ETSI TS 129 535 V18.6.0 (2025-01)

5G;
5G System;
AKMA Anchor Services;
Stage 3
(3GPP TS 29.535 version 18.6.0 Release 18)

Reference
RTS/TSGC-0329535vi60

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 IPR online database.

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™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

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 AAnF Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the AAnF.

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 33.535 [14].

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

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

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

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

[7] 3GPP TR 21.900: "Technical Specification Group working methods".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

[10] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[11] IETF RFC 9113: "HTTP/2".

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

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

[14] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

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

[16] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[17] 3GPP TS 29.503: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[18] 3GPP TS 29.122: "T8 reference point for Northbound Application Programming Interfaces (APIs)".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

3.2 Symbols

No symbol applies in this release of the specification.

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].

AAnF	AKMA Anchor Function
AF	Application Function
AKMA	Authentication and Key Management for Applications
A-KID	AKMA Key IDentifier
AUSF	AUthentication Server Function
NEF	Network Exposure Function
GPSI	Generic Public Subscription Identifier

4 Services offered by the AAnF

4.1 Introduction

The AKMA Anchor Service is used for the AAnF to store AKMA related key material and provide AKMA Application Key information. The AAnF offers to other NFs the following service:

- Naanf_AKMA.

Table 4.1-1: Service provided by AAnF

Service Name	Description	Service Operations	Operation Semantics	Example Consumer(s)
Naanf_AKMA	This service enables the NF service consumers to request the AAnF to store the AKMA related key material or get the AKMA Application Key information from the AAnF.	AnchorKey_Register	Request/Response	AUSF
		ApplicationKey_Get	Request/Response	AF, NEF
		Notify	Request/Response	AF, NEF
		ApplicationKey_AnonUser_Get (NOTE 2)	Request/Response	AF
		ContextRemove	Request/Response	AUSF

NOTE 1: The service corresponds to the Naanf_AKMA service as defined in 3GPP TS 33.535 [14].
NOTE 2: The ApplicationKey_AnonUser_Get service operation is defined reusing the ApplicationKey_Get service operation.

Table 4.1-2 summarizes the corresponding APIs defined for this specification.

Table 4.1-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Naanf_AKMA	4.2	API for Naanf_AKMA	TS29535_Naanf_AKMA.yaml	naanf-akma	Annex A.2 Naanf_AKMA API

4.2 Naanf_AKMA Service

4.2.1 Service Description

4.2.1.1 Overview

The Naanf_AKMA, as defined in 3GPP TS 33.535 [14] is provided by the AKMA Anchor Function (AAnF).

This service:

- allows consumer NFs to store the AKMA related key material.
- allows consumer NFs and the AFs to request the AKMA Application Key information for the UE.

4.2.1.2 Service Architecture

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The Authentication and Key Management for Applications architecture is defined in 3GPP TS 33.535 [14].

The Naanf_AKMA service is part of the Naanf service-based interface exhibited by the AAnF.

Known consumers of the Naanf_AKMA service are:

- AUthentication Server Function (AUSF)
- Application Function (AF)
- Network Exposure Function (NEF)

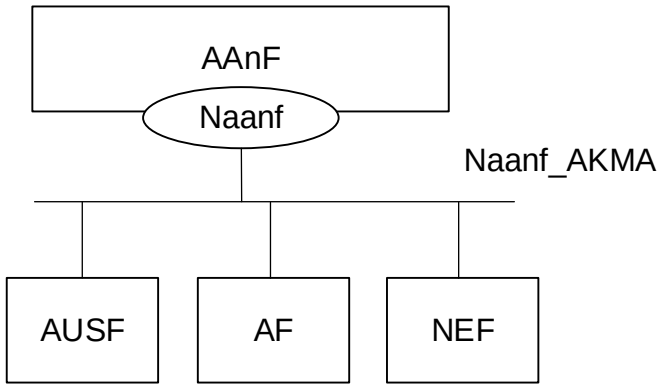

Figure 4.2.1.2-1: Reference Architecture for the Naanf_AKMA Service; SBI representation

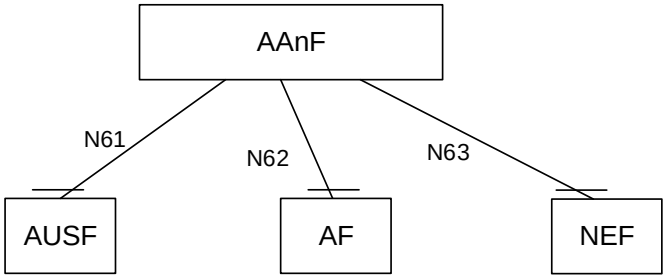

Figure 4.2.1.2-2: Reference Architecture for the Naanf_AKMA Service; reference point representation

4.2.1.3 Network Functions

4.2.1.3.1 AKMA Anchor Function (AAnF)

The AKMA Anchor Function (AAnF) is a functional element that stores the AKMA Anchor Key (K_{AKMA}), A-KID for AKMA service, which is received from the AUSF after the UE completes a successful 5G primary authentication. The AAnF also generates the key material to be used between the UE and the Application Function (AF) and maintains the UE AKMA context as defined in 3GPP TS 33.535 [14].

4.2.1.3.2 NF Service Consumers

The known NF service consumers are as follows:

The AUthentication Server Function (AUSF):

- provides the AKMA key material of the UE to the AAnF; and
- notify an NF service consumer on AKMA service disablement.

The Network Exposure Function (NEF):

- enables and authorizes the external AF accessing AKMA service and forwards the request towards the AAnF;
- performs the AAnF selection.

