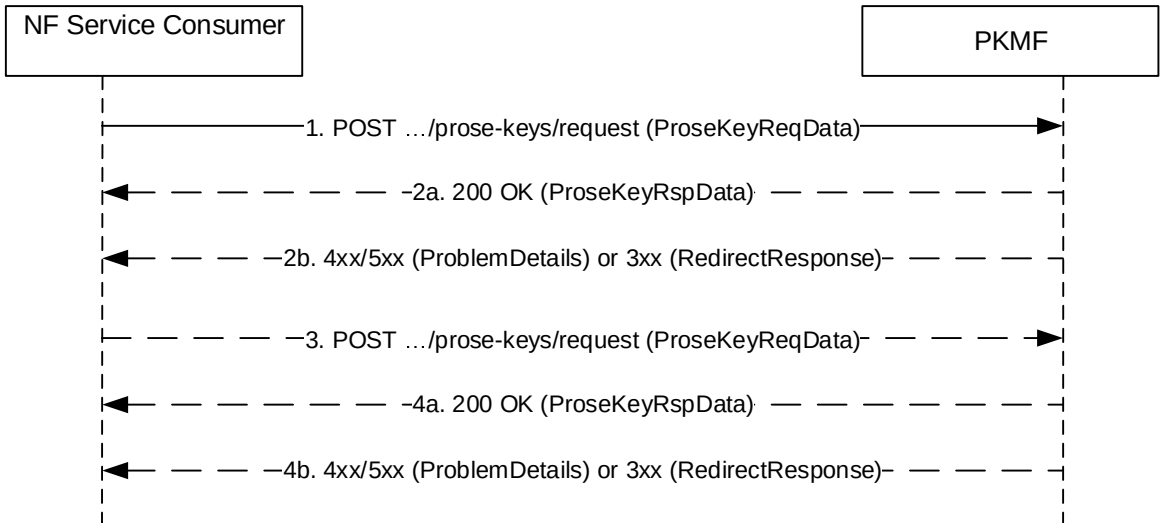

Figure 5.2.2.2.1-1 ProseKey service operation

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 Remote UE or the PRUK ID.

2a. On success, the 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 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.

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 7540 [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 7807 [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.

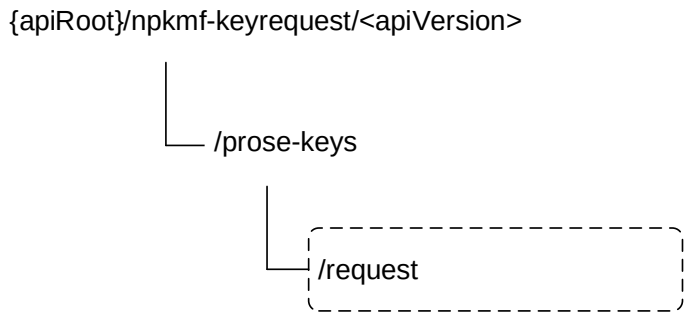

Figure 6.1.3.1-1: Resource URI structure of the Npkmf_PKMFKeyRequest API

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 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 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. The response shall include a Location header field containing a different URI, or the same URI if a request is redirected to the same target resource via a different SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same PKMF or PKMF (service) set. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if a request is redirected to the same target resource via a different SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same PKMF or PKMF (service) set. (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 PKMF or PKMF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 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 PKMF or PKMF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target 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	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 5G ProSe Remote UE.	
knrpFreshness1	KnrpFreshnessParameter1	M	1	This IE shall carry the K_{NRP} Freshness Parameter 1 in 5G ProSe Remote 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 5G ProSe Remote 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 PRUK ID from 5G ProSe Remote 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 5G ProSe Remote 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 PKMF.	
knrpFreshness2	KnrpFreshnessParameter2	M	1	This IE shall carry the K_{NRP} Freshness Parameter 2 generated by the 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	Prose Remote User Key ID String type as defined in OpenAPI Specification [7], carrying the value of the "PRUK ID" IE via PC8 (with "xs:string" type in XML schema) as specified in 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" IE via PC8 (with "xs:hexBinary" type in XML schema) as specified in 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" IE via PC8 (with "xs:hexBinary" type in XML schema) as specified in 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" IE via PC8 (with "xs:hexBinary" type in XML schema) as specified in 3GPP TS 24.554 [16].	
Gpi	string	GBA Push Information String type as defined in OpenAPI Specification [7], carrying the value of the "GPI" IE via PC8 (with "xs:hexBinary" type in XML schema) as specified in 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 PRUK ID is not found in the 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].

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: 1.0.0
  description: |
    PKMF KeyRequest Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.559 V17.0.0; 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-keyerquest/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: 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
#
```

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

History

Document history		
V17.0.0	July 2022	Publication
V17.1.0	October 2022	Publication