

ETSI TS 129 256 V17.0.0 (2022-05)



**5G;  
Uncrewed Aerial Systems Network Function (UAS-NF);  
Aerial Management Services;  
Stage 3  
(3GPP TS 29.256 version 17.0.0 Release 17)**



---

**Reference**

DTS/TSGC-0429256vh00

---

**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

---

**Important notice**

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our  
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.  
All rights reserved.

---

# 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

|   |    |
|---|----|
| Intellectual Property Rights .....                      | 2  |
| Legal Notice .....                                      | 2  |
| Modal verbs terminology.....                            | 2  |
| Foreword.....   | 5  |
| 1 Scope .....   | 7  |
| 2 References .....                                      | 7  |
| 3 Definitions of terms, symbols and abbreviations ..... | 8  |
| 3.1 Terms.....  | 8  |
| 3.2 Symbols.....  | 8  |
| 3.3 Abbreviations .....                                 | 8  |
| 4 Overview .....  | 8  |
| 4.1 Introduction .....                                  | 8  |
| 5 Services offered by the NEF (UAS-NF) .....            | 9  |
| 5.1 Introduction .....                                  | 9  |
| 5.2 Nnef_Authentication Service .....                   | 9  |
| 5.2.1 Service Description.....                          | 9  |
| 5.2.2 Service Operations.....                           | 9  |
| 5.2.2.1 Introduction.....                               | 9  |
| 5.2.2.2 AuthenticateAuthorize Service Operation.....    | 10 |
| 5.2.2.2.1 General .....                                 | 10 |
| 5.2.2.3 AuthNotify Service Operation .....              | 11 |
| 5.2.2.3.1 General .....                                 | 11 |
| 6 API Definitions .....                                 | 12 |
| 6.1 Nnef_Authentication Service API.....                | 12 |
| 6.1.1 Introduction.....                                 | 12 |
| 6.1.2 Usage of HTTP.....                                | 13 |
| 6.1.2.1 General .....                                   | 13 |
| 6.1.2.2 HTTP standard headers .....                     | 13 |
| 6.1.2.2.1 General .....                                 | 13 |
| 6.1.2.2.2 Content type .....                            | 13 |
| 6.1.2.3 HTTP custom headers .....                       | 13 |
| 6.1.3 Resources.....                                    | 13 |
| 6.1.3.1 Overview.....                                   | 13 |
| 6.1.3.2 Resource: uav-authentications.....              | 14 |
| 6.1.3.2.1 Description .....                             | 14 |
| 6.1.3.2.2 Resource Definition .....                     | 14 |
| 6.1.3.2.3 Resource Standard Methods .....               | 14 |
| 6.1.3.2.4 Resource Custom Operations .....              | 15 |
| 6.1.5 Notifications .....                               | 16 |
| 6.1.5.1 General .....                                   | 16 |
| 6.1.5.2 Authentication Notification.....                | 16 |
| 6.1.5.2.1 Description .....                             | 16 |
| 6.1.5.2.2 Target URI.....                               | 16 |
| 6.1.5.2.3 Standard Methods.....                         | 16 |
| 6.1.6 Data Model .....                                  | 17 |
| 6.1.6.1 General .....                                   | 17 |
| 6.1.6.2 Structured data types .....                     | 18 |
| 6.1.6.2.1 Introduction .....                            | 18 |
| 6.1.6.2.2 Type: UVAAuthInfo .....                       | 19 |
| 6.1.6.2.3 Type: AuthNotification .....                  | 20 |
| 6.1.6.2.4 Type: UVAAuthResponse.....                    | 20 |
| 6.1.6.2.5 Type: UVAAuthFailure.....                     | 21 |

|                               |  |           |
|-------------------------------|--|-----------|
| 6.1.6.3                       | Simple data types and enumerations ..... | 21        |
| 6.1.6.3.1                     | Introduction .....                       | 21        |
| 6.1.6.3.2                     | Simple data types.....                   | 21        |
| 6.1.6.3.3                     | Enumeration: AuthResult .....            | 21        |
| 6.1.6.3.4                     | Enumeration: NotifType.....              | 21        |
| 6.1.7                         | Error Handling .....                     | 22        |
| 6.1.7.1                       | General .....                            | 22        |
| 6.1.7.2                       | Protocol Errors .....                    | 22        |
| 6.1.7.3                       | Application Errors.....                  | 22        |
| 6.1.8                         | Feature negotiation .....                | 22        |
| 6.1.9                         | Security .....                           | 22        |
| <b>Annex A (normative):</b>   | <b>OpenAPI specification.....</b>        | <b>24</b> |
| A.1                           | General .....                            | 24        |
| A.2                           | Nnef_Authentication API.....             | 24        |
| <b>Annex B (informative):</b> | <b>Change history .....</b>              | <b>28</b> |
| History .....                 |  | 29        |

---

# 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 UAS-NF functionality of the Nnef Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the NEF (UAS-NF).

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].

The Uncrewed Aerial System Network Function (UAS-NF) provides the UAS-specific NEF services to NF service consumers (e.g. AMF, SMF). The UAS-NF is functionality within the NEF.

