

ETSI TS 129 255 V17.1.0 (2022-06)



**5G;
Uncrewed Aerial System Service Supplier (USS) Services;
Stage 3
(3GPP TS 29.255 version 17.1.0 Release 17)**



Reference

RTS/TSGC-0329255vh10

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.

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 Services offered by the USS.....	8
4.1 Introduction	8
4.2 Naf_Authentication Service	8
4.2.1 Service Description.....	8
4.2.1.1 Overview.....	8
4.2.1.2 Service Architecture.....	9
4.2.1.3 Network Functions.....	9
4.2.1.3.1 Uncrewed Aerial System Service Supplier (USS).....	9
4.2.1.3.2 NF Service Consumers	9
4.2.2 Service Operations	10
4.2.2.1 Introduction.....	10
4.2.2.2 Naf_Authentication_AuthenticateAuthorize Service operation	10
4.2.2.2.1 General	10
4.2.2.2.2 Authentication and Authorization of the UAV	10
4.2.2.3 Naf_Authentication_Notification Service operation.....	11
4.2.2.3.1 General	11
4.2.2.3.2 Notification for Reauthentication, Reauthorization or Revocation	11
5 API Definitions	12
5.1 Naf_Authentication Service API.....	12
5.1.1 Introduction.....	12
5.1.2 Usage of HTTP	12
5.1.2.1 General	12
5.1.2.2 HTTP standard headers	13
5.1.2.2.1 General	13
5.1.2.2.2 Content type	13
5.1.2.3 HTTP custom headers	13
5.1.3 Resources.....	13
5.1.4 Custom Operations without associated resources	13
5.1.4.1 Overview.....	13
5.1.4.2 Operation: request-auth	13
5.1.4.2.1 Description	13
5.1.4.2.2 Operation Definition.....	14
5.1.5 Notifications	14
5.1.5.1 General	14
5.1.5.2 UAV Notification.....	15
5.1.5.2.1 Description	15
5.1.5.2.2 Target URI.....	15
5.1.5.2.3 Standard Methods	15
5.1.5.2.3.1 POST.....	15
5.1.6 Data Model	16
5.1.6.1 General	16
5.1.6.2 Structured data types	17
5.1.6.2.1 Introduction	17

5.1.6.2.2	Type: UAVAuthInfo	17
5.1.6.2.3	Type: ReauthRevokeNotify	18
5.1.6.2.4	Type: UAVAuthResponse	18
5.1.6.2.5	Type: AdditionInfoAuthenticateAuthorize	19
5.1.6.3	Simple data types and enumerations	19
5.1.6.3.1	Introduction	19
5.1.6.3.2	Simple data types	19
5.1.6.3.3	Enumeration: AuthResult	19
5.1.6.3.4	Enumeration: NotifyType	19
5.1.6.3.5	Void	20
5.1.6.4	Data types describing alternative data types or combinations of data types	20
5.1.6.4.1	Type: ProblemDetailsAuthenticateAuthorize	20
5.1.7	Error Handling	20
5.1.7.1	General	20
5.1.7.2	Protocol Errors	20
5.1.7.3	Application Errors	20
5.1.8	Feature negotiation	20
5.1.9	Security	20
Annex A (normative):	OpenAPI specification	22
A.1	General	22
A.2	Naf_Authentication API	22
Annex B (informative):	Change history	26
History		27

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

The 5G System stage 2 architecture and procedures are specified in TS 23.501 [2], TS 23.502 [3], and TS 23.256 [14].

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

The UAS Service Supplier (USS) provides the UAS-specific AF services to NF service consumers (e.g. NEF (UAS-NF)). The USS is functionality within the AF.

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 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".
- [15] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".
- [16] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1]. For the purposes of the present document, the terms and definitions given in TS 23.256 [14] 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 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 TR 21.905 [1].

