ETSI TS 129 526 V18.7.0 (2025-03)

5G;
5G System; Network Slice-Specific and SNPN Authentication and Authorization services; Stage 3
(3GPP TS 29.526 version 18.7.0 Release 18)

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

Reference
RTS/TSGC-0429526vi70

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 the
ETSI Search & Browse Standards application.

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 on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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 2025.
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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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

iTeh Standards
(https://standards.iteh.ai)
Document Preview

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.

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/sist/...ts-129-526-v18.7.0-2025-03

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/58aa0a44-38a2-4dd6-834d-a598b98b3ac2/etsi-ts-129-526-v18.7.0-2025-03

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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.

iTeh Standards (https://standards.iteh.ai) Document Preview
ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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 Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0.

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

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

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

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

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

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

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

[14] 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".

[17] 3GPP TS 29.536: "5G System; Network Slice Admission Control Services; Stage 3".

[18] 3GPP TS 29.509: "5G System; Authentication Server Services; Stage 3".

[19] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

iTeh Standards (https://standards.iteh.ai) Document Preview
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

3 Definitions, abbreviations

3.1 Definitions

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

3.2 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	Network Slice-specific and SNPN Authentication and Authorization Function
SNPN	Standalone Non-Public Network

4 Overview

4.1 Introduction

iTeh Standards
(https://standards.iteh.ai)
Document Preview

Within the 5GC, the NSSAAF offers services to the AMF and the AUSF 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).

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

The AUSF shall make use of the NSSAAF service when it needs to invoke a primary authentication in SNPN with Credentials holder using AAA server; the AUSF shall also make use of this service during the UE onboarding procedure in SNPN scenarios, when the Default Credentials Server (DCS) uses an AAA server for primary authentication.

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

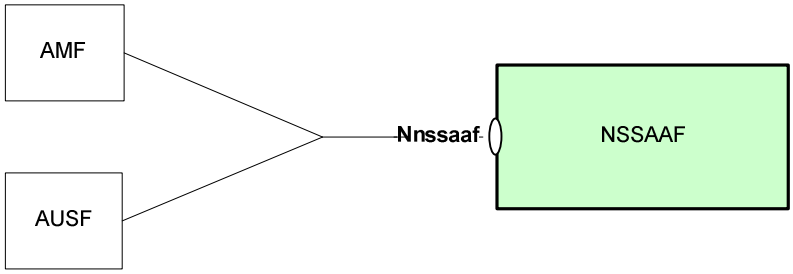

Figure 4.1-1: Reference model – NSSAAF

5 Services offered by the NSSAAF

5.1 Introduction

The NSSAAF offers the following services via the Nnssaaf interface:

- Nnssaaf_NSSAA Service
- Nnssaaf_AIW 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	TS29526_Nnssaaf_NSSAA.yaml	nnssaaf-nssaa	A.2
Nnssaaf_AIW	5.3	AAA Interworking service	TS29526_Nnssaaf_AIW.yaml	nnssaaf-aiw	A.3

5.2 Nnssaaf_NSSAA Service

5.2.1 Service Description

iTeh Standards (https://standards.iteh.ai) Document Preview

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_NSSAA 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.

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/sist/28ce0e4b-20e2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03

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. …/slice-authentications) to request the NSSAAF to create the corresponding resource context and perform slice-specific authentication and authorization.