---

# 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] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".
- [7] 3GPP TR 21.900: "Technical Specification Group working methods".
- [8] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".
- [9] OpenAPI Initiative, "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.
- [10] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".
- [11] IETF RFC 7807: "Problem Details for HTTP APIs".
- [12] 3GPP TS 33.501: "Security architecture and procedures for 5G system".
- [13] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".
- [14] 3GPP TS 29.510: "Network Function Repository Services; Stage 3".
- [15] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; 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].

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.256 [6] shall apply.

### 3.2 Symbols

For the purposes of the present document, the following symbols apply:

### 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].

|       |   |
|-------|---|
| AA    | Authorization/Authentication              |
| BRID  | Broadcast Remote Identification           |
| BVLOS | Beyond Visual Line of Sight               |
| C2    | Command and Control                       |
| NRID  | Networked Remote Identification           |
| PEI   | Permanent Equipment Identifier            |
| RID   | Remote Identification                     |
| TPAE  | Third Party Authorized Entity             |
| UAS   | Uncrewed Aerial System                    |
| UAV   | Uncrewed Aerial Vehicle                   |
| USS   | UAS Service Supplier                      |
| UTM   | Uncrewed Aerial System Traffic Management |
| UUAA  | USS UAV AA                                |
| UUID  | Universal Unique Identifier               |

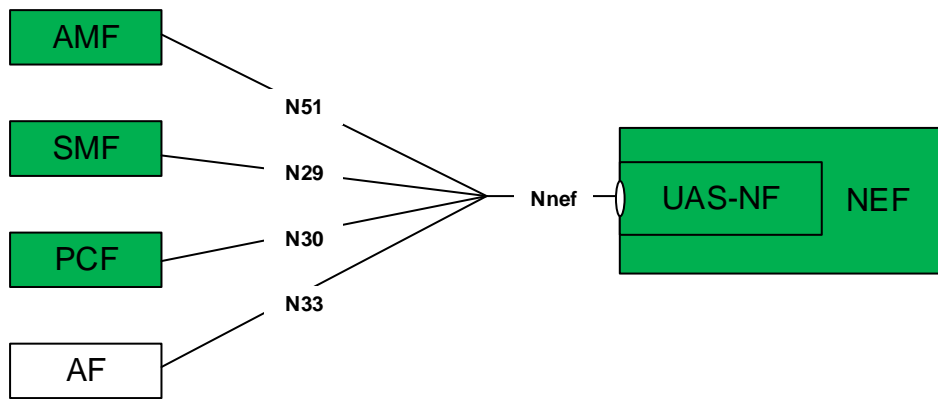
---

## 4 Overview

### 4.1 Introduction

Within the 5GC, the NEF (UAS-NF) offers services to the AMF, SMF, and PCF via the Nnef service based interface, and the NEF (UAS-NF) offers services to the SMF+PGW-C via the Nnef service based interface for UUAA-SM and C2 procedure supported in EPS (see 3GPP TS 23.256 [6]).

Figure 4.1-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the NEF (UAS-NF) and the scope of the present specification.



**Figure 4.1-1: Reference model – NEF (UAS-NF)**

The functionalities supported by the NEF (UAS-NF) are listed in clause 4.3.2 of 3GPP TS 23.256 [6].

## 5 Services offered by the NEF (UAS-NF)

### 5.1 Introduction

The table 5.1-1 shows the NEF (UAS-NF) Services and Service Operations:

**Table 5.1-1 List of NEF (UAS-NF) Services**

| Service Name        | Service Operations    | Operation Semantics | Example Consumer(s) | Mapped Service Operation                  |
|---------------------|-----------------------|---------------------|---------------------|---|
| Nnef_Authentication | AuthenticateAuthorize | Request/Response    | AMF, SMF, SMF+PGW-C | Nnef_Authentication_AuthenticateAuthorize |
|                     | Notification          | Subscribe/Notify    | AMF, SMF, SMF+PGW-C | Nnef_Authentication_Notification          |

### 5.2 Nnef\_Authentication Service

#### 5.2.1 Service Description

The service allows communication of authentication and authorization messages between AMF/SMF and external AF (USS). An NF as service consumer (e.g. AMF, SMF, SMF+PGW-C) can authenticate or subscribe to receive notifications from NEF (UAS-NF) related to reauthentication, update authorization data or revoke authorization of the UAV.