AF	Application Function
UAS	Uncrewed Aerial System
UAS-NF	Uncrewed Aerial System Network Function
UAV	Uncrewed Aerial Vehicle
USS	UAS Service Supplier

4 Services offered by the USS

4.1 Introduction

Table 4.1-1 summarizes the corresponding APIs defined for this specification.

Table 4.1-1: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Naf_Authentication	5.1	USS Authentication and Authorization Service	TS29255_Naf_Authentication.yaml	naf-auth	A.2

4.2 Naf_Authentication Service

4.2.1 Service Description

4.2.1.1 Overview

The Naf_Authentication service as defined in TS 23.256 [14] is provided by the USS via the Naf service-based interface (see TS 23.256 [14]).

This service:

- allows NF consumers to authentication and authorization of the UAV with the USS; and
- notifies NF consumers about reauthentication, reauthorization and revocation.

4.2.1.2 Service Architecture

The Application Function Authentication Service (Naf_Authentication) is part of the Naf service-based interface exhibited by the Application Function (AF).

The known NF service consumers of the Naf_Authentication are the Network Exposure Function (NEF) which owns the functionality of UAS-NF.

Figures 4.2.1.2-1 and 4.2.1.2-2 provide the reference model (in service-based interface representation and in reference point representation), with focus on the USS and the scope of the present specification.

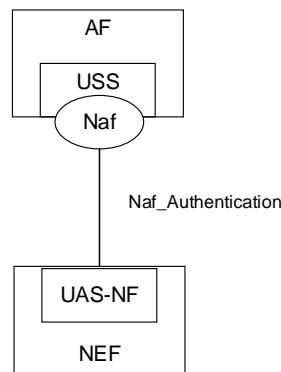


Figure 4.2.1.2-1: Reference architecture for Naf_Authentication service: SBI representation

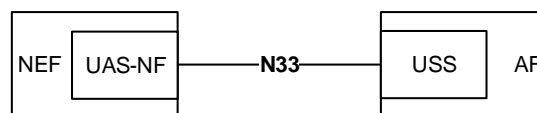


Figure 4.2.1.2-2: Reference architecture for Naf_Authentication service: reference point representation

The functionalities supported by the USS are listed in clause 4.3.2 of TS 23.256 [14].

4.2.1.3 Network Functions

4.2.1.3.1 Uncrewed Aerial System Service Supplier (USS)

The UAS service supplier (USS) application provides authentication and authorization for the UAV.

The UAS service supplier (USS) allows NF consumers to exchange communication messages needed for authentication and authorization procedure. It also notifies NF consumers about reauthentication, reauthorization or revocation of the UAV.

4.2.1.3.2 NF Service Consumers

The Uncrewed Aerial System network function (UAS NF):

- supports authentication and authorization of the UAV with the USS;
- supports subscription for notification of reauthentication, reauthorization and revocation of the UAV from the USS.

4.2.2 Service Operations

4.2.2.1 Introduction

4.2.2.2 Naf_Authentication_AuthenticateAuthorize Service operation

4.2.2.2.1 General

The Naf_Authentication_AuthenticateAuthorize service operation is used by the NF consumers during following procedure:

- UAAA-MM and UAAA-SM procedures (see TS 23.256 [14], clause 5.2.2 and clause 5.2.3, respectively)
- C2 authorization (see TS 23.256 [14], clause 5.2.5.2)

4.2.2.2.2 Authentication and Authorization of the UAV

The Naf_Authentication_AuthenticateAuthorize service operation is invoked by an NF Service Consumer (e.g. an NEF (UAS-NF)) towards the USS, when UAAA-MM is done during 5GS registration, UAAA-SM is done during PDU session establishment, or for authorization for C2 (see TS 23.256 [14]).

The NF Service Consumer (e.g. the NEF (UAS-NF)) shall send the authentication message to USS by sending the HTTP POST request towards the "request-auth" resource as shown in Figure 4.2.2.2.2-1.

