|  |  |
| --- | --- |
| 3GPP TS 29.526 V16.7.0 (2022-03) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  5G System; Network Slice-Specific Authentication and  Authorization (NSSAA) services;  Stage 3  (Release 16) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions, symbols and abbreviations 8

3.1 Definitions 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview 8

4.1 Introduction 8

5 Services offered by the NSSAAF 9

5.1 Introduction 9

5.2 Nnssaaf\_NSSAA Service 9

5.2.1 Service Description 9

5.2.2 Service Operations 10

5.2.2.1 Introduction 10

5.2.2.2 Authenticate 10

5.2.2.2.1 General 10

5.2.2.3 Re-Authentication Notification 13

5.2.2.3.1 General 13

5.2.2.4 Revocation Notification 14

5.2.2.4.1 General 14

6 API Definitions 15

6.1 Nnssaaf\_NSSAA Service API 15

6.1.1 Introduction 15

6.1.2 Usage of HTTP 16

6.1.2.1 General 16

6.1.2.2 HTTP standard headers 16

6.1.2.2.1 General 16

6.1.2.2.2 Content type 16

6.1.2.3 HTTP custom headers 16

6.1.3 Resources 16

6.1.3.1 Overview 16

6.1.3.2 Resource: slice-authentications (Collection) 17

6.1.3.2.1 Description 17

6.1.3.2.2 Resource Definition 17

6.1.3.2.3 Resource Standard Methods 17

6.1.3.2.4 Resource Custom Operations 19

6.1.3.3 Resource: slice-authentication (Document) 19

6.1.3.3.1 Description 19

6.1.3.3.2 Resource Definition 19

6.1.3.3.3 Resource Standard Methods 19

6.1.3.3.4 Resource Custom Operations 21

6.1.4 Custom Operations without associated resources 21

6.1.4.1 Overview 21

6.1.5 Notifications 21

6.1.5.1 General 21

6.1.5.2 Re-authentication Notification 22

6.1.5.2.1 Description 22

6.1.5.2.2 Target URI 22

6.1.5.2.3 Standard Methods 22

6.1.5.3 Revocation Notification 23

6.1.5.3.1 Description 23

6.1.5.3.2 Target URI 23

6.1.5.3.3 Standard Methods 23

6.1.6 Data Model 24

6.1.6.1 General 24

6.1.6.2 Structured data types 25

6.1.6.2.1 Introduction 25

6.1.6.2.2 Type: SliceAuthInfo 25

6.1.6.2.3 Type: SliceAuthContext 25

6.1.6.2.4 Type: SliceAuthConfirmationData 26

6.1.6.2.5 Type: SliceAuthConfirmationResponse 26

6.1.6.2.6 Type: SliceAuthReauthNotification 26

6.1.6.2.7 Type: SliceAuthRevocNotification 26

6.1.6.3 Simple data types and enumerations 26

6.1.6.3.1 Introduction 26

6.1.6.3.2 Simple data types 26

6.1.6.3.3 Enumeration: SliceAuthNotificationType 27

6.1.6.4 Data types describing alternative data types or combinations of data types 27

6.1.6.5 Binary data 27

6.1.7 Error Handling 27

6.1.7.1 General 27

6.1.7.2 Protocol Errors 27

6.1.7.3 Application Errors 27

6.1.8 Feature negotiation 28

6.1.9 Security 28

Annex A (normative): OpenAPI specification 29

A.1 General 29

A.2 Nnssaaf\_NSSAA API 29

Annex B (informative): Change history 34

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

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

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

[6] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[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] IETF RFC 4648: "The Base16, Base32 and Base64 Data Encodings".

[15] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

[16] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

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

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 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].

NSSAA Network Slice-Specific Authentication and Authorization

NSSAAF NSSAA Function

# 4 Overview

## 4.1 Introduction

Within the 5GC, the NSSAAF offers services to the AMF via the Nnssaaf service based interface.

The AMF shall make use of the NSSAAF service when it needs to invoke network slice-specific authentication and authorization for a specific UE and a specific S-NSSAI (see 3GPP TS 23.502 [3] clause 4.2.9.2, and 3GPP TS 33.501 [14] clause 16.2 and 16.3).

The NSSAAF service shall also be used by the AMF to receive slice re-authentication notification or slice authorization revocation notification sent from the AAA-S (see 3GPP TS 23.502 [3] clause 4.2.9.3, 4.2.9.4 and 3GPP TS 33.501 [14] clause 16.3 and 16.4).

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



Figure 4.1-1: Reference model – NSSAAF

# 5 Services offered by the NSSAAF

## 5.1 Introduction

The NSSAAF offers the following services via the Nnssaaf interface:

- Nnssaaf\_NSSAA Service

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

Table 5.1-1: API Descriptions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service Name | Clause | Description | OpenAPI Specification File | apiName | **Annex** |
| Nnssaaf\_NSSAA | 5.2 | slice-Specific authentication and authorization service | Nnssaaf\_NSSAA.yaml | nnssaaf-nssaa | A.2 |

## 5.2 Nnssaaf\_NSSAA Service

### 5.2.1 Service Description

The Nnssaaf\_NSSAA service provides slice-specific authentication and authorization for a given UE. The NSSAAF is acting as NF Service Producer, while the AMF is the NF Service Consumer.

Following functionalities are provided by the Nnssaaf service:

- Perform slice-specific authentication and authorization for a given UE;

- Trigger slice-specific re-authentication to a given UE;

- Revoke the slice-specific authentication and authorization for a given UE.

The Nnssaaf\_NSSAA service supports the following service operations.

Table 5.2.1-1: Service operations supported by the Nnssaaf\_NSSAA service

|  |  |  |  |
| --- | --- | --- | --- |
| Service Operations | Description | Operation  Semantics | Example Consumer(s) |
| Authenticate | Perform slice-specific authentication and authorization for a given UE. | Request/Response | AMF |
| Re-Authentication Notification | Request slice-specific re-authentication and re-authorization for a given UE. | Callback | AMF |
| Revocation Notification | Request revocation of slice-specific authentication and authorization result for a given UE. | Callback | AMF |

### 5.2.2 Service Operations

#### 5.2.2.1 Introduction

See Table 5.2.1-1 for an overview of the service operations supported by the Nnssaaf\_NSSAA service.

