ETSI TS 129 544 V17.2.0 (2022-05)

5G;
5G System;
Secured Packet Application Function (SP-AF) services;
Stage 3
(3GPP TS 29.544 version 17.2.0 Release 17)

Reference
RTS/TSGC-0429544vh20

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

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

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

[13] IETF RFC 7807: "Problem Details for HTTP APIs".

[14] 3GPP TS 29.503: "Unified Data Management Services"; Stage 3.

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

[16] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[17] 3GPP TS 29.509: "Authentication Server Services; Stage 3".

[18] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)"

[19] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

3 Definitions, symbols and abbreviations

3.1 Terms

Void.

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].

OTA	Over The Air
SOR-AF	Steering Of Roaming Application Function
SP-AF	Secured Packet Application Function
UDM	Unified Data Management

4 Overview

4.1 Introduction

Within the 5GC, the SP-AF offers services to the UDM and to the SOR-AF via the Nspaf service based interface.

The UDM or SOR-AF shall make use of the SP-AF services when it needs to protect UE parameters for which the final consumer is the USIM (see 3GPP TS 33.501 [8] clause 6.15.2.1).

Figure 4.1-1 provides the reference model with focus on the SP-AF.

NOTE: The generation of the secured packet and the definition of the storage and handling of OTA keys or other sensitive data are out of scope of this document. For more details, refer to 3GPP TS 23.040 [18] and 3GPP TS 31.115 [16].

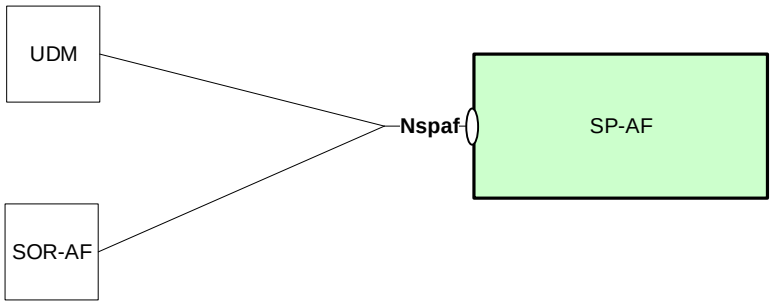

Figure 4.1-1: Reference model – SP-AF

5 Services offered by the SP-AF

5.1 Introduction

The SP-AF offers the following services via the Nspaf interface:

- Nspaf_SecuredPacket Service

Table 5.1-1 summarizes the corresponding APIs defined for this specification.

Table 5.1-1: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Nspaf_SecuredPacket	6.1	Nspaf Secured Packet Service	TS29544_Nspaf_SecuredPacket.yaml	nspaf-secured-packet	A.2

5.2 Nspaf_SecuredPacket Service

5.2.1 Service Description

The Nspaf_SecuredPacket Service may be consumed by the NF consumer (e.g. UDM or SOR-AF) when it has detected that a UICC configuration parameter (e.g. Routing ID data or Steering of Roaming information) needs to be updated, and the new value is not available in secured packet format.

For the list of service operations see clause 5.2.2.1

5.2.2 Service Operations

5.2.2.1 Introduction

For the Nspaf_SecuredPacket service the following service operations are defined:

- Provide

The Nspaf_SecuredPacket Service is used by Consumer NFs (e.g. UDM or SOR-AF) to request the SP-AF to provide a secured packet that contains an UICC configuration parameter as sent in the request by means of the Provide service operation

5.2.2.2 Provide

5.2.2.2.1 General

This service operation is used by the NF Service Consumer (e.g. UDM or SOR-AF) to request construction of a secured packet that contains the provided UICC configuration information (e.g. Routing Indicator or Steering of Roaming information).

The following procedures using the Provide service operation are supported:

- Secured Packet Retrieval

5.2.2.2.2 Secured Packet Retrieval

Figure 5.2.2.2.2-1 shows a scenario where the NF consumer (e.g. UDM or SOR-AF) sends a request to the SP-AF to provide a secured packet.

The request contains the UE's identity (/{supi}) and the UICC configuration parameter.