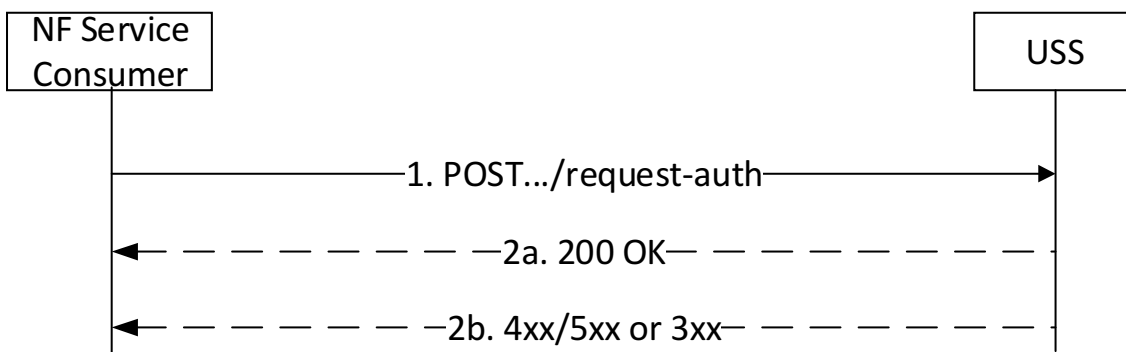


Figure 4.2.2.2.2-1: AuthenticateAuthorize Service Operation

1. The NF Service Consumer shall send a POST request to the resource with a UAVAuthInfo object in the request body. The UAVAuthInfo data type shall include:

- "gpsi" attribute that carries the GPSI (in the format of External Identifier) of the UAV;
- "serviceLevelId" attribute that carries the Service Level Device Identity of the UAV;

The UAVAuthInfo data type may include

- "uavLocInfo" attribute that provides the UAV location;
- "notifyCorrId" attribute that represents the notification correlation ID;
- "notifyUri" attribute that provides the notification URI to receive notifications related to reauthentication, reauthorization or revocation triggered by the USS, which is present in the initial request;
- "authMsg" attribute that contains the authentication message based on the authentication method used, which is present in the intermediate round-trip messages and not in initial request.

In case of UAAA-SM procedure, the UAVAuthInfo data type may also include:

- "ipAddr" attribute that carries the IP Address associated with the PDU session; and
- "pei" attribute that carries the PEI of the UAV.

2a. If the HTTP request message from the NF service consumer is accepted, the USS shall respond with "200 OK" status code with the message body containing the UAVAuthResponse data type in the response body, which shall include "gpsi" attribute.

If the USS triggers more intermediate round-trip messages, the UAVAuthResponse data shall include a "authMsg" attribute that contains the authentication message or authorization data.

Otherwise, the UAVAuthResponse data type shall contain the "authResult" attribute. If the UAV is authenticated successfully, the USS shall set the "authResult" attribute to "AUTH_SUCCESS". The UAVAuthResponse data type may include the authorized "authMsg" attribute delivering configuration information to the UAV.

2b. If the USS cannot successfully fulfil the received HTTP POST request due to an internal error or an error in the HTTP POST request, the USS shall send the HTTP error response as specified in clause 5.1.7.

If the UAV authentication is failed, the USS shall reject the request with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetailsAuthenticateAuthorize data structure set to "FAILED_AUTH". The USS shall also include an indication of "uasResRelInd" attribute in the ProblemDetailsAuthenticateAuthorize data type to indicate if an UAS service related network resource can be released or not, during re-authentication failure, when the service operation is used during Re-authentication procedure.

If the USS determines the received HTTP POST request needs to be redirected, the USS shall send an HTTP redirect response as specified in clause 5.2.10 of TS 29.122 [16].