#### 5.2.2 Service Operations

##### 5.2.2.1 Introduction

The Nnef\_Authentication service supports following service operations:

- AuthenticateAuthorize
- Notification

## 5.2.2.2 AuthenticateAuthorize Service Operation

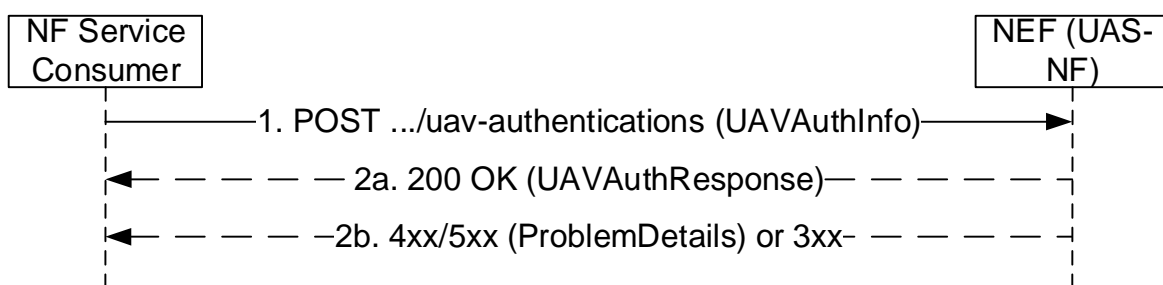
### 5.2.2.2.1 General

The AuthenticateAuthorize service operation is used during the following procedure:

- UAAA-MM and UAAA-SM procedures (see 3GPP TS 23.256 [6], clause 5.2.2 and clause 5.2.3, respectively)
- C2 authorization (see 3GPP TS 23.256 [6], clause 5.2.5)

The AuthenticateAuthorize service operation is invoked by an NF Service Consumer (e.g. an AMF, SMF, SMF+PGW-C) towards the NEF (UAS-NF), when UAAA-MM is done at 5GS registration, UAAA-SM is done at PDU session establishment, or for Authorization for C2 in 5GS or EPS.

The NF Service Consumer (e.g. the AMF or the SMF or the SMF+PGW-C) shall send the authentication message to NEF (UAS-NF) by sending the HTTP POST request towards the UAV Authentications resource as shown in Figure 5.2.2.2.1-1.



**Figure 5.2.2.2.1-1: AuthenticateAuthorize Service Operation**

1. The NF Service Consumer shall send a POST request to the resource representing the UAV Authentications resource of the NEF (UAS-NF) with a "UAVAuthInfo" object in the request body, including:

- gpsi IE set to GPSI (in the format of External Identifier) of the UAV;
- serviceLevelId IE set to Service Level Device Identity;
- authMsg IE contains the service-level AA message;
- authNotificationURI IE provides the notification URI to receive notifications related to authentication;
- authServerAddress IE provides the Authorization Server Address, e.g. Authorization Server FQDN. This IE is not included for intermediate round-trip authentication messages;
- nfType IE carries the NF type of the NF service consumer (e.g. AMF or SMF or SMF+PGW-C); and
- userLocInfo IE provides the user location information (e.g. cell Id).

If the NF Service Consumer is SMF or SMF+PGW-C, the "UAVAuthInfo" also may include:

- ipAddr IE carries the IP Address associated with the PDU session;
- pei IE carries the PEI;

If the NF Service Consumer is SMF or SMF+PGW-C, for UAAA-MM and UAAA-SM procedures the "UAVAuthInfo" also may include:

- dnn IE carries the DNN which can be used by NEF (UAS-NF) later on to create a subscription at SMF; and
- sNssai IE carries the S-NSSAI which can be used by NEF (UAS-NF) later on to create a subscription at SMF.

2a. On success, the NEF (UAS-NF) shall store the result and return "200 OK".

For intermediate round-trip messages, the payload body (i.e. UAVAuthResponse) shall contain the GPSI of the UAV and Service Level Device Identity. The payload body optionally includes "authMsg".

For the final NEF (UAS-NF) to NF service consumer message, the payload body (i.e. UAVAuthResponse) shall contain the GPSI of the UAV, authSessCorrId attribute and "authResult" attribute. If the UAV is authenticated successfully, the NEF (UAS-NF) shall set the "authResult" attribute to "AUTH\_SUCCESS". The payload body optionally contains the authorized Service Level Device Identity and "authMsg" payload delivering configuration information to the UAV. The AMF forwards the message transparently to UE over NAS MM.

2b. On failure or redirection, one of the HTTP status codes listed in Table 6.1.7.3-1 shall be returned. For a 4xx/5xx response, the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application errors listed in Table 6.1.7.3-1.

If the NEF (UAS-NF) cannot successfully fulfil the received HTTP POST request due to an internal error or an error in the HTTP POST request, the NEF (UAS-NF) shall send the HTTP error response as specified in clause 6.1.7.

If the UAV authentication is failed, the NEF (UAS-NF) shall reject the request with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "AUTHENTICATION\_FAILURE". NEF (UAS-NF) shall also include an indication of uasResourceRelease received from the USS in case of reauthentication failure.

In above steps, while there is no expected response from the USS in the case of time out, the NEF(UAS-NF) shall return HTTP status code "504 Gateway Timeout", with the message body containing a ProblemDetails structure with the "cause" attribute set to "PEER\_NOT\_RESPONDING".