#### 5.2.2.2 Authenticate

##### 5.2.2.2.1 General

The Authenticate service operation permits the NF Service Consumer (i.e. the AMF) to initiate slice-specific authentication and authorization, e.g. during a UE Registration procedure or upon reception of a re-authentication notification from the NSSAAF (see clause 5.2.2.3). The NSSAAF may relay the EAP message to an AAA-S and collect the result of slice-specific authentication and authorization from the AAA-S, as specified in clause 4.2.9.2 of 3GPP TS 23.502 [3], and clause 16.3 of 3GPP TS 33.501 [8].

The NF Service Consumer (i.e. the AMF) shall send a POST request to the resource representing slice authentication collection (i.e. …/v1/slice-authentications) to request the NSSAAF to create the corresponding resource context and perform slice-specific authentication and authorization.



Figure 5.2.2.2.1-1: Slice-Specific Authentication and Authorization

1. The NF Service Consumer (AMF) shall send a POST request to the NSSAAF, targeting the resource of slice authentication collection (i.e. …/v1/slice-authentications), to perform slice-specific authentication and authorization.

The payload of the body shall contain the slice authentication information, which includes:

- UE ID (i.e. GPSI)

- S-NSSAI

- EAP ID Response message (if it is received from the UE), or the EAP ID Response message with EAP ID stored, or the EAP ID Response message with Null value (if EAP ID is not requested or received);

- optionally, the callback URI of the AMF to receive re-authentication notification from the NSSAAF;

- optionally, the callback URI of the AMF to receive revocation notification from the NSSAAF.

Based on local policy, the AMF may determine to provide callback URI(s) for receiving re-authentication notification or revocation notification. For example, the callback URIs are provided for an UE identified with low mobility characteristic.

If Slice-Specific Authentication and Authorization is triggered by the AMF during a Registration procedure as described in clause 4.2.9.2 of 3GPP TS 23.502 [3], the AMF shall set "status" attribute for the given slice listed in "nssaaStatusList" attribute to "PENDING" (See 3GPP TS 29.518 [16]).

2. The NSSAAF creates slice authentication context for the UE, and starts the slice-specific authentication and authorization procedure. If the AAA-S is involved in slice-specific authentication and authorization procedure, the NSSAAF shall forward the EAP ID Response message to the AAA-S if the EAP ID Response message does not contain the Null value. Depending on the result, either step 3a or step 3b is performed. The NSSAAF obtains the AAA-S address from local configuration, based on S-NSSAI.

3a. On success, "201 Created" shall be returned. The "Location" header shall contain the URI of the created resource (e.g. .../v1/slice-authentications/{authCtxId}). The payload body shall contain the slice authentication context, which includes the EAP message generated by the NSSAAF or from the AAA-S. The NF Service Consumer (i.e. the AMF) shall forward the received EAP message to the UE in NAS message, as specified in clause 4.2.9.2 of 3GPP TS 23.502 [3].

3b. On failure, one of the HTTP status code listed in Table 6.1.7.3-1 shall be returned with the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1. If the slice is not authorized, the NSSAAF shall use the "SLICE\_AUTH\_REJECTED" application error code.

3c. On redirection, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned. A RedirectResponse IE may be included in the payload body of POST response, as specified in table 6.1.3.2.3.1-3.

4. Once receiving EAP message from the UE, the NF Service Consumer (i.e. the AMF) shall send a PUT request to the NSSAAF, targeting the resource of the slice authentication context (i.e. …/v1/slice-authentications/{authCtxId}).

The payload body shall carry the slice authentication confirmation data which includes:

- UE ID (i.e. GPSI)

- S-NSSAI

- AAA-S address

- EAP Message (which is received from the UE)

5. The NSSAAF checks and confirms the slice-specific authentication and authorization. If the AAA-S is involved, the NSSAAF shall forward the EAP Message to the AAA-S to confirm the slice-specific authentication and authorization. Depending on the result, either step 6a or step 6b is performed.

6a. On success, "200 OK" shall be returned. The payload body shall contain the slice authentication confirmation response, which includes the EAP message (e.g. EAP success/failure message) generated by the NSSAAF or from the AAA-S. The NF Service Consumer (i.e. the AMF) shall forward the EAP message to the UE in NAS message.

If the UE is authenticated, the NSSAAF shall set the "authResult" attribute to "EAP\_SUCCESS". If failed to authenticate the UE, the "authResult" attribute shall be set to "EAP\_FAILURE".

If subsequent EAP message exchange is needed between the UE and the NSSAAF(AAA-S), the NSSAAF shall not include SliceAuthResult in the response message.

6b. On failure, one of the HTTP status codes listed in Table 6.1.7.3-1 shall be returned with the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

6c. On redirection, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned. A RedirectResponse IE may be included in the payload body of POST response, as specified in table 6.1.3.3.3.1-3.

7-9. If subsequent EAP message exchange is needed between the UE and the NSSAAF to finish the EAP based authentication, step 7-9 are performed. On failure, one of the HTTP status codes listed in Table 6.1.7.3-1 shall be returned with the message body containing a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1. On redirection, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned, and a RedirectResponse IE may be included in the message body, as specified in table 6.1.3.3.3.1-3.

In above steps, if the AAA-S is involved in the slice-specific authentication and authorization procedure while there is no expected response from the AAA-S in the case of time out, the NSSAAF shall return HTTP status code "504 Gateway Timeout", with the message body containing a ProblemDetails structure with the "cause" attribute set to "TIMED\_OUT\_REQUEST".

After the completion of slice-specific authentication and authorization procedure, it is up to implementation whether the NSSAAF stores the slice authentication context and related resources for a configured period, or deletes the context and resource immediately, e.g. depending on the potential need for AAA-S initiated slice-specific re-authentication/revocation notification.