4.2.2.3 Naf_Authentication_Notification Service operation

4.2.2.3.1 General

The Naf_Authentication_Notification service operation is used by the NF consumers during the following procedure:

- USS Initiated Re-authentication and Re-authorization (see TS 23.256 [14], clause 5.2.4)
- USS Initiated Revocation (see TS 23.256 [14], clause 5.2.7)

4.2.2.3.2 Notification for Reauthentication, Reauthorization or Revocation

The Naf_Authentication_Notification service operation is invoked by the USS to inform a NF Service Consumer (e.g. NEF (UAS-NF)), when USS triggers reauthentication, update authorization data or revoke authorization of the UAV.

The USS shall send the request by sending the HTTP POST method towards the Notification URI as shown in Figure 4.2.2.3.2-1.

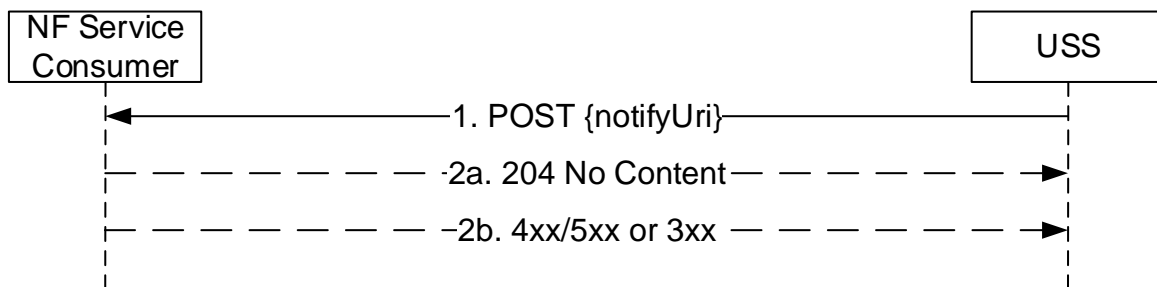


Figure 4.2.2.3.2-1: UAV Notification Service Operation

1. The USS shall send a POST request towards the Notification URI received in the Authenticate service operation request (See clause 4.2.2.1). The request body shall contain a ReauthRevokeNotify object containing the reauthentication information, update authorization information or revoke authorization indication. The ReauthRevokeNotify data type shall include
 - the "gpsi" attribute is set to the GPSI (in the format of External Identifier) of the given UAV required to be reauthenticated, reauthorized or revoked;
 - the "serviceLevelId" attribute is set to the Service Level Device Identity of the UAV;

- the "notifyCorrId" attribute is set to the same value as the "notifyCorrId" attribute of UAVAuthInfo data type received in the request;
- the "notifyType" attribute is set to REAUTHENTICATE for reauthentication and set to REAUTHORIZE for authorization data update and set to REVOKE for revocation of authorization. In addition, if "notifyType" attribute is set to REAUTHORIZE, then attribute "authMsg" containing the authorization data shall be included.

The ReauthRevokeNotify may also include:

- the "ipAddr" attribute carries the IP Address associated with the PDU session;
- 2a. On success, "204 No content" shall be returned without response body. If the "notifyType" attribute in the request indicated REVOKE, then UAS service related network resources are released.
- 2b. 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 5.1.7.

If the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 5.2.10 of TS 29.122 [16].

5 API Definitions

5.1 Naf_Authentication Service API

5.1.1 Introduction

The Naf_Authentication shall use the Naf_Authentication API.

The API URI of the Naf_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 TS 29.501 [5], i.e.:

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

with the following components:

- The {apiRoot} shall be set as described in TS 29.501 [5].
- The <apiName> shall be "naf-auth".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 5.1.3.

5.1.2 Usage of HTTP

5.1.2.1 General

HTTP/2, IETF RFC 7540 [11], shall be used as specified in of TS 29.122 [16].

HTTP/2 shall be transported as specified in TS 29.122 [16].

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

5.1.2.2 HTTP standard headers

5.1.2.2.1 General

See TS 29.122 [16] 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 TS 29.122 [16]. 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].