The Application Function (AF):

- requests for AKMA Application Key from the AAnF;
- shall be authenticated and authorized by the operator network before receiving the K_{AF} from the AAnF;
- performs the AAnF selection if the AF located inside the operator's network.

4.2.2 Service Operations

4.2.2.1 Introduction

Table 4.2.2.1-1: Operations of the Naanf_AKMA Service

Service operation name	Description	Initiated by
Naanf_AKMA_AnchorKey_Register	This service operation is used by an NF to store the AKMA related key material.	AUSF
Naanf_AKMA_ApplicationKey_Get	This service operation is used by an NF to request the AKMA Application Key information for the UE	NEF, AF
Naanf_AKMA_ApplicationKey_AnonUser_Get	This service operation is used by an AF to request the AKMA Application Key information for the UE when authorized AF are not expected to receive the SUPI of the UE	AF
Naanf_AKMA_ContextRemove	This service operation is used by an NF to delete the AKMA related key material.	AUSF
Naanf_AKMA_Notify	This service operation is used by the AAnF to notify a previously subscribed NF service consumer on AKMA service disablement.	AAnF
Naanf_AKMA_Notify	This service operation is used by the AAnF to notify a previously subscribed NF service consumer on AKMA service disablement.	AAnF

4.2.2.2 Naanf_AKMA_AnchorKey_Register service operation

4.2.2.2.1 General

The procedures support:

- store the AKMA related key material by the NF service consumer to the AAnF as described in 3GPP TS 33.535 [14];

4.2.2.2.2 Store the AKMA related key material

Figure 4.2.2.2.2-1 illustrates the registration of AKMA related key material at the AAnF.

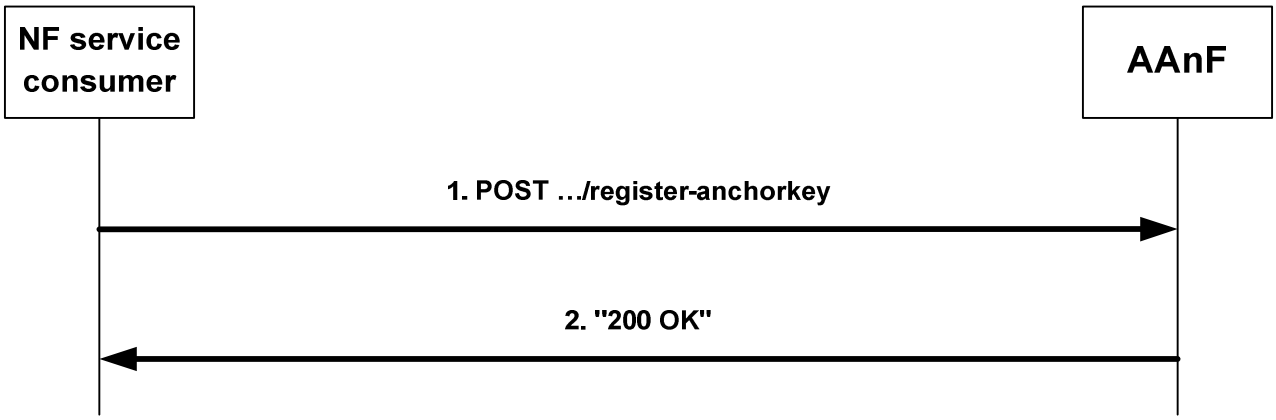

Figure 4.2.2.2.2-1: Registration of AKMA related key material

In order to store the AKMA related key material, the NF service consumer shall send an HTTP POST request message to the resource URI "{apiRoot}/naanf-akma/<apiVersion>/register-anchorkey" as shown in step 1 of figure 4.2.2.2.2-1, and the AkmaKeyInfo data structure as request body.

The AkmaKeyInfo data structure shall include:

- SUPI as "supi" attribute;

- A-KID as "aKId" attribute; and
- K_{AKMA} as "kAkma" attribute.

If the AAnF cannot successfully fulfil the received HTTP POST request due to an internal error or an error in the HTTP POST request, the AAnF shall send an HTTP error response as specified in clause 5.1.7.

If the AAnF determines the received HTTP POST request needs to be redirected, the AAnF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

Upon successful reception of an HTTP POST request, the AAnF shall store the key material information and respond to the NF service consumer with a 200 OK status code, including the AkmaKeyInfo data structure as response body.

4.2.2.3 Naanf_AKMA_ApplicationKey_Get service operation

4.2.2.3.1 General

The Naanf_AKMA_ApplicationKey_Get service operation is used by an NF service consumer to request the AKMA Application Key information for the UE.

4.2.2.3.2 AKMA Application Key request

Figure 4.2.2.3.2-1 shows a scenario where the NF service consumer sends a request to the AAnF to request and get the AKMA Application Key information for the UE (as shown in 3GPP TS 33.535 [14]).