If the slice-specific authentication and authorization was successful (i.e. "authResult" attribute received from NSSAAF in step 6a is set to "EAP\_SUCCESS"), the AMF shall set "status" attribute for the given slice listed in "nssaaStatusList" attribute to "EAP\_SUCCESS" (see 3GPP TS 29.518 [16]).

If the slice-specific authentication and authorization finally fails (i.e. "authResult" attribute received from NSSAAF in step 6a is set to "EAP\_FAILURE"), the AMF shall set "status" attribute for the given slice listed in "nssaaStatusList" attribute to "EAP\_FAILURE" (see 3GPP TS 29.518 [16]). In this case, if there are PDU sessions previously established corresponding to the S-NSSAIs required to be authenticated, the AMF should additionally trigger the release of those PDU sessions.

If the slice-specific authentication and authorization cannot be completed, then:

- If it is due to receiving a response with HTTP status code "504 Gateway Timeout" or due to lack of response from the NSSAAF during an NSSAA procedure, the AMF may later re-initiate slice-specific authentication and authorization procedure based on its policy. The AMF should wait for a configured period before re-initiating slice-specific authentication and authorization procedure. If the retry attempts are exhausted, the AMF stops the slice-specific authentication and authorization procedure.

NOTE 1: It is recommended to limit the number of retry attempts as described in 3GPP TS 29.500 [4].

- If it is due to the UE becoming unreachable during an NSSAA procedure, the AMF stops the slice-specific authentication and authorization procedure.

- If the AMF stops the slice-specific authentication and authorization procedure (i.e. after exhausting the retry attempts or when the UE becomes unreachable), the AMF shall keep the "status" attribute set to "PENDING", for the given slice(s) listed in "nssaaStatusList" attribute (see 3GPP TS 29.518 [16]).

NOTE 2: The AMF initiates the slice-specific authentication and authorization for S-NSSAIs in "PENDING" status at next UE uplink activity.

#### 5.2.2.3 Re-Authentication Notification

##### 5.2.2.3.1 General

The Re-Authentication Notification service operation shall be used by the NSSAAF to notify the AMF to re-initiate slice-specific authentication and authorization for a given UE, as specified in clause 4.2.9.3 of 3GPP TS 23.502 [3], and clause 16.4 of 3GPP TS 33.501 [8].

If there are two different AMFs serving the UE (e.g. the NSSAAF retrieves two different AMFs from the UDM), the NSSAAF may determine to send the re-authentication notification to both AMFs. Or, the NSSAAF may first send re-authentication notification to one of the AMF, and then send revocation notification to another AMF if EAP authentication fails in first AMF. If EAP authentication succeeds in first AMF then NSSAAF does not notify the other AMF.

The NSSAAF shall notify the NF Service Consumer (i.e. the AMF) by using the HTTP POST method as shown in Figure 5.2.2.3.1-1.



Figure 5.2.2.3.1-1: Re-authentication Notification

1. The NSSAAF shall send a POST request to the callback URI used to receiving re-authentication notification, which is either provided by the NF Service Consumer (i.e. the AMF), or retrieved from the AMF profile stored in the NRF.

The HTTP payload body of the POST request shall contain the SliceAuthReauthNotification data structure, within which:

- the notificationType set to the SliceAuthNotificationType of "SLICE\_RE\_AUTH";

- the gpsi set to the GPSI of the given UE required to be re-authenticated;

- the snssai set to the S-NSSAI required to be re-authenticated;

- the supi set to the SUPI of the given UE required to be re-authenticated.

NOTE: The NSSAAF can obtain the SUPI of the UE in the response of a previous Nudm\_UECM\_Get used by the NSSAAF to retrieve the AMF ID.

2a. On success, "204 No Content" shall be returned and the payload body of the POST response shall be empty.

After responding the request, the NF Service Consumer (i.e. the AMF) shall send NAS message to the UE to trigger re-authentication and re-authorization for the given slice.

The AMF then decides to execute the Slice-Specific Authentication and Authorization if needed as described in clause 5.2.2.2.1.

2b. On failure, one of the HTTP status code (e.g. "404 Not Found") listed in Table 6.1.7.3-1 shall be returned.

For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

2c. On redirection, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned. A RedirectResponse IE may be included in the payload body of POST response, as specified in table 6.1.5.2.3.1-3.

If the NF Service Consumer (i.e. the AMF) is not able to handle the request, but knows that another NF Service Consumer (i.e. the AMF) is able to handle it, it shall reply with an HTTP 3xx redirect error response pointing to the URI of the new NF Service Consumer (i.e. the AMF).

#### 5.2.2.4 Revocation Notification

##### 5.2.2.4.1 General

The Revocation Notification service operation shall be used by the NSSAAF to notify the AMF to revoke slice-specific authentication and authorization result, as specified in clause 4.2.9.4 of 3GPP TS 23.502 [3], and clause 16.5 of 3GPP TS 33.501 [8], and may trigger the AMF to release the corresponding PDU sessions associated to the indicated slice.

If there are two different AMFs serving the UE (e.g. the NSSAAF retrieves two different AMFs from the UDM), the NSSAAF may determine to send revocation notification to both AMFs.

The NSSAAF shall notify the NF Service Consumer (i.e. the AMF) by using the HTTP POST method as shown in Figure 5.2.2.4.1-1.



Figure 5.2.2.4.1-1: Revocation Notification

1. The NSSAAF shall send a POST request to the revocation notification callback URI, which is either provided by the NF Service Consumer (i.e. the AMF), or retrieved from the AMF profile stored in the NRF.

The HTTP payload body of the POST request shall contain the SliceAuthRevocNotification data structure, within which:

- the notificationType set to the SliceAuthNotificationType of "SLICE\_REVOCATION";

- the gpsi set to the GPSI of the given UE for whom the slice-specific authorization revocation is required;

- the snssai set to the S-NSSAI for which the slice-specific authorization revocation is required;

- the supi set to the SUPI of the given UE for whom the slice-specific authorization revocation is required.

NOTE: The NSSAAF can obtain the SUPI of the UE in the response of a previous Nudm\_UECM\_Get used by the NSSAAF to retrieve the AMF ID.