NOTE: This release only supports the content type JSON.

5.1.2.3 HTTP custom headers

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

5.1.3 Resources

None

5.1.4 Custom Operations without associated resources

5.1.4.1 Overview

The structure of the custom operation URIs of the Naf_Authentication service is shown in Figure 5.1.4.1-1.

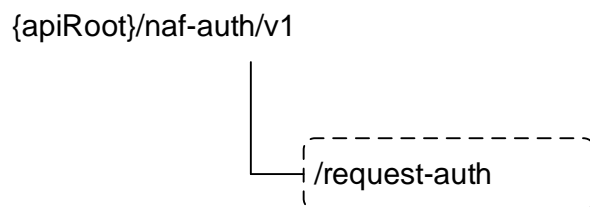


Figure 5.1.4.1-1: Custom operation URI structure of the Naf_Authentication API

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

Table 5.1.4.1-1: Custom operations without associated resources

Custom operation URI	Mapped HTTP method	Description
<code>{apiRoot}/naf-auth/<apiVersion>/request-auth</code>	POST	Request UAV authentication and authorization and subscribe to notifications triggered by the USS

5.1.4.2 Operation: request-auth

5.1.4.2.1 Description

The operation is used by the NF service consumer to request UAV authentication and authorization and subscribe to notifications triggered by the USS.

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
UAVAuthInfo	M	1	Represents the data to be used for UAV authentication and authorization

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
UAVAuthResponse	M	1	200 OK	Successful request of UAV authentication and authorization and subscription to notification of re-authentication and revocation triggered by the USS.
N/A			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 AF.
N/A			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 AF.
ProblemDetailsAuthenticateAuthorization	O	0..1	403 Forbidden	The "cause" attribute may be used to indicate the following application errors: - FAILED_AUTH See table 5.1.7.3-1 for the description of these errors.
NOTE: The mandatory HTTP error status code for the POST method listed in Table 5.2.6-1 of TS 29.122 [16] also apply.				

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	An alternative URI representing the end point of an alternative AF.

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	An alternative URI representing the end point of an alternative AF.

5.1.5 Notifications

5.1.5.1 General

This clause specifies the notifications provided by the Naf_Authentication service.

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

Table 5.1.5.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
UAV Notification	{notifyUri}	notify (POST)	Reauthentication, Reauthorization or Revocation notification

5.1.5.2 UAV Notification

5.1.5.2.1 Description

The UAV Notification is used by the USS to trigger reauthentication, reauthorization or revocation notification to a NF service consumer that has subscribed to such notifications. The USS shall notify the NF Service Consumer when reauthentication is required.

5.1.5.2.2 Target URI

The Callback URI "{**notifyUri**}" 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	Definition
notifyUri	String formatted as URI with the Callback Uri

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 5.1.5.2.3.2-1.

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

Data type	P	Cardinality	Description
ReauthRevokeNotify	M	1	Contains the reauthentication, reauthorization or revocation information.

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

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful notification of reauthentication or reauthorization or revocation.
N/A			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 NEF.
N/A			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 NEF.
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.6-1 of TS 29.122 [16] also apply.				

Table 5.1.5.2.3.1-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NEF.

Table 5.1.5.2.3.1-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NEF.

5.1.6 Data Model

5.1.6.1 General

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

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

Table 5.1.6.1-1: Naf_Authentication specific Data Types

Data type	Clause defined	Description	Applicability
UAVAuthInfo	5.1.6.2.2	Information within Authenticate Request	
UAVAuthResponse	5.1.6.2.4	Information within Authenticate Response	
AuthResult	5.1.6.3.3	Enumeration indicating authentication result	
ReauthRevokeNotify	5.1.6.2.3	Information within notification	
NotifyType	5.1.6.3.4	Enumeration Notification type	
ProblemDetailsAuthenticateAuthorize	5.1.6.4.1	Data type that extends ProblemDetails.	
AdditionInfoAuthenticateAuthorize	5.1.6.2.5	Contains more details (not only the ProblemDetails) in case an UAV authentication request is rejected.	