### 5.2.2.3 AuthNotify Service Operation

#### 5.2.2.3.1 General

The AuthNotify service operation is used during the following procedure:

- USS Initiated reauthentication (see 3GPP TS 23.256 [6], clause 5.2.4)
- USS Initiated update authorization data or revoke authorization of the UAV

The AuthNotify service operation is invoked by the NEF (UAS-NF) to inform a NF Service Consumer (e.g. AMF, SMF, SMF+PGW-C), when USS triggers reauthentication, update authorization data or revoke authorization of the UAV. NEF (UAS-NF) shall determine the NF service consumer based on the previously stored UUA context during the successful UUA procedure as defined in clause 5.2.2.2.

The NEF (UAS-NF) shall send the AuthNotify request by sending the HTTP POST method towards the Notification URI as shown in Figure 5.2.2.3.1-1.

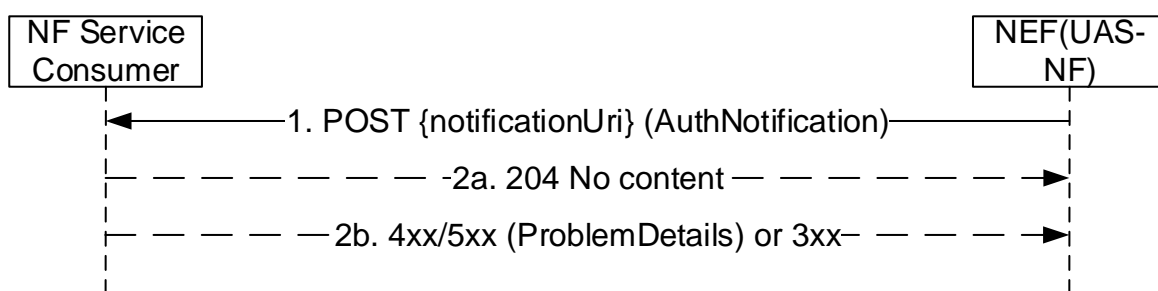


Figure 5.2.2.3.1-1: AuthNotify Service Operation

1. The NEF (UAS-NF) shall send a POST request towards the Notification URI received in the Authenticate service operation request (See clause 5.2.2.2.1). The NEF (UAS-NF) shall be able to determine the NF type of the NF service consumer by nfType IE received in the Authenticate service operation request. The request body shall contain a "AuthNotification" object containing the reauthentication information or update authorization information or revoke authorization indication.

When the procedure is used for reauthentication or reauthorization/update authorization information, the AuthNotification object includes:

- the gpsi IE set to the GPSI (in the format of External Identifier) of the given UAV required to be reauthenticated;

- serviceLevelId IE set to the Service Level Device Identity of the UAV;
- authMsg IE contains the service-level AA message;
- authSessCorrId IE set to the authentication session correlation id;
- notifType IE set to REAUTH used for reauthentication and/or notifType IE set to UPDATEAUTH used for update authorization data.

When the procedure is used for authorization revocation, the AuthNotification object includes:

- the gpsi IE set to the GPSI (in the format of External Identifier) of the given UAV;
- serviceLevelId IE set to the Service Level Device Identity of the UAV;
- authSessCorrId IE set to the authentication session correlation id;
- revokeCause IE set to cause of revocation received from USS; and
- notifType IE set to REVOKE.

2a. On success, "204 No content" shall be returned without response body. If the NF Service consumer remove the successful UUAA result during UUAA Revocation procedure, the NEF (UAS-NF) shall remove the UUAA context (see clause 5.2.7 of 3GPP TS 23.256 [6]).

2b. On failure or redirection, one of the HTTP status code listed in Table 6.1.5.2.3.1-3 shall be returned. For a 4xx/5xx response, the response body should contain a "ProblemDetails" object.

If the NF service consumer cannot successfully fulfil the received HTTP POST request due to an internal error or an error in the HTTP POST request, the NF service consumer shall send an HTTP error response as specified in clause 6.1.7.

## 6 API Definitions

### 6.1 Nnef\_Authentication Service API

#### 6.1.1 Introduction

The Nnef\_Authentication shall use the Nnef\_Authentication API.

The API URI of the Nnef\_Authentication 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 "nnef-authentication".
- 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 [4].

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

The OpenAPI [9] specification of HTTP messages and content bodies for the Nnef\_Authentication 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 [10], 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 [11].

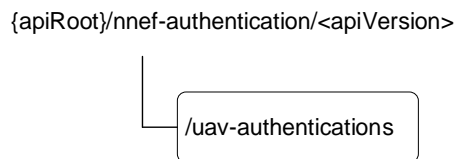
### 6.1.2.3 HTTP custom headers

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

The structure of the Resource URIs of the Nnef\_Authentication API is shown in Figure 6.1.3.1-1



**Figure 6.1.3.1-1: Resource URI structure of the Nnef\_Authentication 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          |
|---------------------|----------------------|---------------------------------|----------------------|
| uav-authentications | /uav-authentications | POST                            | A UAV authentication |

### 6.1.3.2 Resource: uav-authentications

The resource represents UAV Authentications to be done with the NEF (UAS-NF).

#### 6.1.3.2.1 Description

#### 6.1.3.2.2 Resource Definition

Resource URI: {apiRoot}/nnef-authentication/<apiVersion>/uav-authentications

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 |
| apiVersion | string    | See clause 6.1.1 |

#### 6.1.3.2.3 Resource Standard Methods

##### 6.1.3.2.3.1 POST

This method performs UAV authentication.