2a. On success, "204 No Content" shall be returned and the payload body of the POST response shall be empty.

On receiving the request, the NF Service Consumer (i.e. the AMF) shall revoke the slice-specific authentication and authorization result for the given UE. If there is PDU session associated to the given slice, the AMF shall trigger the PDU session release to the SMF, with appropriate cause value.

The AMF shall remove the "status" for the given slice in "nssaaStatusList" attribute (see 3GPP TS 29.518 [16]).

2b. On failure, one of the HTTP status code (e.g. "404 Not Found") listed in Table 6.1.7.3-1 shall be returned.

For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

2c. On redirection, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned. A RedirectResponse IE may be included in the payload body of POST response, as specified in table 6.1.5.3.3.1-2.

If the NF Service Consumer (i.e. the AMF) is not able to handle the request, but knows that another NF Service Consumer (i.e. the AMF) is able to handle it, it shall reply with an HTTP 3xx redirect error response pointing to the URI of the new NF Service Consumer (i.e. the AMF).

# 6 API Definitions

## 6.1 Nnssaaf\_NSSAA Service API

### 6.1.1 Introduction

The Nnssaaf\_NSSAA service shall use the Nnssaaf\_NSSAA API.

The API URI of the <Service 1> API shall be:

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

The request URIs used in HTTP request 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 "nnssaaf-nssaa".

- The <apiVersion> shall be "v1".

- The <apiSpecificResourceUriPart> shall be set as described in clause 5.3.

### 6.1.2 Usage of HTTP

#### 6.1.2.1 General

HTTP/2, IETF RFC 7540 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

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

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

#### 6.1.2.2 HTTP standard headers

##### 6.1.2.2.1 General

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

##### 6.1.2.2.2 Content type

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

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [13].

#### 6.1.2.3 HTTP custom headers

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

### 6.1.3 Resources

#### 6.1.3.1 Overview

The structure of the Resource URIs of the Nnssaaf\_NSSAA service is shown in Figure 6.1.3.1-1



Figure 6.1.3.1-1: Resource URI structure of the NSSAA 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 |
| slice-authentications  (Collection) | /v1/slice-authentications | POST | Initiate the slice-specific authentication and authorization process by providing inputs related to the UE and a specific slice. |
| slice-authentication  (Document) | /v1/slice-authentications/{authCtxId} | PUT | Put the UE response from the EAP process. |

#### 6.1.3.2 Resource: slice-authentications (Collection)

##### 6.1.3.2.1 Description

This resource represents a collection of the slice-authentication resources generated by the NSSAAF.

##### 6.1.3.2.2 Resource Definition

Resource URI: **{apiRoot}/nnssaaf-nssaa /<apiVersion>/slice-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 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 |
| SliceAuthInfo | M | 1 | Contains the GPSI, S-NSSAI, and EAP ID Response from the UE, etc. |

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 |
| SliceAuthContext | M | 1 | 201 Created | This case indicates the corresponding resource has been created by the NSSAAF for the requested slice-specific authentication and authorization, and further EAP process is required.  The HTTP response shall include a "Location" header that contains the resource URI of the created resource. |
| 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 this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSSAAF or NSSAAF (service) set. |
| 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 this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSSAAF or NSSAAF (service) set.  (NOTE 2) |
| ProblemDetails | O | 0..1 | 400 Bad Request | This case represents the failure to start slice-specific authentication and authorization because of input parameter error. |
| ProblemDetails | O | 0..1 | 403 Forbidden | This case represents when the UE or the slice is not allowed to be authenticated.  The "cause" attribute may be used to indicate one of the following application errors:  - SLICE\_AUTH\_REJECTED |
| ProblemDetails | O | 0..1 | 404 Not Found | This case represents the user or user context is not found.  The "cause" attribute may be used to indicate one of the following application errors:  - CONTEXT\_NOT\_FOUND  - USER\_NOT\_FOUND |
| ProblemDetails | O | 0..1 | 504 Gateway Time out | This case represents network error or remote peer (i.e. AAA-S) error, e.g. not reachable, no response and time out.  The "cause" attribute may be used to indicate one of the following application errors:  - NETWORK\_FAILURE  - UPSTREAM\_SERVER\_ERROR  - TIME\_OUT\_REQUEST |
| 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 POST method on this resource

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

Table 6.1.3.2.3.1-5: Headers supported by the 201 response code on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | URI | M | 1 | URI of created resource for the slice authentication context.  The URI structure is defined in clause 6.1.3.3.1. |

Table 6.1.3.2.3.1-6: Links supported by the 201 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Resource name | HTTP method or custom operation | Link parameter(s) | Description |
| n/a |  |  |  |  |

Table 6.1.3.2.3.1-7: Headers supported by the 307 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | URI pointing to the resource of another NF service producer to which the request should be sent.  Or the same URI, if a request is redirected to the same target resource via a different SCP. |

Table 6.1.3.2.3.1-8: Headers supported by the 308 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | URI pointing to the resource of another NF service producer to which the request should be sent.  Or the same URI, if a request is redirected to the same target resource via a different SCP. |

##### 6.1.3.2.4 Resource Custom Operations

There is no Resource Custom Operations in the current version of this API.

#### 6.1.3.3 Resource: slice-authentication (Document)

##### 6.1.3.3.1 Description

The sub-resource "slice-authentication" is generated by the NSSAAF. This subresource should not persist after the slice-specific authentication and authorization process finishes.

##### 6.1.3.3.2 Resource Definition

Resource URI: **{apiRoot}/nnssaaf-nssaa/<apiVersion>/slice-authentications/{authCtxId}**

This resource shall support the resource URI variables defined in table 6.1.3.3.2-1.

Table 6.1.3.3.2-1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data type | Definition |
| apiRoot | string | See clause 6.1.1 |
| apiVersion | string | See clause 6.1.1 |
| authCtxId | string | The slice authentication context ID, which is of data type SliceAuthCtxId defined in clause 6.1.6.3.2. |

##### 6.1.3.3.3 Resource Standard Methods

6.1.3.3.3.1 PUT

This method shall support the URI query parameters specified in table 6.1.3.3.3.1-1.