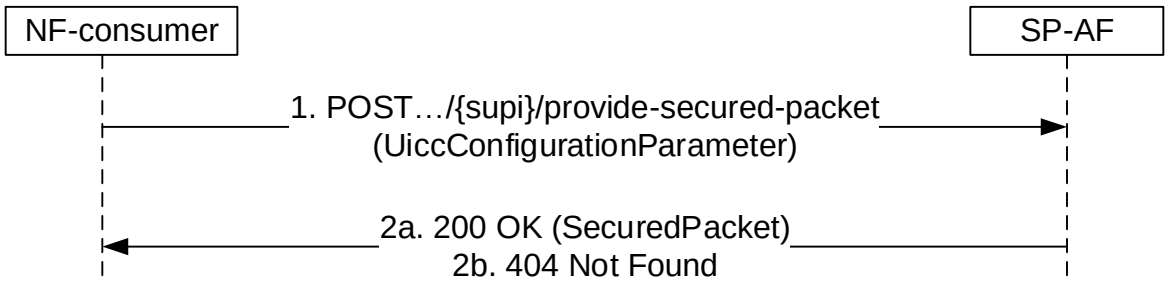

Figure 5.2.2.2.2-1: NF consumer requests the SP-AF to provide a secured packet

1. The NF consumer sends a POST request (custom method: provide-secured-packet) to the resource representing the SUPI.

2a. On success, the SP-AF responds with "200 OK", containing the requested SecuredPacket.

2b. If the resource does not exist (the supi is unknown in the SP-AF), the SP-AF returns the HTTP status code "404 Not Found", and additional error information should be included in the response body (in "ProblemDetails" element).

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

6 API Definitions

6.1 Nspaf_SecuredPacket Service API

6.1.1 Introduction

The Nspaf_SecuredPacket service shall use the Nspaf_SecuredPacket API.

The request URI used in HTTP request from the NF service consumer towards the NF service producer shall have the 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 "nspaf-secured-packet".
- 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 [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 Nspaf_SecuredPacket API is contained in Annex A.

6.1.2.2 HTTP standard headers

6.1.2.2.1 General

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

6.1.2.2.2 Content type

JSON, IETF RFC 8259 [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 7807 [13].

6.1.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be applicable.

6.1.3 Resources

6.1.3.1 Overview

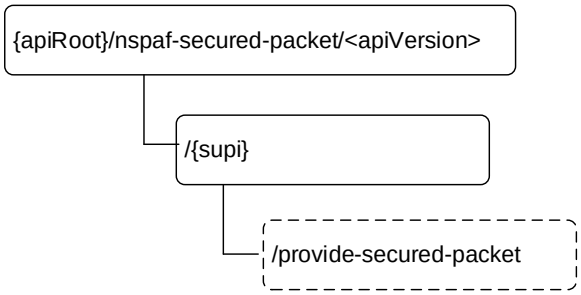

Figure 6.1.3.1-1: Resource URI structure of the nspaf-secured-packet API

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
SecuredPacket (Custom operation)	/{supi}/provide-secured-packet	Provide-secured-packet (POST)	The SP-AF generates a secured packet containing the presented UICC configuration parameter

6.1.3.2 Resource: SecuredPacket

6.1.3.2.1 Description

This resource represents the information that is needed to construct secured packets for the SUPI.

6.1.3.2.2 Resource Definition

Resource URI: **{apiRoot}/nspaf-secured-packet/v1/{supi}/provide-secured-packet**

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	Definition
apiRoot	See clause 6.1.1
supi	Represents the Subscription Permanent Identifier (see 3GPP TS 23.501 [2] clause 5.9.2) pattern: "^(imsi-[0-9]{5,15}|nai-.+|.+)$"

6.1.3.2.3 Resource Standard Methods

No Standard Methods are supported for this 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

Custom operaration URI	Mapped HTTP method	Description
/provide-secured-packet	POST	The SP-AF generates a secured packet for the SUPI that contains the presented UICC configuration parameter.

6.1.3.2.4.2 Operation: provide-secured-packet

6.1.3.2.4.2.1 Description

This custom operation is used by the NF service consumer (e.g. UDM) to request a secured packet for the SUPI containing the presented UICC configuration parameter. The returned secured packet shall be constructed as an SMS-Deliver as specified in 3GPP TS 23.040 [18] and protected as specified in 3GPP TS 31.115 [16].

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
UiccConfiguration Parameter	M	1	Contains the parameter that is to be updated in the UICC

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
SecuredPacket	M	1	200 OK	Upon success, a response body containing the generated secured packet shall be returned.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to convey the following application error: - USER_NOT_FOUND
NOTE: 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.				

6.1.4 Custom Operations without associated resources

In this release of this specification, no custom operations without associated resources are defined for the Nspaf_SecuredPacket Service.