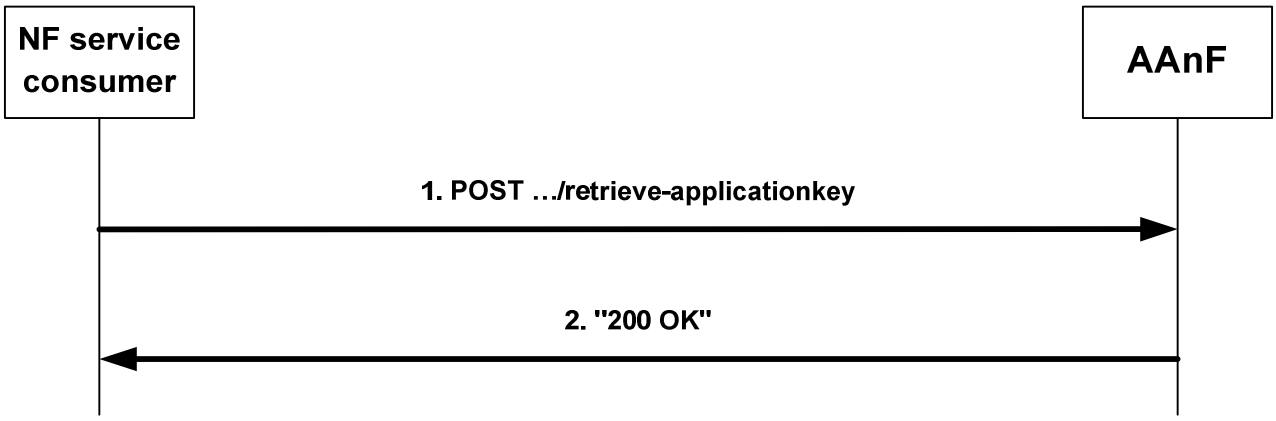

Figure 4.2.2.3.2-1: NF service consumer retrieve AKMA Application Key information

The NF service consumer shall invoke the Naanf_AKMA_ApplicationKey_Get service operation to retrieve the AKMA Application Key information. The NF service consumer shall send for this purpose an HTTP POST request with "{apiRoot}/naanf-akma/<apiVersion>/retrieve-applicationkey" as Resource URI, as shown in step 1 of figure 4.2.2.3.2-1, and the request body containing the AkmaAfKeyRequest data structure.

If the request corresponds to a Naanf_AKMA_ApplicationKey_AnonUser_Get request, then the AkmaAfKeyRequest shall contain the "anonInd" attribute set to "true".

If the AAnF determines the received HTTP POST request needs to be redirected, the AAnF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

If the AAnF cannot successfully fulfil the received HTTP POST request due to an internal error or an error in the HTTP POST request, the AAnF shall send an HTTP error response as specified in clause 5.1.7.

The AAnF shall also verify the presence of the UE specific K_{AKMA} key identified by the A-KID.

- If K_{AKMA} is not present in the AAnF, the AAnF shall reply with an HTTP "403 Forbidden" status code and the response message body including a ProblemDetails data structure with the "cause" attribute set to the "K_AKMA_NOT_PRESENT" application error specified in table 5.1.7.3-1.
- If K_{AKMA} is present in the AAnF, the AAnF shall continue and process the request as specified below.

Upon the reception of the HTTP POST request, the AAnF shall respond with an HTTP "200 OK" status code and the response message body containing the AkmaAfKeyData data structure which shall include:

- K_{AF} as "kaf" attribute;
- K_{AF} expiration time as "expiry" attribute; and
- if the "anonInd" attribute was not present in the request or it was present and set to "false", the SUPI within the "supi" attribute or, if the "AKMA_GPSI_Support" feature is supported, either the SUPI within the "supi" attribute or the GPSI within the "gpsi" attribute.

If the requested AKMA Application Key information for the UE does not exist, the AAnF shall respond with "204 No Content".

If the NF service consumer is an NEF, and if UE identifier is required to relay to the AF based on local policy, the NEF invokes the Nudm_SubscriberDataManagement service defined in 3GPP TS 29.503 [17] to translate the SUPI to a GPSI (External Id), and then invoke the AKMA API to include the GPSI (External Id) in the response to the AF as defined in 3GPP TS 29.522 [16]. The NEF shall not send the SUPI to the AF.

If the AAnF identifies that the request is targeting a UE that is currently roaming (e.g. the AAnF have received a roaming status information reporting from the UDM indicating that the UE is currently roaming) and if the AKMA service is not allowed for the roaming UE (e.g., based on the local policy), the AAnF shall reply with an HTTP "403 Forbidden" status code with the response message body including a ProblemDetails data structure containing the "cause" attribute set to the "ROAMING_AKMA_SERVICE_DENIED" application error as specified in clause 5.1.7.3.

NOTE: The UE is considered as roaming if at least one of the serving PLMNs of the UE registered PLMN(s) is a VPLMN.

4.2.2.4 Naanf_AKMA_ContextRemove service operation

4.2.2.4.1 General

The Naanf_AKMA_ContextRemove service operation is used by an NF service consumer to request the AAnF to remove the AKMA related key material.

4.2.2.4.2 AKMA Context removal

Figure 4.2.2.4.2-1 shows a scenario where the NF service consumer sends a request to the AAnF to delete the AKMA related key material (as shown in 3GPP TS 33.535 [14]).