Table 6.1.3.3.3.1-1: URI query parameters supported by the PUT method on this resource

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

This method shall support the request data structures specified in table 6.1.3.3.3.1-2 and the response data structures and response codes specified in table 6.1.3.3.3.1-3.

Table 6.1.3.3.3.1-2: Data structures supported by the PUT Request Body on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| SliceAuthConfirmationData | M | 1 | Contains the EAP message generated by the UE and provided to the AMF. |

Table 6.1.3.3.3.1-3: Data structures supported by the PUT Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| SliceAuthConfirmationResponse | M | 1 | 200 OK | This case indicates that the NSSAAF has performed the slice-specific authentication. The response body shall contain the result of the slice-specific 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 this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSSAAF or NSSAAF (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 this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSSAAF or NSSAAF (service) set.  (NOTE 2) |
| ProblemDetails | O | 0..1 | 400 Bad Request | This case represents a slice-specific authentication failure because of input parameter error. This indicates that the NSSAAF was not able to process the slice-specific authentication. |
| ProblemDetails | O | 0..1 | 403 Forbidden | This case represents when the UE or the slice is not allowed to be authenticated.  The "cause" attribute may be used to indicate one of the following application errors:  - SLICE\_AUTH\_REJECTED |
| ProblemDetails | O | 0..1 | 404 Not Found | This case represents the UE or UE related context is not found.  The "cause" attribute may be used to indicate one of the following application errors:  - CONTEXT\_NOT\_FOUND  - USER\_NOT\_FOUND |
| ProblemDetails | O | 0..1 | 504 Gateway Time out | This case represents network error or remote peer (i.e. AAA-S) error, e.g. not reachable, no response when time out.  The "cause" attribute may be used to indicate one of the following application errors:  - NETWORK\_FAILURE  - UPSTREAM\_SERVER\_ERROR  - TIMED\_OUT\_REQUEST |
| NOTE 1: The mandatory HTTP error status code for the PUT 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 6.1.3.3.3.1-4: Headers supported by the PUT method on this resource

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

Table 6.1.3.3.3.1-5: Headers supported by the 200 response code on this resource

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

Table 6.1.3.3.3.1-6: Links supported by the 200 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Resource name | HTTP method or custom operation | Link parameter(s) | Description |
| n/a |  |  |  |  |

Table 6.1.3.3.3.1-7: Headers supported by the 307 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | URI pointing to the resource of another NF service producer to which the request should be sent.  Or the same URI, if a request is redirected to the same target resource via a different SCP. |

Table 6.1.3.3.3.1-8: Headers supported by the 308 Response Code on this endpoint

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | URI pointing to the resource of another NF service producer to which the request should be sent.  Or the same URI, if a request is redirected to the same target resource via a different SCP. |

##### 6.1.3.3.4 Resource Custom Operations

There is no Resource Custom Operations in the current version of this API.

### 6.1.4 Custom Operations without associated resources

#### 6.1.4.1 Overview

There is no Custom Operation in the current version of this API.

### 6.1.5 Notifications

#### 6.1.5.1 General

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].

Table 6.1.5.1-1: Notifications overview

|  |  |  |  |
| --- | --- | --- | --- |
| Notification | Resource URI | HTTP method or custom operation | Description  (service operation) |
| Re-authentication Notification | {reauthNotifUri}  (NF Service Consumer provided callback reference) | POST | Re-authentication Notification |
| Revocation Notification | {revocNotifUri}  (NF Service Consumer provided callback reference) | POST | Revocation Notification |

#### 6.1.5.2 Re-authentication Notification

##### 6.1.5.2.1 Description

The Re-authentication Notification is used by the NSSAAF to trigger the NF Service Consumer (i.e. the AMF) to re-initiate slice-specific authentication and authorization for a given UE.

##### 6.1.5.2.2 Target URI

The Notification URI **"{reauthNotifUri}"** shall be used with the resource URI variables defined in table 6.1.5.2.2-1.

Table 6.1.5.2.2-1: Resource URI variables for this resource

|  |  |
| --- | --- |
| Name | Definition |
| reauthNotifUri | String formatted as URI which carries the re-authentication notification 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 on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| SliceAuthReauthNotification | M | 1 | SliceAuthReauthNotification which carries the re-authentication notification for a given UE. |

Table 6.1.5.2.3.1-2: Data structures supported by the POST Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response codes | Description |
| n/a |  |  |  |  |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection. The NF service consumer shall generate a Location header field containing a URI pointing to the endpoint of another NF service consumer to which 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 NF service consumer shall generate a Location header field containing a URI pointing to the endpoint of another NF service consumer to which 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.  NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. | | | | |

#### 6.1.5.3 Revocation Notification

##### 6.1.5.3.1 Description

The Revocation Notification is used by the NSSAAF to trigger the NF Service Consumer (i.e. the AMF) to revoke the slice-specific authentication and authorization result for a given UE.

##### 6.1.5.3.2 Target URI

The Notification URI **"{revocNotifUri}"** shall be used with the resource URI variables defined in table 6.1.5.3.2-1.

Table 6.1.5.3.2-1: Resource URI variables for this resource

|  |  |
| --- | --- |
| Name | Definition |
| revocNotifUri | String formatted as URI which carries the revocation notification URI. |

##### 6.1.5.3.3 Standard Methods

6.1.5.3.3.1 POST

This method shall support the request data structures specified in table 6.1.5.3.3.1-1 and the response data structures and response codes specified in table 6.1.5.3.3.1-2.