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

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

| Name | Data type | P | Cardinality | Description | Applicability |
|------|-----------|---|-------------|-------------|---------------|
| n/a  |           |   |             |             |               |

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

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

| Data type   | P | Cardinality | Description   |
|-------------|---|-------------|---|
| UAVAuthInfo | M | 1           | Represents the data to be used for UAV authentication |

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

| Data type  | P | Cardinality | Response codes         | Description   |
|--|---|-------------|------------------------|---|
| UAVAuthResponse  | M | 1           | 200 OK                 | Successful request of UAV authentication and authorization.   |
| 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 NEF (UAS-NF) or NEF (UAS-NF) (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 NEF (UAS-NF) or NEF (UAS-NF) (service) set. (NOTE 2) |
| UAVAuthFailure   | O | 0..1        | 403 Forbidden          | This represents that the UAV authentication is failed, the "cause" attribute of the ProblemDetails data structure set to:<br>- AUTHENTICATION_FAILURE<br>See table 6.1.7.3-1 for the description of these errors.   |
| ProblemDetails   | O | 0..1        | 504 Gateway Timeout    | The "cause" attribute may be used to indicate the following application error:<br>- PEER_NOT_RESPONDING<br><br>See table 6.1.7.3-1 for the description of the error.  |
| NOTE 1: The mandatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. |   |             |                        |   |
| NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].                               |   |             |                        |   |

**Table 6.1.3.2.3.1-4: 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 NEF (UAS-NF) or NEF (UAS-NF) (service) set.<br>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 NF (service) instance ID towards which the request is redirected   |

**Table 6.1.3.2.3.1-5: 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 NEF (UAS-NF) or UAS-NF/NEF (service) set.<br>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 NF (service) instance ID towards which the request is redirected   |

#### 6.1.3.2.4 Resource Custom Operations

None



## 6.1.5 Notifications

### 6.1.5.1 General

This clause specifies the notifications provided by the Nnef\_Authentication service.

Notifications shall comply to clause 6.2 of 3GPP TS 29.500 [4] and clause 4.6.2.3 of 3GPP TS 29.501 [5].

### 6.1.5.2 Authentication Notification

#### 6.1.5.2.1 Description

The NF Service Consumer (e.g. the AMF or SMF or SMF+PGW-C) provides the Notification URI for getting notified about reauthentication requested by the USS. The NEF (UAS-NF) shall notify the NF Service Consumer when reauthentication is requested by the USS.

#### 6.1.5.2.2 Target URI

The Notification URI "{notifUri}" shall be used with the callback URI variables defined in table 6.1.5.2.2-1.

**Table 6.1.5.2.2-1: Callback URI variables**

| Name            | Definition                                    |
|-----------------|---|
| notificationUri | String formatted as URI with the Callback Uri |

#### 6.1.5.2.3 Standard Methods

##### 6.1.5.2.3.1 POST

This method shall support the request data structures specified in table 6.1.5.2.3.1-1 and the response data structures and response codes specified in table 6.1.5.2.3.1-2.

**Table 6.1.5.2.3.1-1: Data structures supported by the POST Request Body**

| Data type        | P | Cardinality | Description                                |
|------------------|---|-------------|--|
| AuthNotification | M | 1           | Contains the reauthentication information. |

**Table 6.1.5.2.3.1-2: Data structures supported by the POST Response Body**

| Data type   | P | Cardinality | Response codes         | Description  |
|---|---|-------------|------------------------|--|
| n/a   |   |             | 204 No Content         | Successful notification of reauthentication  |
| RedirectResponse  | O | 0..1        | 307 Temporary Redirect | Temporary redirection. The response shall include a Location header field containing a different URI. The URI shall be an alternative URI of the resource located on an alternative service instance within the same NF consumer where the notification should be sent. If an SCP redirects the message to another SCP then the location header field shall contain the same URI or a different URI pointing to the endpoint of the NF service consumer to which the notification should be sent. (NOTE 2) |
| RedirectResponse  | O | 0..1        | 308 Permanent Redirect | Permanent redirection. The response shall include a Location header field containing a different URI. The URI shall be an alternative URI of the resource located on an alternative service instance within the same NF consumer where the notification should be sent. If an SCP redirects the message to another SCP then the location header field shall contain the same URI or a different URI pointing to the endpoint of the NF service consumer to which the notification should be sent. (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, with response body containing an object of ProblemDetails data type (see clause 5.2.7 of 3GPP TS 29.500 [4]). |   |             |                        |  |
| NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].  |   |             |                        |  |

**Table 6.1.5.2.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name                  | Data type | P | Cardinality | Description  |
|-----------------------|-----------|---|-------------|--|
| Location              | string    | M | 1           | A URI pointing to the endpoint of NF service consumer to which the notification should be sent |
| 3gpp-Sbi-Target-Nf-Id | string    | O | 0..1        | Identifier of the target NF (service) instance ID towards which the notification is redirected |