6.1.5 Notifications

In this release of this specification, no notifications are defined for the Nspaf_SecuredPacket 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 Nspaf service based interface protocol.

Table 6.1.6.1-1: Nspaf specific Data Types

Data type	Clause defined	Description	Applicability
UiccConfigurationParameter	6.1.6.2.2	UICC Configuration Parameters	
RoutingId	6.1.6.3.2	Routing ID	
ExtendedSteeringContainer	6.1.6.2.3	Extended Steering Container (including the contents of Steering Container and SOR-CMCI)	

Table 6.1.6.1-2 specifies data types re-used by the Nspaf 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 N_{spaf} service based interface.

Table 6.1.6.1-2: Nspaf re-used Data Types

Data type	Reference	Comments	Applicability
SecuredPacket	3GPP TS 29.503 [14]	Secured Packet	
ProblemDetails	3GPP TS 29.571 [15]		
SteeringInfo	3GPP TS 29.509 [17]	Steering Information	
SorCmci	3GPP TS 29.503 [14]	Contains SOR-CMCI as defined in 3GPP TS 24.501 [19]	

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: UiccConfigurationParameter

Table 6.1.6.2.2-1: Definition of type UiccConfigurationParameter

Attribute name	Data type	P	Cardinality	Description	Applicability
routingId	RoutingId	C	0..1	The Routing Id that needs to be updated in the USIM.	
steeringContainer	array(SteeringInfo)	C	1..N	List of PLMN/AccessTechnologies combinations that need to be updated in the USIM.	
extendedSteeringContainer	ExtendedSteeringContainer	C	0..1	Extended Steering Container that includes list of PLMN/AccessTechnologies combinations with the SOR-CMCI that need to be updated in the USIM	
Note: Exactly one attribute shall be present					

6.1.6.2.3 Type: ExtendedSteeringContainer

Table 6.1.6.2.3-1: Definition of type ExtendedSteeringContainer

Attribute name	Data type	P	Cardinality	Description	Applicability
steeringContainer	array(SteeringInfo)	C	1..N	List of PLMN/AccessTechnologies combinations that need to be updated in the USIM.	
sorCmci	SorCmci	C	0..1	When present, provides the SOR-CMCI values as defined in 3GPP TS 24.501 [19]	
storeSorCmciInMe	boolean	C	0..1	When present, indicates "Store the SOR-CMCI in the ME", i.e. whether to instruct UE to store SOR-CMCI in the ME as defined in 3GPP TS 23.122 [14] and 3GPP TS 24.501 [27]. - True: Indicates to store the SOR-CMCI in the ME - False or absent: Indicates storing the SOR-CMCI in the ME is not required	
NOTE: At least one attribute shall be present. If no additional attributes than steeringContainer is included, then use of steeringContainer can be considered instead of using ExtendedSteeringContainer.					

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
RoutingId	string	Pattern: "^[0-9]{1,4}$"	

6.1.7 Error Handling

6.1.7.1 General

For the Nspaf_SecuredPacket 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 Nspaf_SecuredPacket API.

6.1.7.2 Protocol Errors

No specific procedures for the Nspaf_SecuredPacket service are specified.

6.1.7.3 Application Errors

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

Table 6.1.7.3-1: Application errors

Application Error	HTTP status code	Description
USER_NOT_FOUND	404 Not Found	The user does not exist

6.1.8 Feature negotiation

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

Table 6.1.8-1: Supported Features

Feature number	Feature Name	Description

6.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Nspaf_SecuredPacket 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 Nspaf_SecuredPacket 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 Nspaf_SecuredPacket service.

The Nspaf_SecuredPacket API defines a single scope "nspaf-secured-packet" for the entire service, and it does not define any additional scopes at resource or operation level.