Table 6.1.5.3.3.1-1: Data structures supported by the POST Request Body on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| SliceAuthRevocNotification | M | 1 | SliceAuthNotification which carries the revocation notification for a given UE. |

Table 6.1.5.3.3.1-2: Data structures supported by the POST Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response codes | Description |
| n/a |  |  |  |  |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection. The NF service consumer shall generate a Location header field containing a URI pointing to the endpoint of another NF service consumer to which 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 NF service consumer shall generate a Location header field containing a URI pointing to the endpoint of another NF service consumer to which 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.  NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. | | | | |

### 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 Nnssaaf service based interface protocol.

Table 6.1.6.1-1: Nnssaaf specific Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Clause defined | Description | Applicability |
| SliceAuthInfo | 6.1.6.2.2 | Contains the GPSI, S-NSSAI, EAP ID Response, etc. |  |
| SliceAuthContext | 6.1.6.2.3 | Contains the information of the resource created for slice-specific authentication and authorization. |  |
| SliceAuthConfirmationData | 6.1.6.2.4 | Contains the EAP message from the UE for EAP process. |  |
| SliceAuthConfirmationResponse | 6.1.6.2.5 | Contains the slice-specific authentication and authorization result from the NSSAAF to the UE. |  |
| SliceAuthReauthNotification | 6.1.6.2.6 | Contains the re-authentication notification for slice-specific authentication and authorization. |  |
| SliceAuthRevocNotification | 6.1.6.2.7 | Contains the revocation notification for slice-specific authentication and authorization. |  |
| SliceAuthCxtId | 6.1.6.3.2 | Contains the resource ID of slice authentication context. |  |
| EapMessage | 6.1.6.3.2 | Contains the string formatted EAP message. |  |
| SliceNotificationType | 6.1.6.3.3 | Notification type of slice-specification authentication and authorization. |  |

Table 6.1.6.1-2 specifies data types re-used by the Nnssaaf 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 Nnssaaf service based interface.

Table 6.1.6.1-2: Nnssaaf re-used Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Reference | Comments | Applicability |
| ProblemDetails | 3GPP TS 29.571 [10] | Common Data Type used in response bodies |  |
| RedirectResponse | 3GPP TS 29.571 [10] | Redirect Response |  |
| Gpsi | 3GPP TS 29.571 [10] | GPSI |  |
| Snssai | 3GPP TS 29.571 [10] | S-NSSAI |  |
| AuthStatus | 3GPP TS 29.571 [10] | Slice Authentication Status |  |
| Supi | 3GPP TS 29.571 [10] | SUPI of the UE |  |

#### 6.1.6.2 Structured data types

The following clause defines the structures to be used in resource representations.

##### 6.1.6.2.1 Introduction

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

##### 6.1.6.2.2 Type: SliceAuthInfo

Table 6.1.6.2.2-1: Definition of type SliceAuthInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| eapIdRsp | EapMessage | M | 1 | Contains the EAP ID Responses message from the UE.  If no EAP ID Responses message is received or requested, it shall contain the Null value. |  |
| amfInstanceId | NfInstanceId | O | 0..1 | This IE may be present, if the AMF determines to provide the re-authentication/revocation notification URI to the NSSAAF.  When present, it shall contain the NF Instance Id of the AMF. |  |
| reauthNotifUri | Uri | O | 0..1 | This IE may be present, e.g. if the AMF determines the UE with low mobility characteristic.  When present, it shall contain the re-authentication notification URI. |  |
| revocNotifUri | Uri | O | 0..1 | This IE may be present, e.g. if the AMF determines the UE with low mobility characteristic.  When present, it shall contain the revocation notification URI. |  |

##### 6.1.6.2.3 Type: SliceAuthContext

Table 6.1.6.2.3-1: Definition of type SliceAuthContext

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| authCtxId | SliceAuthCtxId | M | 1 | Indicates the resource ID uniquely identifying the slice authentication context, generated by the NSSAAF. |  |
| eapMessage | EapMessage | M | 1 | Contains the EAP message to be sent to the UE. |  |

##### 6.1.6.2.4 Type: SliceAuthConfirmationData

Table 6.1.6.2.4-1: Definition of type SliceAuthConfirmationData

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| eapMessage | EapMessage | M | 1 | Contains the EAP message received from the UE. |  |

##### 6.1.6.2.5 Type: SliceAuthConfirmationResponse

Table 6.1.6.2.5-1: Definition of type SliceAuthConfirmationResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| eapMessage | EapMessage | M | 1 | Contains the EAP success/failure message needs to be sent to the UE. |  |
| authResult | AuthStatus | O | 0..1 | When present, it shall indicate the result of slice-specific authentication and authorization. |  |

##### 6.1.6.2.6 Type: SliceAuthReauthNotification

Table 6.1.6.2.6-1: Definition of type SliceAuthReauthNotification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| notificationType | SliceAuthNotificationType | M | 1 | Indicate the type of slice authentication notification. |  |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| supi | Supi | C | 0..1 | This IE should be sent by the NSSAAF to the AMF, if available. |  |

##### 6.1.6.2.7 Type: SliceAuthRevocNotification

Table 6.1.6.2.7-1: Definition of type SliceAuthRevocNotification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| notificationType | SliceAuthNotificationType | M | 1 | Indicate the type of slice authentication notification. |  |
| gpsi | Gpsi | M | 1 | Contains the GPSI of the UE. |  |
| snssai | Snssai | M | 1 | Contains the S-NSSAI for authentication. |  |
| supi | Supi | C | 0..1 | This IE should be sent by the NSSAAF to the AMF, if available. |  |

#### 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 |
| SliceAuthCtxId | string | The resource ID uniquely identifying the slice authentication context, generated by the NSSAAF. |  |
| EapMessage | string | The EAP packet is encoded using base64 (see IETF RFC 4648 [14]) and represented as a String.  Format: base64 |  |

##### 6.1.6.3.3 Enumeration: SliceAuthNotificationType

The enumeration SliceAuthNotificationType represents the notification type of slice-specific authentication and authorization. It shall comply with the provisions defined in table 6.1.6.3.3-1.

Table 6.1.6.3.3-1: Enumeration SliceAuthNotificationType

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| SLICE\_RE\_AUTH | This value is used to indicate the re-authentication is needed |  |
| SLICE\_REVOCATION | This value is used to indicate the previous slice-specific authentication and authorization shall be revoked. |  |

#### 6.1.6.4 Data types describing alternative data types or combinations of data types

There is no alternative data types defined in this specification.

#### 6.1.6.5 Binary data

There is no binary data type defined in this specification.

### 6.1.7 Error Handling

#### 6.1.7.1 General

For the Nnssaaf\_NSSAA 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 Nnssaaf\_NSSAA API.