**Table 6.1.5.2.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name                  | Data type | P | Cardinality | Description  |
|-----------------------|-----------|---|-------------|--|
| Location              | string    | M | 1           | A URI pointing to the endpoint of NF service consumer to which the notification should be sent |
| 3gpp-Sbi-Target-Nf-Id | string    | O | 0..1        | Identifier of the target NF (service) instance ID towards which the notification is redirected |

## 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 Nnef\_Authentication service based interface protocol.

**Table 6.1.6.1-1: Nnef\_Authentication specific Data Types**

| Data type        | Clause defined | Description                                  | Applicability |
|------------------|----------------|--|---------------|
| UAVAuthInfo      | 6.1.6.2.2      | Information within Authenticate Request      |               |
| AuthNotification | 6.1.6.2.3      | Information within notification              |               |
| UAVAuthResponse  | 6.1.6.2.4      | Information within Authenticate Response     |               |
| UAVAuthFailure   | 6.1.6.2.5      | Information within Authenticate Response     |               |
| AuthResult       | 6.1.6.3.3      | Enumeration indicating authentication result |               |
| NotifType        | 6.1.6.3.4      | Enumeration Notification type                |               |

Table 6.1.6.1-2 specifies data types re-used by the Nnef\_Authentication 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 Nnef\_Authentication service based interface.

**Table 6.1.6.1-2: Nnef\_Authentication re-used Data Types**

| Data type        | Reference           | Comments                                 | Applicability |
|------------------|---------------------|--|---------------|
| IpAddr           | 3GPP TS 29.571 [15] | IP address                               |               |
| Pei              | 3GPP TS 29.571 [15] | Permanent Equipment Identifier           |               |
| Uri              | 3GPP TS 29.571 [15] | Uri                                      |               |
| Gpsi             | 3GPP TS 29.571 [15] | GPSI                                     |               |
| ExtSnssai        | 3GPP TS 29.571 [15] | Ext Snssai                               |               |
| Dnn              | 3GPP TS 29.571 [15] | DNN information                          |               |
| UserLocation     | 3GPP TS 29.571 [15] | User location                            |               |
| RedirectResponse | 3GPP TS 29.571 [15] | Contains redirection related information |               |
| NFType           | 3GPP TS 29.510 [14] | NF Type                                  |               |
| RefToBinaryData  | 3GPP TS 29.571 [15] | authMsg data                             |               |

## 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: UAVAAuthInfo

Table 6.1.6.2.2-1: Definition of type UAVAAuthInfo

| Attribute name      | Data type       | P | Cardinality | Description   | Applicability |
|---------------------|-----------------|---|-------------|---|---------------|
| gpsi                | Gpsi            | M | 1           | GPSI of the UAV   |               |
| serviceLevelId      | string          | M | 1           | Service Level Device Identity of the UAV  |               |
| ipAddr              | IpAddr          | O | 0..1        | This IE may be present if the NF Service Consumer is the SMF or SMF+PGW-C.<br><br>When present, this IE indicates the IP address associated with the PDU session. |               |
| authMsg             | RefToBinaryData | O | 0..1        | Contains the service-level AA message.  |               |
| pei                 | Pei             | O | 0..1        | This IE may be present if the NF Service Consumer is the SMF or SMF+PGW-C.<br><br>When present, PEI associated with the UAV.                                      |               |
| authServerAddress   | string          | O | 0..1        | Provides the Authorization Server Address, e.g. Authorization Server FQDN.  |               |
| authNotificationURI | Uri             | C | 0..1        | This IE shall be present in the initial authentication message.<br><br>It carries the notification URI to receive authentication related notifications            |               |
| dnn                 | Dnn             | C | 0..1        | This IE shall be present if the NF Service Consumer is the SMF or SMF+PGW-C.<br><br>When present, this IE indicates DNN associated with the PDU session.          |               |
| sNssai              | ExtSnsai        | C | 0..1        | This IE shall be present if the NF Service Consumer is the SMF.<br><br>When present, this IE indicates the S-NSSAI associated with the PDU session.               |               |
| ueLocInfo           | UserLocation    | O | 0..1        | This IE shall contain the UE location information if it is available.   |               |
| nfType              | NFType          | M | 0..1        | NFType of the NF service consumer.<br>Possible NFType values supported in this release of the specification are<br>- AMF<br>- SMF                                 |               |

## 6.1.6.2.3 Type: AuthNotification

Table 6.1.6.2.3-1: Definition of type AuthNotification

| Attribute name | Data type       | P | Cardinality | Description   | Applicability |
|----------------|-----------------|---|-------------|---|---------------|
| gpsi           | Gpsi            | M | 1           | GPSI of the UAV   |               |
| serviceLevelId | string          | M | 1           | Service Level Device Identity of the UAV  |               |
| authMsg        | RefToBinaryData | C | 0..1        | Contains the service-level AA message.<br>This IE may be present if the notifType is set to "UPDATEAUTH".                           |               |
| authSessCorrId | string          | M | 0..1        | When present, this IE shall contain the authentication Session Correlation Id.  |               |
| notifType      | NotifType       | M | 1           | This IE shall contain the notification type.  |               |
| revokeCause    | string          | C | 0..1        | This IE shall contain the cause of revocation received from the USS.<br>This IE may be present if the notifType is set to "REVOKE". |               |