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

Table 5.1.6.1-2: Naf_Authentication re-used Data Types

Data type	Reference	Comments	Applicability
Pei	TS 29.571 [15]	Permanent Equipment Identifier	
Uri	TS 29.571 [15]	Uri	
Gpsi	TS 29.571 [15]	GPSI	
IpAddr	TS 29.571 [15]	IPv4 address	
LocationArea5G	TS 29.122 [16]	User location	
SupportedFeatures	TS 29.571 [15]	Used to negotiate the applicability of the optional features defined in table 5.1.8-1.	

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: UAVAuthInfo

Table 5.1.6.2.2-1: Definition of type UAVAuthInfo

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	When present, this attribute indicates the IP address associated with the PDU session.	
authMsg	string	O	0..1	Contains the authentication message or authorization data (which is not present in the initial request) used in the subsequent request messages during multiple round trip message exchanges.	
pei	Pei	O	0..1	PEI associated with the UAV.	
notifyUri	Uri	O	0..1	This attribute shall be present in the initial authentication message. It carries the notification URI to receive reauthentication, reauthorization or revocation related notifications	
notifyCorrId	string	O	0..1	Notification correlation ID assigned by the NF service consumer.	
uavLocInfo	LocationArea5G	O	0..1	This attribute shall contain the UE location information if it is available.	
suppFeat	SupportedFeatures	C	0..1	This IE shall be present if at least one optional feature defined in clause 5.1.8 is supported.	

5.1.6.2.3 Type: ReauthRevokeNotify

Table 5.1.6.2.3-1: Definition of type ReauthRevokeNotify

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	string	C	0..1	Contains the authentication message or authorization data. This attribute shall be present when "notifyType" attribute is set to REAUTHORIZE.	
ipAddr	IpAddr	O	0..1	When present, this IE indicates the IP address associated with the PDU session.	
notifyCorrId	string	C	0..1	Notification correlation ID used to identify the request to which the notification relates. It shall be present if the "notifyCorrId" attribute is provided in the request and set to the same value as the "notifyCorrId" attribute of UAVAuthInfo data type.	
notifyType	NotifyType	M	1	This attribute shall contain the notification type.	

5.1.6.2.4 Type: UAVAuthResponse

Table 5.1.6.2.4-1: Definition of type UAVAuthResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
gpsi	Gpsi	M	1	GPSI of the UAV	
authResult	AuthResult	O	0..1	Conveys the UAV authentication result (success/failure)	
authMsg	string	O	0..1	Contains the authentication message or authorization data.	
suppFeat	SupportedFeatures	C	0..1	This IE shall be present if at least one optional feature defined in clause 5.1.8 is supported.	

5.1.6.2.5 Type: AdditionInfoAuthenticateAuthorize

Table 5.1.6.2.5-1: Definition of type AdditionInfoAuthenticateAuthorize

Attribute name	Data type	P	Cardinality	Description	Applicability
uasResRelInd	boolean	C	0..1	This attribute is used to indicate if an UAS service related network resource can be released or not, during re-authentication failure. It shall be included if the "cause" attribute within the ProblemDetails data type is set to "FAILED_AUTH". When present, it shall be set as follows: - true: UAS resource release is requested; - false (default): UAS resource release is not requested.	

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

The simple data types defined in table 5.1.6.3.2-1 shall be supported.

Table 5.1.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability

5.1.6.3.3 Enumeration: AuthResult

The enumeration AuthResult represents the result of authentication and/or authorization. It shall comply with the provisions defined in table 5.1.6.3.3-1.