#### 6.1.7.2 Protocol Errors

No specific procedures for the Nnssaaf\_NSSAA service are specified.

#### 6.1.7.3 Application Errors

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

Table 6.1.7.3-1: Application errors

|  |  |  |
| --- | --- | --- |
| Application Error | HTTP status code | Description |
| RESOURCE\_TEMP\_MOVED | 307 Temporary Redirect | Indicates that the NSSAAF is not able to handle the request, but points to the URI of another NSSAAF. |
| RESOURCE\_MOVED | 308 Permanent Redirect | Indicates that the NSSAAF is not able to handle the request, but points to the URI of another NSSAAF. |
| SLICE\_AUTH\_REJECTED | 403 Forbidden | The user cannot be authenticated, e.g. authentication request rejected by the AAA-S. |
| CONTEXT\_NOT\_FOUND | 404 Not Found | The NSSAAF cannot find the resource corresponding to the URI provided by the NF Service Consumer, i.e. the resource identified by the authCtxId does not exist in the NSSAAF. |
| USER\_NOT\_FOUND | 404 Not Found | The user does not exist in the HPLMN. |
| UPSTREAM\_SERVER\_ERROR | 504 Gateway Timeout | Error happens in reaching the remote peer (i.e. the AAA-S). |
| NETWORK\_FAILURE | 504 Gateway Timeout | The request is rejected due to a network problem. |
| TIMED\_OUT\_REQUEST | 504 Gateway Timeout | No response is received from the remote peer (i.e. the AAA-S) when time out. |

## 6.1.8 Feature negotiation

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

Table 6.1.8-1: Supported Features

|  |  |  |
| --- | --- | --- |
| Feature number | Feature Name | Description |
|  |  |  |

## 6.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Nnssaaf\_NSSAA API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Nnssaaf\_NSSAA API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Nnssaaf\_NSSAA service.

The Nnssaaf\_NSSAA API defines a single scope "nnssaaf-nssaa" for the entire service, and it does not define any additional scopes at resource or operation level.

Annex A (normative):  
OpenAPI specification

## A.1 General

This Annex specifies the formal definition of the API(s) defined in the present specification. It consists of OpenAPI 3.0.0 specifications in YAML format.

This Annex takes precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API(s).

NOTE : The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification files contained in this 3GPP Technical Specification are available on a Git-based repository hosted, 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 Nnssaaf\_NSSAA API

openapi: 3.0.0

info:

title: Nnssaaf\_NSSAA

version: 1.0.5

description: |

Network Slice-Specific Authentication and Authorization Service.

© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

externalDocs:

description: 3GPP TS29.526, NSSAA Service, version 16.7.0.

url: https://www.3gpp.org/ftp/Specs/archive/29\_series/29.526/

servers:

- url: '{apiRoot}/nnssaaf-nssaa/v1'

variables:

apiRoot:

default: https://example.com

description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:

- {}

- oAuth2ClientCredentials:

- nnssaaf-nssaa

paths:

/slice-authentications:

post:

summary: Create slice authentication context

operationId: CreateSliceAuthenticationContext

tags:

- Slice Authentication Context Creation

requestBody:

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthInfo'

required: true

responses:

'201':

description: SliceAuthContext

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthContext'

headers:

Location:

description: 'Contains the URI of the newly created resource according to the structure: {apiRoot}/nnssaaf-nssaa/v1/slice-authentications/{authCtxId}'

required: true

schema:

type: string

'307':

$ref: 'TS29571\_CommonData.yaml#/components/responses/307'

'308':

$ref: 'TS29571\_CommonData.yaml#/components/responses/308'

'400':

description: Bad Request from the AMF

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

'403':

description: Forbidden due to slice authentication rejected

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

'404':

description: User does not exist

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

'504':

description: Network error or remote peer error

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

callbacks:

reauthenticationNotification:

'{request.body#/reauthNotifUri}':

post:

requestBody:

required: true

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthReauthNotification'

responses:

'204':

description: slice re-authentication notification response

'307':

description: Temporary Redirect

content:

application/json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/RedirectResponse'

headers:

Location:

description: 'The URI pointing to the resource located on the redirect target'

required: true

schema:

type: string

'308':

description: Permanent Redirect

content:

application/json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/RedirectResponse'

headers:

Location:

description: 'The URI pointing to the resource located on the redirect target'

required: true

schema:

type: string

'400':

$ref: 'TS29571\_CommonData.yaml#/components/responses/400'

'404':

$ref: 'TS29571\_CommonData.yaml#/components/responses/404'

'500':

$ref: 'TS29571\_CommonData.yaml#/components/responses/500'

'503':

$ref: 'TS29571\_CommonData.yaml#/components/responses/503'

default:

description: Unexpected error

revocationNotification:

'{request.body#/revocNotifUri}':

post:

requestBody:

required: true

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthRevocNotification'

responses:

'204':

description: slice revocation notification response

'307':

description: Temporary Redirect

content:

application/json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/RedirectResponse'

headers:

Location:

description: 'The URI pointing to the resource located on the redirect target'

required: true

schema:

type: string

'308':

description: Permanent Redirect

content:

application/json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/RedirectResponse'

headers:

Location:

description: 'The URI pointing to the resource located on the redirect target'

required: true

schema:

type: string

'400':

$ref: 'TS29571\_CommonData.yaml#/components/responses/400'

'404':

$ref: 'TS29571\_CommonData.yaml#/components/responses/404'

'500':

$ref: 'TS29571\_CommonData.yaml#/components/responses/500'

'503':

$ref: 'TS29571\_CommonData.yaml#/components/responses/503'

default:

description: Unexpected error

/slice-authentications/{authCtxId}:

put:

summary: Confirm the slice authentication result

operationId: ConfirmSliceAuthentication

tags:

- Confirm Slice Authentication

parameters:

- name: authCtxId

in: path

required: true

schema:

type: string

requestBody:

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthConfirmationData'

responses:

'200':

description: Request processed (EAP success or Failure)

content:

application/json:

schema:

$ref: '#/components/schemas/SliceAuthConfirmationResponse'

'307':

$ref: 'TS29571\_CommonData.yaml#/components/responses/307'

'308':

$ref: 'TS29571\_CommonData.yaml#/components/responses/308'

'400':

description: Bad Request

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

'500':

description: Internal Server Error

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

'504':

description: Network error or remote peer error

content:

application/problem+json:

schema:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/ProblemDetails'

components:

securitySchemes:

oAuth2ClientCredentials:

type: oauth2

flows:

clientCredentials:

tokenUrl: '{nrfApiRoot}/oauth2/token'

scopes:

nnssaaf-nssaa: Access to the nnssaaf-nssaa API

schemas:

#

# COMPLEX TYPES:

#

SliceAuthInfo:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapIdRsp:

$ref: '#/components/schemas/EapMessage'

amfInstanceId:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/NfInstanceId'

reauthNotifUri:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uri'

revocNotifUri:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uri'

required:

- gpsi

- snssai

- eapIdRsp

SliceAuthContext:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

authCtxId:

$ref: '#/components/schemas/SliceAuthCtxId'

eapMessage:

$ref: '#/components/schemas/EapMessage'

required:

- gpsi

- snssai

- authCtxId

- eapMessage

SliceAuthConfirmationData:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapMessage:

$ref: '#/components/schemas/EapMessage'

required:

- gpsi

- snssai

- eapMessage

SliceAuthConfirmationResponse:

type: object

properties:

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

eapMessage:

$ref: '#/components/schemas/EapMessage'

authResult:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/AuthStatus'

required:

- gpsi

- snssai

- eapMessage

SliceAuthReauthNotification:

type: object

properties:

notifType:

$ref: '#/components/schemas/SliceAuthNotificationType'

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

supi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Supi'

required:

- notifType

- gpsi

- snssai

SliceAuthRevocNotification:

type: object

properties:

notifType:

$ref: '#/components/schemas/SliceAuthNotificationType'

gpsi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Gpsi'

snssai:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Snssai'

supi:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Supi'

required:

- notifType

- gpsi

- snssai

#

# SIMPLE TYPES:

#

SliceAuthCtxId:

type: string

description: contains the resource ID of slice authentication context

nullable: false

SliceAuthNotificationType:

type: string

enum:

- SLICE\_RE\_AUTH

- SLICE\_REVOCATION

EapMessage:

type: string

format: base64

description: contains an EAP packet

nullable: true

Annex B (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-06 | CT4#98E | C4-203683 |  |  |  | TS skeleton. | 0.1.0 |
| 2020-06 | CT4#98E | C4-202084  C4-202085  C4-202086  C4-203709  C4-203710 |  |  |  | Implementation of pCRs agreed in CT4#98E | 0.2.0 |
| 2020-06 | CT#88e | CP-201193 |  |  |  | TS presented for information and approval. | 1.0.0 |
| 2020-06 | CT#88e |  |  |  |  | TS approved at CT#88e | 16.0.0 |
| 2020-09 | CT#89 | CP-202104 | 0005 | 1 | F | Update References | 16.1.0 |
| 2020-09 | CT#89 | CP-202104 | 0007 | 1 | F | Release PDU Session if NSSAA Re-Authentication and Re-Authorization Fails | 16.1.0 |
| 2020-09 | CT#89 | CP-202104 | 0008 | 1 | F | NSSAA status management | 16.1.0 |
| 2020-12 | CT#90 | CP-203054 | 0009 | 2 | F | Amendments for stateless NF support | 16.2.0 |
| 2020-12 | CT#90 | CP-203040 | 0010 | - | F | Remove Editor's Notes on AAA Server Address | 16.2.0 |
| 2020-12 | CT#90 | CP-203048 | 0011 | 1 | F | Storage of YAML files in 3GPP Forge | 16.2.0 |
| 2020-12 | CT#90 | CP-203040 | 0012 | 1 | F | AMF behaviour for NSSAA procedure due to temporal NW failure | 16.2.0 |
| 2020-12 | CT#90 | CP-203036 | 0013 | - | F | API version and External doc update | 16.2.0 |
| 2021-03 | CT#91 | CP-210049 | 0014 | - | F | Incorrect Media Type | 16.3.0 |
| 2021-03 | CT#91 | CP-210054 | 0016 | - | F | 29.526 Rel-16 API version and External doc update | 16.3.0 |
| 2021-06 | CT#92 | CP-211068 | 0017 | 1 | F | Rel-16 Unsuccessful cases for handling of NSSAA status in AMF | 16.4.0 |
| 2021-06 | CT#92 | CP-211068 | 0020 | 1 | F | Rel-16 SUPI in Notifications from NSSAAF | 16.4.0 |
| 2021-06 | CT#92 | CP-211059 | 0022 | 1 | F | Redirect Response | 16.4.0 |
| 2021-06 | CT#92 | CP-211073 | 0025 | - | F | 29.526 Rel-16 API version and External doc update | 16.4.0 |
| 2021-09 | CT#93 | CP-212070 | 0027 | 1 | F | NSSAA procedure from two different AMFs | 16.5.0 |
| 2021-09 | CT#93 | CP-212060 | 0030 | - | F | 3xx description correction for SCP | 16.5.0 |
| 2021-09 | CT#93 | CP-212080 | 0035 | - | F | 29.526 Rel-16 API version and External doc update | 16.5.0 |
| 2021-12 | CT#94 | CP-213139 | 0038 | 1 | F | Correction to Re-Authentication / Revocation Notification Procedure | 16.6.0 |
| 2021-12 | CT#94 | CP-213139 | 0040 | 1 | F | Remove AMF behaviour related to back-off timer from NSSAA procedure | 16.6.0 |
| 2022-03 | CT#95 | CP-220026 | 0052 | 1 | F | 3xx Redirect Response | 16.7.0 |
| 2022-03 | CT#95 | CP-220075 | 0056 | - | F | EAP ID Response message | 16.7.0 |
| 2022-03 | CT#95 | CP-220067 | 0059 | - | F | 29.526 Rel-16 API version and External doc update | 16.7.0 |