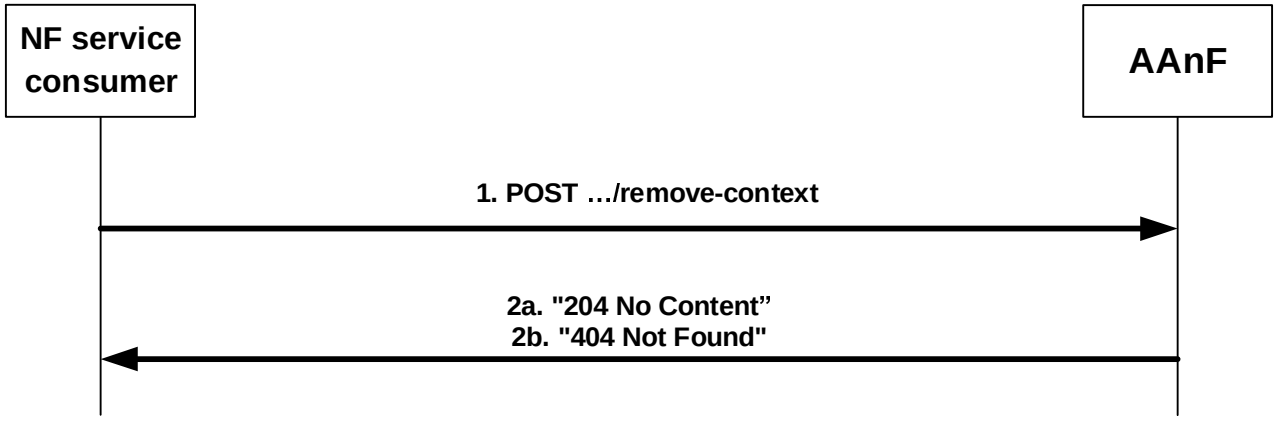

Figure 4.2.2.4.2-1: NF service consumer request to remove the AKMA related key material

The NF service consumer shall invoke the Naanf_AKMA_ContextRemove service operation to request the AAnF to remove the AKMA related key material. The NF service consumer shall send an HTTP POST request with "{apiRoot}/naanf-akma/<apiVersion>/remove-context" as Resource URI, as shown in figure 4.2.2.4.2-1, step 1, to request to remove AKMA related key material according to the value of the "CtxRemove" data type in the request body.

If errors occur when processing the HTTP POST request, the AAnF shall send an HTTP error response as specified in clause 5.1.7.

If the AAnF determines the received HTTP POST request needs to be redirected, the AAnF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

Upon the reception of the HTTP POST request, if the AKMA context (e.g. A-KID, K_{AKMA}) for the UE has been removed successfully, the AAnF shall send an HTTP "204 No Content" response.

If the AKMA Context resource does not exist, the AAnF shall respond with "404 Not Found" and the "cause" attribute of the "ProblemDetails" data structure set to "AKMA_CONTEXT_NOT_FOUND".

4.2.2.5 Naanf_AKMA_Notify service operation

4.2.2.5.1 General

The Naanf_AKMA_Notify service operation is used by the AAnF to notify a previously subscribed service consumer on AKMA service disablement.

4.2.2.5.2 AKMA Service Disablement Notification

Figure 4.2.2.5.2-1 shows a scenario where the AAnF sends a notification to the NF service consumer on AKMA service disablement (see also 3GPP TS 33.535 [14]).

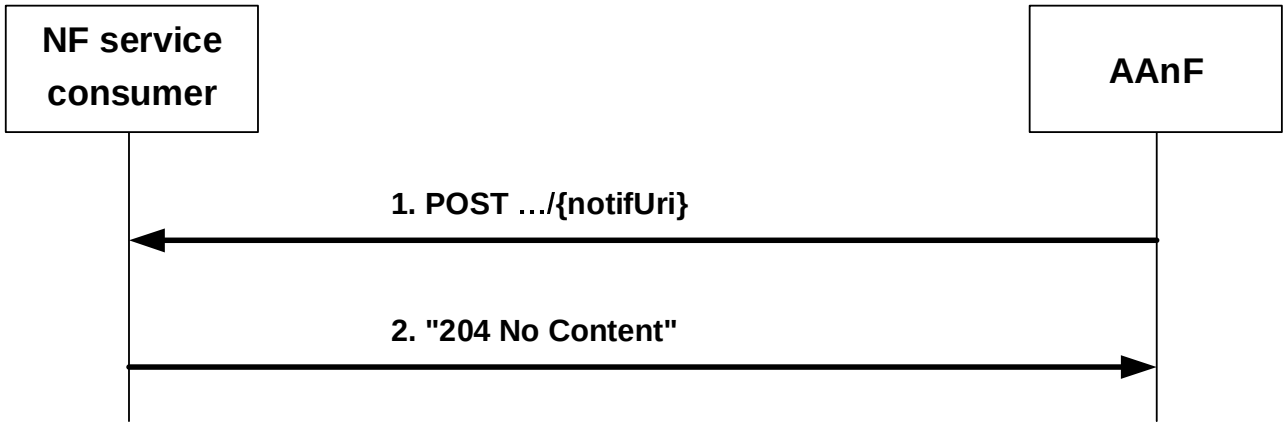

Figure 4.2.2.5.2-1: AAnF notification to NF service consumer

In order to notify a previously subscribed service consumer on AKMA service disablement, the AAnF shall invoke the Naanf_AKMA_Notify service operation by sending an HTTP POST request to the NF service consumer using the notification URI received during the related AKMA application key request procedure, as specified in clause 4.2.2.3.2, and the request body including the ServiceDisableNotif data structure.

Upon reception of the notification, the NF service consumer shall acknowledge the successful reception of the notification with a "204 No Content" status code.

If errors occur when processing the HTTP POST request, the NF service consumer shall send an appropriate HTTP error response as specified in clause 5.1.7. If the service consumer determines the received HTTP POST request needs to be redirected, the service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

5 API Definitions

5.1 Naanf_AKMA Service API

5.1.1 Introduction

The Naanf_AKMA service shall use the Naanf_AKMA API.

The API URI of the Naanf_AKMA 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 [5], i.e.:

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

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].
- The <apiName> shall be "naanf-akma".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 5.1.3 and 5.1.4.