Table 5.1.6.3.3-1: Enumeration AuthResult

Enumeration value	Description	Applicability
AUTH_SUCCESS	The UAV authentication and/or authorization has succeeded.	

5.1.6.3.4 Enumeration: NotifyType

The enumeration NotifyType represents the type of notification. It shall comply with the provisions defined in table 5.1.6.3.4-1.

Table 5.1.6.3.4-1: Enumeration NotifyType

Enumeration value	Description	Applicability
REAUTHENTICATE	The UAV needs to be reauthenticated.	
REAUTHORIZE	Authorization data needs to be updated to UAV.	
REVOKE	Revoke UAV authentication and authorization	

5.1.6.3.5 Void

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

5.1.6.4.1 Type: ProblemDetailsAuthenticateAuthorize

Table 5.1.6.4.1-1: Definition of type ProblemDetailsAuthenticateAuthorize as a list of to be combined data types

Data type	Cardinality	Description	Applicability
ProblemDetails	1	Details of the problem as defined in TS 29.571 [15].	
AdditionInfoAuthenticateAuthorize	1	Contains additional information to indicate the handling of the UAS service related network resource, during re-authentication failure.	

5.1.7 Error Handling

5.1.7.1 General

Response bodies for error handling, as described in 3GPP TS 29.122 [16], are applicable to the APIs in the present specification unless specified otherwise, with the following clarifications:

- the SCEF is the AF; and
- the SCS/AS is the NEF invoking an API.

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

5.1.7.2 Protocol Errors

No specific procedures for the Naf_Authentication service are specified.

5.1.7.3 Application Errors

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

Table 5.1.7.3-1: Application errors

Application Error	HTTP status code	Description
FAILED_AUTH	403 Forbidden	The HTTP request is rejected because the UAV authentication is failed by the USS.

5.1.8 Feature negotiation

The optional features in table 5.1.8-1 are defined for the Naf_Authentication API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of TS 29.122 [16].

Table 5.1.8-1: Supported Features

Feature number	Feature Name	Description

5.1.9 Security

TLS shall be used to support the security communication between the NEF and the AF over N33 interface. The access to the Naf_Authentication API shall be authorized by means of OAuth2 protocol (see IETF RFC 6749 [9]), based on

local configuration, using the "Client Credentials" authorization grant. If OAuth2 is used, a client, prior to consuming services offered by the Naf_Authentication API, shall obtain a "token" from the authorization server.

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

A.2 Naf_Authentication API

```

openapi: 3.0.0
info:
  title: Naf_Authentication
  version: 1.0.0
  description: |
    AF Authentication Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.255 V17.1.0; 5G System;Uncrewed Aerial System Service Supplier (USS) Services; Stage
    3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.255/

servers:
- url: '{apiRoot}/naf-auth/v1'
  variables:
    apiRoot:
      default: https://example.com
      description: apiRoot as defined in clause 5.2.4 of 3GPP TS 29.122

security:
- {}
- oAuth2ClientCredentials: []

paths:
  /request-auth:
    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: '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':
  description: >
    The request is rejected by the USS and more details (not only the ProblemDetails) are
    returned.
  content:
    application/problem+json:
      schema:
        $ref: '#/components/schemas/ProblemDetailsAuthenticateAuthorize'
'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'
callbacks:
  reauthRevokeNotification:
    '{request.body#/notifyUri}':
      post:
        requestBody:
          required: true
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ReauthRevokeNotify'
  responses:
    '204':
      description: Successful Notification response
    '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'

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:

```



```
    tokenUrl: '{tokenUrl}'
    scopes: {}

schemas:
#
# STRUCTURED DATA TYPES
#
UAVAuthInfo:
  description: UAV auth data
  type: object
  required:
    - gpsi
    - serviceLevelId
  properties:
    gpsi:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    serviceLevelId:
      type: string
    notifyUri:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
    notifyCorrId:
      type: string
    ipAddr:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/IpAddr'
    pei:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
    authMsg:
      type: string
    uavLocInfo:
      $ref: 'TS29122_CommonData.yaml#/components/schemas/LocationArea5G'
    suppFeat:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'

UAVAuthResponse:
  description: UAV auth response data
  type: object
  required:
    - gpsi
  properties:
    gpsi:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    authMsg:
      type: string
    authResult:
      $ref: '#/components/schemas/AuthResult'
    suppFeat:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'

ReauthRevokeNotify:
  description: UAV related notification
  type: object
  required:
    - gpsi
    - serviceLevelId
    - notifyType
  properties:
    gpsi:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    serviceLevelId:
      type: string
    notifyCorrId:
      type: string
    authMsg:
      type: string
    notifyType:
      $ref: '#/components/schemas/NotifyType'
    ipAddr:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/IpAddr'

#
# SIMPLE DATA TYPES
#
```

```
#
# ENUMERATIONS
#

AuthResult:
  anyOf:
    - type: string
      enum:
        - AUTH_SUCCESS
    - type: string
NotifyType:
  anyOf:
    - type: string
      enum:
        - REAUTHENTICATE
        - REAUTHORIZE
        - REVOKE
    - type: string

ProblemDetailsAuthenticateAuthorize:
  description: Extends ProblemDetails to indicate more details during Authentication failure
  allOf:
    - $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
    - $ref: '#/components/schemas/AdditionInfoAuthenticateAuthorize'
AdditionInfoAuthenticateAuthorize:
  description: Indicates additional information during authentication failure
  type: object
  properties:
    uasResRelInd:
      type: boolean
      description: >
        Indicates to release the UAV resources during authentication failure, when set to
        "true". Default is set to "false".
```

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-08	CT3#117-e	C3-214483	-	-	-	TS skeleton	0.0.0
2021-08	CT3#117-e	C3-214588				Added scope, introduction, references, and abbreviations.	0.1.0
2021-10	CT3#118-e	C3-215474				Added service description, operations for Naf_Authentication Service and Naf_Authentication_ReauthNotify, also added resources and data model.	0.2.0
2021-11	CT3#119-e	C3-215474				Added specification related to reauthentication and revocation. Removed resource and added custom operation.	0.3.0
2021-12	CT#94-e	CP-213207				Presented for information	1.0.0
2022-01	CT3#119 bis-e	C3-220450				Inclusion of C3-220494, C3-220265, C3-220362, C3-220340, C3-220268, C3-220279, and C3-220280	1.1.0
2022-02	CT3#120	C3-221513				Inclusion of C3-221241, C3-221242, C3-221686, and C3-221302	1.2.0
2022-03	CT#95e	CP-220156				Presentation to TSG CT for approval	2.0.0
2022-03	CT#95e	CP-220156				Approved by TSG CT	17.0.0
2022-06	CT#96	CP-221143	0001			EN resolution	17.1.0
2022-06	CT#96	CP-221143	0002			Updates to Naf_Authentication_Notification	17.1.0
2022-06	CT#96	CP-221143	0003	1		Updates to Naf_Authentication_AuthenticateAuthorize service	17.1.0
2022-06	CT#96	CP-221143	0004	2		Correction to remove revocation cause	17.1.0
2022-06	CT#96	CP-221143	0005	1		Corrections to open API	17.1.0
2022-06	CT#96	CP-221143	0007			Update the data structures and OpenAPI for Naf_Authentication service	17.1.0
2022-06	CT#96	CP-221143	0008			Correction on data types for UAV Authentication and Authorization	17.1.0
2022-06	CT#96	CP-221143	0009			Correction on Security	17.1.0
2022-06	CT#96	CP-221143	0010			Correction on status codes	17.1.0
2022-06	CT#96	CP-221151	0011			Update of info and externalDocs fields	17.1.0

History

Document history		
V17.0.0	May 2022	Publication
V17.1.0	June 2022	Publication