## 6.1.6.2.4 Type: UAVAuthResponse

Table 6.1.6.2.4-1: Definition of type UAVAuthResponse

| Attribute name | Data type       | P | Cardinality | Description  | Applicability |
|----------------|-----------------|---|-------------|--|---------------|
| gpsi           | Gpsi            | M | 1           | GPSI of the UAV  |               |
| authResult     | AuthResult      | C | 0..1        | This IE shall be present for the final NEF (UAS-NF) to NF service consumer message.<br><br>Conveys the UAV authentication result |               |
| authMsg        | RefToBinaryData | O | 0..1        | Contains the service-level AA message.   |               |
| serviceLevelId | string          | O | 0..1        | This IE contains the authorized Service Level Device Identity  |               |
| authSessCorrId | string          | O | 0..1        | This IE shall contain the authentication Session Correlation Id.   |               |

## 6.1.6.2.5 Type: UAVAuthFailure

**Table 6.1.6.2.x-1: Definition of type UAVAuthFailure**

| Attribute name     | Data type      | P | Cardinality | Description  | Applicability |
|--------------------|----------------|---|-------------|--|---------------|
| error              | ProblemDetails | M | 0..1        | Represents the application error information. The application level error cause shall be encoded in the "cause" attribute.   |               |
| uasResourceRelease | boolean        | C | 0..1        | This IE shall be present and set to "true" when the NEF(UAS NF) rejects the reauthentication request with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "AUTHENTICATION_FAILURE" to indicate the UAS resource release is requested. |               |

## 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 |
|-----------|-----------------|-------------|---------------|
|           |                 |             |               |

## 6.1.6.3.3 Enumeration: AuthResult

The enumeration AuthResult represents the result of authentication and/or authorization. It shall comply with the provisions defined in table 6.1.5.3.3-1.

**Table 6.1.6.3.3-1: Enumeration AuthResult**

| Enumeration value | Description                           | Applicability |
|-------------------|---------------------------------------|---------------|
| "AUTH_SUCCESS"    | The UAV authentication has succeeded. |               |

## 6.1.6.3.4 Enumeration: NotifType

The enumeration NotifType represents the type of notification. It shall comply with the provisions defined in table 6.1.6.3.4-1.

**Table 6.1.6.3.4-1: Enumeration NotifType**

| Enumeration value | Description                                    | Applicability |
|-------------------|--|---------------|
| "REAUTH"          | The UAV needs to be reauthenticated.           |               |
| "UPDATEAUTH"      | Authorization data needs to be updated to UAV. |               |
| "REVOKE"          | Revoke UAV authentication and authorization    |               |

## 6.1.7 Error Handling

### 6.1.7.1 General

For the Nnef\_Authentication 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 Nnef\_Authentication API.

### 6.1.7.2 Protocol Errors

No specific procedures for the Nnef\_Authentication service are specified.

### 6.1.7.3 Application Errors

The application errors defined for the Nnef\_Authentication service are listed in Table 6.1.7.3-1.

**Table 6.1.7.3-1: Application errors**

| Application Error      | HTTP status code    | Description  |
|------------------------|---------------------|--|
| AUTHENTICATION_FAILURE | 403 Forbidden       | The UAV authentication is failed                                       |
| PEER_NOT_RESPONDING    | 504 Gateway Timeout | No response is received from the remote peer (i.e. USS) when time out. |

## 6.1.8 Feature negotiation

The optional features in table 6.1.8-1 are defined for the Nnef\_Authentication 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 [12] and 3GPP TS 29.500 [4], the access to the Nnef\_Authentication API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [13]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [14]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Nnef\_Authentication API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [14], 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 Nnef\_Authentication service.

The Nnef\_Authentication API defines a single scope "nnef-authentication" 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, following guidelines in 3GPP TS 29.501 [5].