5.1.2 Usage of HTTP

5.1.2.1 General

HTTP/2, IETF RFC 9113 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

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

The OpenAPI [6] specification of HTTP messages and content bodies for the Naanf_AKMA API is contained in Annex A.

5.1.2.2 HTTP standard headers

5.1.2.2.1 General

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

5.1.2.2.2 Content type

JSON, IETF RFC 8259 [12], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 9457 [13].

5.1.2.3 HTTP custom headers

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

In this release of the specification, no specific custom headers are defined for the Naanf_AKMA Service API.

5.1.3 Resources

There are no resources defined for this API in this release of the specification.

5.1.4 Custom Operations without associated resources

5.1.4.1 Overview

The structure of the custom operation URIs of the Naanf_AKMA API is shown in figure 5.1.4.1-1.

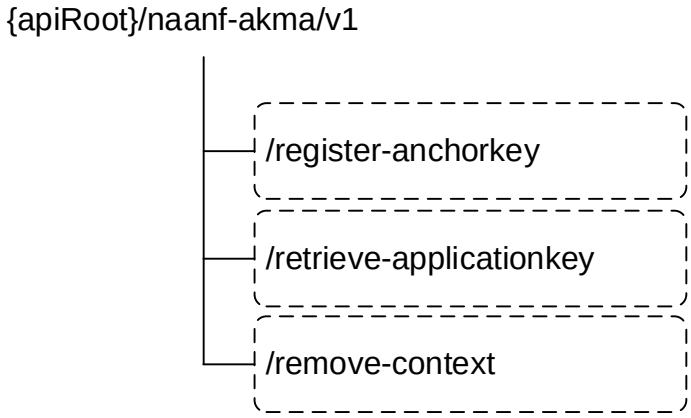

Figure 5.1.4.1-1: Custom operation URI structure of the Naanf_AKMA API

Table 5.1.4.1-1 provides an overview of the custom operations and applicable HTTP methods defined for the Naanf_AKMA API.

Table 5.1.4.1-1: Custom operations without associated resources

Operation	Custom operation URI	Mapped HTTP method	Description
register-anchorkey	/register-anchorkey	POST	Request to store AKMA related key material in the AAnF.
retrieve-applicationkey	/retrieve-applicationkey	POST	Request to retrieve AKMA Application Key information.
remove-context	/remove-context	POST	Request to remove AKMA context in the AAnF.

5.1.4.2 Operation: Register

5.1.4.2.1 Description

The custom operation allows a NF service consumer to store AKMA related key material in the AAnF.

5.1.4.2.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 5.1.4.2.2-1 and 5.1.4.2.2-2.

Table 5.1.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
AkmaKeyInfo	M	1	AKMA related key material which is requested to be stored in the AAnF

Table 5.1.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AkmaKeyInfo	M	1	200 OK	The AKMA related key material was stored successfully.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during the retrieval notification. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during the retrieval notification. (NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: The RedirectResponse data structure may be provided by an SCP (cf. clause 6.10.9.1 of 3GPP TS 29.500 [4]).				

Table 5.1.4.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification is redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected.

Table 5.1.4.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected.

5.1.4.3 Operation: Retrieve

5.1.4.3.1 Description

The custom operation allows a NF service consumer to retrieve AKMA Application Key information for the UE.

5.1.4.3.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 5.1.4.3.2-1 and 5.1.4.3.2-2.

Table 5.1.4.3.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
AkmaAfKeyRequest	M	1	Parameters to request to retrieve AKMA Application Key information.

Table 5.1.4.3.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AkmaAfKeyData	M	1	200 OK	The requested AKMA Application Key information was returned successfully. (NOTE 2)
n/a			204 No Content	If the requested data does not exist, the AAnF shall respond with "204 No Content".
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during the retrieval notification. (NOTE 4)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during the retrieval notification. (NOTE 4)
ProblemDetails	O	0..1	403 Forbidden	(NOTE 3)
NOTE 1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: For the "AkmaAfKeyData" data structure used in the current release of this specification, the “gpsi” attribute is not applicable and the "supi" attribute shall be included, except in the case of the anonymous user access procedure using the Naanf_AKMA_ApplicationKey_AnonUser_Get service operation, as defined in clause 6.2.2 of 3GPP TS 33.535 [14]. NOTE 3: Failure cases are described in clause 5.1.7.3 NOTE 4: The RedirectResponse data structure may be provided by an SCP (cf. clause 6.10.9.1 of 3GPP TS 29.500 [4]).				

Table 5.1.4.3.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected.

Table 5.1.4.3.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected.

5.1.4.4 Operation: Remove

5.1.4.4.1 Description

The custom operation allows a NF service consumer to delete the AKMA context for the UE.

5.1.4.4.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 5.1.4.4.2-1 and 5.1.4.4.2-2.

Table 5.1.4.4.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
CtxRemove	M	1	Parameters to request to delete the AKMA context for the UE.

Table 5.1.4.4.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful case: The AKMA context matching the "CtxRemove" in the request body was deleted, the AAnF shall respond with "204 No Content".
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during remove procedure. The response shall include a Location header field containing an alternative URI of the resource located in an alternative AAnF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during remove procedure. The response shall include a Location header field containing an alternative URI of the resource located in an alternative AAnF (service) instance.
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 5.1.7.3				

Table 5.1.4.4.2-3: 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 in an alternative AAnF (service) instance.
3gpp-Sbi-Target-Nf-Id	String	O	0..1	Identifier of the target AAnF (service) instance towards which the request is redirected.