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 Nspaf_SecuredPacket API

```
openapi: 3.0.0
info:
  title: 'Nspaf_SecuredPacket'
  version: '1.1.0-alpha.3'
  description: |
    Nspaf Secured Packet Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: 3GPP TS 29.544, SP-AF Services, version V17.2.0
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.544/
servers:
  - url: '{apiRoot}/nspaf-secured-packet/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501
security:
  - {}
  - oAuth2ClientCredentials:
    - nspaf-secured-packet
paths:
  /{supi}/provide-secured-packet:
    post:
      summary: request generation of a secured packet
      operationId: ProvideSecuredPacket
      tags:
        - SecuredPacket Generation (Custom Operation)
      parameters:
        - name: supi
          in: path
          description: SUPI of the user
          required: true
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/UiccConfigurationParameter'
      responses:
        '200':
          description: Success
          content:
            application/json:
              schema:
                $ref: 'TS29503_Nudm_SDM.yaml#/components/schemas/SecuredPacket'
```

```
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '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:
            nspaf-secured-packet: Access to the nspaf-secured-packet API
  schemas:

# COMPLEX TYPES:

    UiccConfigurationParameter:
      description: Represents UICC Configuration Parameters.
      type: object
      oneOf:
        - required: [routingId ]
        - required: [steeringContainer ]
        - required: [extendedSteeringContainer ]
      properties:
        routingId:
          $ref: '#/components/schemas/RoutingId'
        steeringContainer:
          type: array
          items:
            $ref: 'TS29509_Nausf_SoRProtection.yaml#/components/schemas/SteeringInfo'
          minItems: 1
        extendedSteeringContainer:
          $ref: '#/components/schemas/ExtendedSteeringContainer'

    ExtendedSteeringContainer:
      description: Represents Extended Steering Containers.
      type: object
      properties:
        steeringContainer:
          type: array
          items:
            $ref: 'TS29509_Nausf_SoRProtection.yaml#/components/schemas/SteeringInfo'
          minItems: 1
        sorCmci:
          $ref: 'TS29503_Nudm_SDM.yaml#/components/schemas/SorCmci'
        storeSorCmciInMe:
          type: boolean

# SIMPLE TYPES:

    RoutingId:
      description: Represents a routing indicator.
      type: string
      pattern: '^[0-9]{1,4}$'

# ENUMS:
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-10	CT4#94	C4-194013				Initial Draft.	0.1.0
2019-10	CT4#94	C4-194367				Notaf Overview	0.2.0
2019-10	CT4#94	C4-194488				Notaf_SecuredPacket-Provide service operation	0.2.0
2019-10	CT4#94	C4-194492				Resources	0.2.0
2019-10	CT4#94	C4-194516				Data Model	0.2.0
2019-10	CT4#94	C4-194490				OpenAPI Specification	0.2.0
2019-11	CT4#95	C4-195481				Clean Up	0.3.0
2019-12	CT#86	CP-193071				TS presented for information	1.0.0
2019-12	CT#86	CP-193285				A title updated	1.0.1
2020-03	CT4#96e	C4-201119				Pseudo-CR on SOR	1.1.0
2020-03	CT4#96e	C4-201123				Pseudo-CR on Clean Up	1.1.0
2020-03	CT4#96e	C4-201217				Pseudo-CR on the necessary modifications to change OTAF NF name to SP-AF	1.1.0
2020-03	CT4#96e	C4-201314				Pseudo-CR on API descriptions table in clause 5.1	1.1.0
2020-03	CT#87e	CP-200062				TS presented for approval	2.0.0
2020-03	CT#87e					Approved at CT#87e	16.0.0
2020-07	CT#88e	CP-201040	0001	1	C	Clarification on Secured Packet format provided by SP-AF	16.1.0
2020-07	CT#88e	CP-201040	0002		F	Storage of YAML files in ETSI Forge	16.1.0
2020-07	CT#88e	CP-201040	0003	1	F	Miscellaneous Corrections	16.1.0
2020-07	CT#88e	CP-201073	0005		F	3GPP TS 29.544 API Version and External doc Update	16.1.0
2020-09	CT#89e	CP-202110	0006	1	F	Miscelaneous corrections	16.2.0
2020-09	CT#89e	CP-202096	0007		F	API version and External doc update	16.2.0
2020-12	CT#90e	CP-203048	0008		F	Storage of yaml files	16.3.0
2021-06	CT#92e	CP-211051	0011		F	OpenAPI Reference	17.0.0
2021-06	CT#92e	CP-211028	0012	1	F	Adding some missing description fields to data type definitions in OpenAPI specification files of the Nspaf_SecuredPacket API	17.0.0
2021-06	CT#92e	CP-211050	0013		F	29.544 Rel-17 API version and External doc update	17.0.0
2021-12	CT#94e	CP-213197	0014	2	B	SOR-CMCI support	17.1.0
2021-12	CT#94e	CP-213121	0015		F	29.544 Rel-17 API version and External doc update	17.1.0
2022-03	CT#95e	CP-220041	0016		B	Addition of SOR-CMCI related attribute as input to SP-AF	17.2.0
2022-03	CT#95e	CP-220066	0017		F	API version and External doc update	17.2.0

History

Document history		
V17.2.0	May 2022	Publication