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

## A.2 Nnef\_Authentication API

```
openapi: 3.0.0

info:
  title: Nnef_Authentication
  version: 1.0.0-alpha.4
  description: |
    NEF Auth Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.256 V17.0.0; 5G System;Uncrewed Aerial Systems Network Function (UAS-NF);
    Aerial Management Services; Stage 3
  url: http://www.3gpp.org/ftp/Specs/archive/29_series/29.256/

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

security:
- {}
- oAuth2ClientCredentials:
  - nnef-authentication

paths:
  /uav-authentications:
    post:
      summary: UAV authentication
      tags:
        - UAV authentication
      requestBody:
        description: UAV authentication
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/UAVAuthInfo'
      responses:
        '200':
          description: UAV Auth response or message exchange
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/UAVAuthResponse'
```

```

'307':
  $ref: 'TS29571_CommonData.yaml#/components/responses/307'
'308':
  $ref: 'TS29571_CommonData.yaml#/components/responses/308'
'400':
  $ref: 'TS29571_CommonData.yaml#/components/responses/400'
'403':
  description: UAV authentication failure
  content:
    application/json:
      schema:
        $ref: '#/components/schemas/UAVAuthFailure'
'504':
  $ref: 'TS29571_CommonData.yaml#/components/responses/504'
default:
  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
callbacks:
  authNotification:
    '{request.body#/authNotification}':
      post:
        requestBody:
          required: true
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AuthNotification'
        responses:
          '204':
            description: Successful Notification response
          '307':
            $ref: 'TS29571_CommonData.yaml#/components/responses/307'
          '308':
            $ref: 'TS29571_CommonData.yaml#/components/responses/308'
          '400':
            $ref: 'TS29571_CommonData.yaml#/components/responses/400'
          default:
            $ref: 'TS29571_CommonData.yaml#/components/responses/default'

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nnef-authentication: Access to the Nnef_authentication API

  schemas:
    #
    # STRUCTURED DATA TYPES
    #
    UAVAuthInfo:
      description: UAV auth data
      type: object
      required:
        - gpsi
        - serviceLevelId
        - nfType
      properties:
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        serviceLevelId:
          type: string
        authNotificationURI:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        ipAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/IpAddr'
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        authServerAddress:
          type: string
        authMsg:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RefToBinaryData'

```

```

ueLocInfo:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
dnn:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
sNssai:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtSnsai'
nfType:
  $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/NFType'

```

```

UVAAuthResponse:
  description: UAV auth response data
  type: object
  required:
    - gpsi
  properties:
    gpsi:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    serviceLevelId:
      type: string
    authSessCorrId:
      type: string
    authMsg:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/RefToBinaryData'
    authResult:
      $ref: '#/components/schemas/AuthResult'

```

```

AuthNotification:
  description: UAV related notification
  type: object
  required:
    - gpsi
    - serviceLevelId
    - notifType
    - authSessCorrId
  properties:
    gpsi:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    serviceLevelId:
      type: string
    authSessCorrId:
      type: string
    authMsg:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/RefToBinaryData'
    notifType:
      $ref: '#/components/schemas/NotifType'
    revokeCause:
      type: string

```

```

UVAAuthFailure:
  description: UAV auth failure
  type: object
  required:
    - error
  properties:
    error:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
    uasResourceRelease:
      type: boolean

```

```

#
# SIMPLE DATA TYPES
#

```

```

#
# ENUMERATIONS
#

```

```

AuthResult:
  description: Enumeration representing the result of authentication and/or authorization.
  anyOf:
    - type: string
      enum:
        - AUTH_SUCCESS
    - type: string
NotifType:
  description: Enumeration representing the type of notification.
  anyOf:
    - type: string

```

```
enum:  
- REAUTH  
- UPDATEAUTH  
- REVOKE  
- type: string
```

## Annex B (informative): Change history

| Change history |              |           |    |     |     |  |             |
|----------------|--------------|-----------|----|-----|-----|--|-------------|
| Date           | Meeting      | TDoc      | CR | Rev | Cat | Subject/Comment  | New version |
| 2021-04        | CT4#103-e    | C4-212292 |    |     |     | Initial TS skeleton.   | 0.0.0       |
| 2021-04        | CT4#103-e    | C4-212598 |    |     |     | Added scope, introduction, references, and abbreviations.  | 0.1.0       |
| 2021-05        | CT4#104-e    | C4-213529 |    |     |     | Aligned introduction terminology. Added, updated references.   | 0.2.0       |
| 2021-08        | CT4#105-e    | C4-214758 |    |     |     | Aligned interfaces, added Nnef_Auth service.   | 0.3.0       |
| 2021-10        | CT4#106-e    | C4-215522 |    |     |     | Several alignments with stage-2, clean-up, added OpenAPI for Nnef_Auth.  | 0.4.0       |
| 2021-11        | CT4#107-e    | C4-216474 |    |     |     | Several further alignments with stage-2: aligned API and operation names, terminology. Further clean-up done.                          | 0.5.0       |
| 2021-12        | CT#94        | CP-213160 |    |     |     | V1.0.0 presented for information   | 1.0.0       |
| 2022-01        | CT4#107bis-e | C4-220456 |    |     |     | Several consistency issues addressed. Implemented pCRs C4-220121, C4-220122, C4-220285, C4-220291, C4-220292, C4-220293, and C4-220387 | 1.1.0       |
| 2022-02        | CT4#108-e    | C4-221594 |    |     |     | Further consistency issues addressed. Implemented pCRs C4-221324, C4-221494, C4-221519, and C4-221340.                                 | 1.2.0       |
| 2022-03        | CT#95e       | CP-220109 |    |     |     | TS presented for approval  | 2.0.0       |
| 2022-03        | CT#95e       |           |    |     |     | TS approved  | 17.0.0      |

---

# History

| <b>Document history</b> |          |             |
|-------------------------|----------|-------------|
| V17.0.0                 | May 2022 | Publication |
|                         |          |             |
|                         |          |             |
|                         |          |             |
|                         |          |             |