Table 5.1.4.4.2-4: 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 in an alternative AAnF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target AAnF (service) instance towards which the request is redirected.

5.1.5 Notifications

5.1.5.1 General

Notifications shall comply to clause 6.2 of 3GPP TS 29.500 [5] and clause 4.6.2.3 of 3GPP TS 29.501 [6].

Table 5.1.5-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
AKMA Service Disablement Notification	{notifUri}	POST	Enables the AAnF to notify a previously subscribed NF service consumer on AKMA service disablement.

5.1.5.2 AKMA Service Disablement Notification

5.1.5.2.1 Description

The AKMA Service Disablement Notification is used by the AAnF to notify a previously subscribed NF service consumer on AKMA service disablement.

5.1.5.2.2 Target URI

The Callback URI **"{notifUri}"** shall be used with the callback URI variables defined in table 5.1.5.2.2-1.

Table 5.1.5.2.2-1: Callback URI variables

Name	Data type	Definition
notifUri	Uri	The Notification URI provided by the NF service consumer during retrievel of AKMA application key as defined in table 5.1.4.3.2-1.

5.1.5.2.3 Standard Methods

5.1.5.2.3.1 POST

This method shall support the request data structures specified in table 5.1.5.2.3.1-1 and the response data structures and response codes specified in table 5.1.5.2.3.1-2.

Table 5.1.5.2.3.1-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
ServiceDisableNotif	M	1	Represents the AKMA Service Disablement Notification.

Table 5.1.5.2.3.1-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful case. The notification is successfully received and acknowledged.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the HTTP POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply. NOTE 2: The RedirectResponse data structure may be provided by an SCP (see clause 6.10.9.1 of 3GPP TS 29.500 [5]).				

Table 5.1.5.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification is redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

Table 5.1.5.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification is redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

5.1.6 Data Model

5.1.6.1 General

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

Table 5.1.6.1-1 specifies the data types defined for the Naanf_AKMA service based interface protocol.

Table 5.1.6.1-1: Naanf_AKMA specific Data Types

Data type	Clause defined	Description	Applicability
AkmaKeyInfo	5.1.6.2.2	AKMA related key material.	
CtxRemove	5.1.6.2.3	Indicate the AKMA context to be remove.	

Table 5.1.6.1-2 specifies data types re-used by the Naanf_AKMA 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 Naanf_AKMA service based interface.

Table 5.1.6.1-2: Naanf_AKMA re-used Data Types

Data type	Reference	Comments	Applicability
AKId	3GPP TS 29.522 [16]		
AkmaAfKeyData	3GPP TS 29.522 [16]	Parameters to present AKMA Application Key information.	
AkmaAfKeyRequest	3GPP TS 29.522 [16]	Parameters to request to retrieve AKMA Application Key information.	
ServiceDisableNotif	3GPP TS 29.522 [16]	Represents the AKMA Service Disablement Notification.	RoamingRestriction
RedirectResponse	3GPP TS 29.571 [15]	Contains redirection related information.	
Supi	3GPP TS 29.571 [15]	Represents the SUPI.	
Gpsi	3GPP TS 29.571 [15]	Represents the GPSI.	
SupportedFeatures	3GPP TS 29.571 [15]	Used to negotiate the applicability of the optional features.	
Uri	3GPP TS 29.122 [18]	Represents a URI.	RoamingRestriction

5.1.6.2 Structured data types

5.1.6.2.1 Introduction

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

5.1.6.2.2 Type: AkmaKeyInfo

Table 5.1.6.2.2-1: Definition of type AkmaKeyInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi	C	0..1	SUPI of the UE. (NOTE)	
aKId	AKId	M	1	A-KID	
kAkma	string	M	1	K_{AKMA}	
gpsi	Gpsi	C	0..1	GPSI of the UE. (NOTE)	AKMA_GPSI_Support
suppFeat	SupportedFeatures	O	0..1	Indicates the list of Supported features used as described in clause 5.1.8.	
NOTE: When the "AKMA_GPSI_Support" feature is supported, the presence of "supi" attribute and the "gpsi" attribute are mutually exclusive. When the "AKMA_GPSI_Support" feature is not supported, only the "supi" attribute shall be present.					

5.1.6.2.3 Type: CtxRemove

Table 5.1.6.2.3-1: Definition of type CtxRemove

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi	C	0..1	SUPI of UE	
NOTE: In current release of specification, only "supi" can be used to indicate the AKMA context to be remove. The "supi" attribute shall be included.					

5.1.6.3 Simple data types and enumerations

5.1.6.3.1 Introduction

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

5.1.6.3.2 Simple data types

None in this release of the specification.

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

None in this release of the specification.

5.1.6.5 Binary data

None in this release of the specification.

5.1.7 Error Handling

5.1.7.1 General

For the Naanf_AKMA API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

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

5.1.7.2 Protocol Errors

No specific procedures for the Naanf_AKMA service are specified.

5.1.7.3 Application Errors

The application errors defined for the Naanf_AKMA service are listed in Table 5.1.7.3-1.

Table 5.1.7.3-1: Application errors

Application Error	HTTP status code	Description	Applicability
K_AKMA_NOT_PRESENT	403 Forbidden	Indicates that the K_{AKMA} identified by the A-KID provided in the AKMA Application Key retrieval request body is not present at the AAnF.	
ROAMING_AKMA_SERVICE_DENIED	403 Forbidden	Indicates that the AAnF identifies the request is for a roaming UE and denies the request if the AKMA service is not allowed for the roaming UE.	RoamingRestriction
AKMA_CONTEXT_NOT_FOUND	404 Not Found	Indicates that the AKMA context to be deleted indicated by the "CtxRemove" Data type in the request body is not found.	