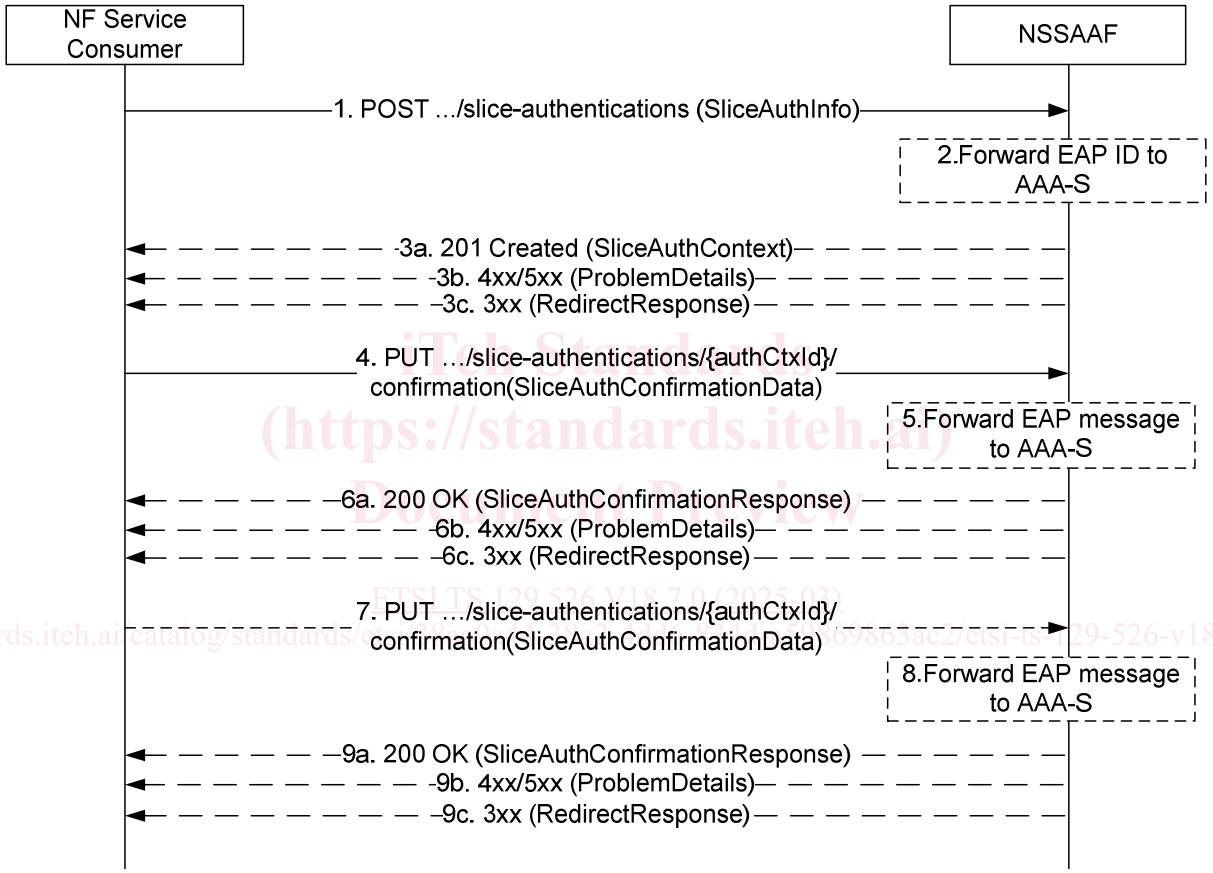

Figure 5.2.2.2.1-1: Slice-Specific Authentication and Authorization

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

   The HTTP content shall contain the slice authentication information, which includes:

   - UE ID (i.e. GPSI), if multiple GPSIs received from the UDM, the NF Service Consumer shall include any one of the GPSIs.

   - 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;

iTeh Standards (https://standards.iteh.ai) Document Preview
ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/...-ts-129-526-v18-7-0-2025-03

- 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. .../slice-authentications/{authCtxId}). The content 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. For a 4xx/5xx response, 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 content 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. …/slice-authentications/{authCtxId}).

The HTTP content shall carry the slice authentication confirmation data which includes:

- UE ID (i.e. GPSI)
- S-NSSAI
- 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 content 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. For a 4xx/5xx response, 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 content 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

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03
iTeh Standards
(https://standards.iteh.ai)
Document Preview

returned. For a 4xx/5xx response, 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.

If an S-NSSAI subject to the NSSAA is rejected due to Network Slice Admission Control as the total number of UEs exceeds the maximum number of UEs allowed to be registered to this slice as specified in clause 5.2.2.2.2 of 3GPP TS 29.536 [17]), the AMF shall keep the "status" attribute stored as not impacted (see clause 4.2.9.1 of 3GPP TS 23.502 [3] and 3GPP TS 29.518 [16]).

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.

ETSI TS 129 526 V18.7.0 (2025-03)
https://standards.iteh.ai/catalog/standards/etsi/38aa0a44-38a2-4dd6-834d-a59869863ac2/etsi-ts-129-526-v18-7-0-2025-03