5.1.8 Feature negotiation

The optional features in table 5.1.8-1 are defined for the Naanf_AKMA API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 5.1.8-1: Supported Features

Feature number	Feature Name	Description
1	AKMA_GPSI_Support	This feature indicates the support of sending the GPSI as an alternative UE ID to an internal AF based on local policy.
2	RoamingRestriction	This feature indicates the support of roaming UE detection by the network and the denial of the AKMA services to roaming UEs.

5.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Naanf_AKMA 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 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Naanf_AKMA API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], 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 Naanf_AKMA service.

The Naanf_AKMA API defines the following scopes for OAuth2 authorization as described in clause 4.10 of 3GPP TS 29.501 [5].

Table 5.1.9-1: OAuth2 scopes defined in Naanf_AKMA API

Scope	Description
"naanf-akma"	Access to the Naanf_AKMA API
"naanf-akma:anchorkey"	Access to service operations applying to store and remove the AKMA related key material.
"naanf-akma:applicationkeyget"	Access to service operations applying to request the AKMA Application Key information for the UE.
"naanf-akma:applicationkeyget: supi-access"	Access to the Naanf_AKMA API to enable the returning of SUPI in the AKMA Application Key information for the UE.

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: 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 3GPP TS 29.501 [5] clause 5.3.1 and 3GPP TR 21.900 [7] clause 5B).

A.2 Naanf_AKMA API

```
openapi: 3.0.0
info:
  title: 3gpp-akma
  version: 1.1.0
  description: |
    API for Naanf_AKMA.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.535 V18.4.0; 5G System; AKMA Anchor Services.
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.535/'

security:
  - {}
  - oAuth2ClientCredentials:
    - naanf-akma
servers:
  - url: '{apiRoot}/naanf-akma/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501.


paths:
  /register-anchorkey:
    post:
      summary: Store AKMA related key material.
      operationId: RegisterAKMAKey
      tags:
        - Register the AKMA related key material
      security:
        - {}
        - oAuth2ClientCredentials:
          - naanf-akma
        - oAuth2ClientCredentials:
          - naanf-akma
          - naanf-akma:anchorkey
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/AkmaKeyInfo'
      responses:
```

```
        '200':
          description: The requested information was returned successfully.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AkmaKeyInfo'
        '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'

  /retrieve-applicationkey:
    post:
      summary: Request to retrieve AKMA Application Key information.
      operationId: GetAKMAAPPKeyMaterial
      tags:
        - Retrieve the AKMA Application key material (Collection)
      security:
        - {}
        - oAuth2ClientCredentials:
          - naanf-akma
        - oAuth2ClientCredentials:
          - naanf-akma
          - naanf-akma:applicationkeyget
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: 'TS29522_AKMA.yaml#/components/schemas/AkmaAfKeyRequest'
      responses:
        '200':
          description: The requested information was returned successfully.
          content:
            application/json:
              schema:
                $ref: 'TS29522_AKMA.yaml#/components/schemas/AkmaAfKeyData'
        '204':
          description: No Content (The requested AKMA Application material does not exist.)
        '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:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    callbacks:
      ServiceDisablementNotification:
        '{$request.body#/notifUri}':
          post:
            requestBody:
              description: >
                Represents the AKMA Service Disablement Notification.
              required: true
              content:
                application/json:
                  schema:
                    $ref: 'TS29522_AKMA.yaml#/components/schemas/ServiceDisableNotif'
            responses:
              '204':
                description: No content. The notification is successfully received and processed.
              '307':
                $ref: 'TS29122_CommonData.yaml#/components/responses/307'
              '308':
                $ref: 'TS29122_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29122_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29122_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29122_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29122_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29122_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29122_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29122_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29122_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29122_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29122_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29122_CommonData.yaml#/components/responses/default'

  /remove-context:
    post:
      summary: Request to remove the AKMA related key material.
      operationId: RemoveContext
      tags:
        - Remove the AKMA Application key material (deletion)
      security:
        - {}
        - oAuth2ClientCredentials:
          - naanf-akma
        - oAuth2ClientCredentials:
          - naanf-akma
          - naanf-akma:anchorkey
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/CtxRemove'
      responses:
        '204':
          description: No Content (The AKMA context for the UE has been removed successfully.)
        '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:
            naanf_akma: Access to the Naanf_AKMA API
            naanf_akma:anchorkey: >
              Access to service operations applying to store or remove the AKMA related key
              material.
            naanf_akma:applicationkeyget: >
              Access to service operations applying to request the AKMA Application Key information
              for the UE.
            naanf-akma:applicationkeyget:supi-access: >
              Return SUPI in the AKMA Application Key information for the UE.

  schemas:
    AkmaKeyInfo:
      description: Represents AKMA related key material.
      type: object
      properties:
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        aKId:
          $ref: 'TS29522_AKMA.yaml#/components/schemas/AKId'
        kAkma:
          type: string
      required:
        - aKId
        - kAkma
      oneOf:
        - required: [supi]
        - required: [gpsi]

    CtxRemove:
      description: >
        Parameters to request to delete the AKMA context for the UE, the "supi" attribute shall be
        included.
      type: object
      properties:
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2020-11	CT3#112e					TS skeleton of AKMA Anchor Services.	0.0.0
2020-11	CT3#112e					Inclusion of documents agreed in CT3#112e C3-205585, C3-205586.	0.1.0
2021-01	CT3#113e					Inclusion of documents agreed in CT3#113e C3-210291, C3-210292, C3-210222, C3-210293, C3-210294, C3-210295.	0.2.0
2021-01	CT3#113e					Inclusion of documents agreed in CT3#114e C3-211238. C3-21396, C3-211397, C3-211398, C3-211399, C3-211400, and C3-211401.	0.3.0
2021-03	CT#91e	CP-210182				Sent to plenary for Approval	1.0.0
2021-03	CT#91e	CP-210182				TS approved by plenary	17.0.0
2021-06	CT#92e	CP-211234	0001	1	F	Adding a missing description field to data type definitions in OpenAPI specification files of the Naanf_AKMA API	17.1.0
2021-06	CT#92e	CP-211214	0002	1	F	Adding a missing description field to data type definitions in OpenAPI specification files of the Naanf_AKMA API	17.1.0
2021-06	CT#92e	CP-211214	0003		F	Adding Clause 5.1.4.3.1	17.1.0
2021-06	CT#92e	CP-211214	0005	1	F	Custom operation URI	17.1.0
2021-06	CT#92e	CP-211214	0006		F	Terminology alignment of AKMA Application Key information	17.1.0
2021-06	CT#92e	CP-211234	0007	1	F	Redirect responses with "application/json" media type	17.1.0
2021-06	CT#92e	CP-211234	0008	1	F	Optional header clarification	17.1.0
2021-06	CT#92e	CP-211265	0009		F	Update of OpenAPI version and TS version in externalDocs field	17.1.0
2021-09	CT#93e	CP-212220	0011	1	F	CR 0011 29.535 Rel-17 Correcting CR #0007 implementation	17.2.0
2021-12	CT#94e	CP-213218	0012	2	B	Naanf_AKMA_ContextRemove service operation	17.3.0
2021-12	CT#94e	CP-213218	0014	2	F	Correction on Naanf_AKMA_ApplicationKey_Get service operation on sending UE ID to the AKMA AF	17.3.0
2021-12	CT#94e	CP-213246	0015		F	Update of OpenAPI version and TS version in externalDocs field	17.3.0
2022-01						Update of specification filename in the zip	17.3.1
2022-03	CT#95e	CP-220180	0016		B	Specifying the error case of KAKMA key not present in the AAnF	17.4.0
2022-03	CT#95e	CP-220180	0017	1	F	Miscellaneous corrections	17.4.0
2022-03	CT#95e	CP-220194	0018		F	Update of info and externalDocs fields	17.4.0
2022-06	CT#96	CP-221159	0019		F	Update of info and externalDocs fields	17.5.0
2022-09	CT#97e	CP-222096	0020	2	F	Application errors reference update in the tables defining methods on the resources for Naanf_AKMA API	17.6.0
2022-09	CT#97e	CP-222096	0021	1	F	Support for Naanf_AKMA_ApplicationKey_ AnonUser_Get service operation	17.6.0
2022-09	CT#97e	CP-222096	0023		F	Missing redirection in AKMA Context removal procedure	17.6.0
2022-09	CT#97e	CP-222121	0024		F	Update of info and externalDocs fields	17.6.0
2022-12	CT#98e	CP-223168	0026	1	F	Correction for AKMA Application Key Request	17.7.0
2022-12	CT#98e	CP-223168	0027	1	F	Cardinality for CtxRemove	17.7.0
2022-12	CT#98e	CP-223188	0028		F	Update of info and externalDocs fields	17.7.0
2022-12	CT#98e	CP-223191	0025		F	Adding the mandatory error code 502 Bad Gateway	18.0.0
2022-12	CT#98e	CP-223189	0029		F	Update of info and externalDocs fields	18.0.0
2023-03	CT#99	CP-230167	0030	1	B	OAuth2 scopes in Naanf_AKMA API	18.1.0
2023-03	CT#99	CP-230166	0031		F	Miscellaneous changes in Naanf_AKMA API	18.1.0
2023-03	CT#99	CP-230161	0033		F	Update of info and externalDocs fields	18.1.0
2023-06	CT#100	CP-231131	0034	1	F	Correction of a referenced clause number	18.2.0
2023-06	CT#100	CP-231261	0037	2	B	Including GPSI attribute support	18.2.0
2023-06	CT#100	CP-231132	0040	1	F	Corrections to the redirection mechanism description	18.2.0
2023-06	CT#100	CP-231141	0041		F	Update of info and externalDocs fields	18.2.0
2023-09	CT#101	CP-232086	0039	2	F	Support for SUPI access in AKMA Application Key information	18.3.0
2023-09	CT#101	CP-232085	0042		F	Update of info and externalDocs fields	18.3.0
2023-12	CT#102	CP-233229	0044	1	F	IETF RFC 7540, RFC 7807 obsoleted by RFC 9113 and RFC 9457 respectively	18.4.0
2024-06	CT#104	CP-241095	0046	1	B	Update AKMA procedures to support Roaming restrictions.	18.5.0
2024-06	CT#104	CP-241085	0048		F	Update of info and externalDocs fields	18.5.0
2024-07	CT#105					Correction to fix OpenAPI parsing errors” in the comments	18.5.1
2024-12	CT#106	CP-243103	0050	1	F	Correcting the name of the data type conveying the AKMA service disablement notification	18.6.0

History

Document history		
V18.4.0	May 2024	Publication
V18.5.1	August 2024	Publication
V18.6.0	January 2025	Publication