ETSI TS 129 509 V15.8.0 (2022-07)

5G ;
5G System;
Authentication Server Services;
Stage 3
(3GPP TS 29.509 version 15.8.0 Release 15)

Reference
RTS/TSGC-0429509vf80

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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

Trademarks

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

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

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the stage 3 protocol and data model for the Nausf Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the AUSF.

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 33.501 [8].

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] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

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

[8] 3GPP TS 33.501: "Security Architecture and Procedures for 5G System".

[9] Void

[10] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

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

[12] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

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

[14] 3GPP TS 29.510: "Network Function Repository Services; Stage 3".

[15] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[16] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[17] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[18] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

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

[20] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[21] 3GPP TR 21.900: "Technical Specification Group working methods".

3 Definitions 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].

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].

AMF	Access and Mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
MAC	Message Authentication Code
NF	Network Function
SEAF	SEcurity Anchor Function
SoR	Steering of Roaming
URI	Uniform Resource Identifier
UPU	UE Parameters Update

4 Overview

4.1 Introduction

The Network Function (NF) Authentication Server Function (AUSF) is the network entity in the 5G Core Network (5GC) supporting the following functionalities:

- Authenticate the UE for the requester NF,
- Provide keying material to the requester NF,
- Protect the Steering Information List for the requester NF.

Figure 4-1 shows the reference architecture for the AUSF:

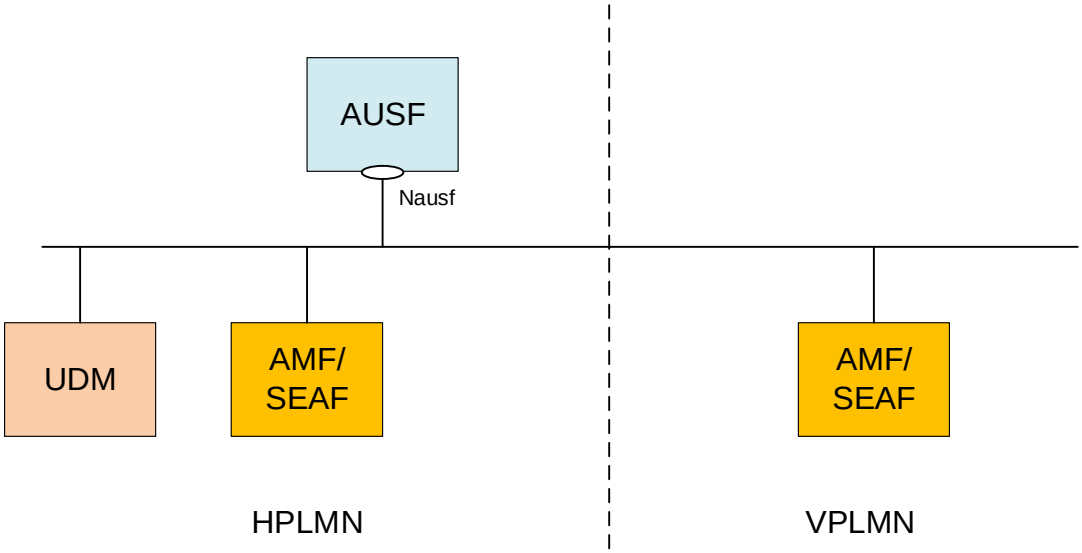

Figure 4-1: AUSF in 5G System architecture

This figure represents the AUSF architecture in the Service-based Architecture model. In the reference point model, the interface between the AMF and the AUSF is named N12. In this release, the SEAF function is collocated with the AMF. The AUSF may provide the service to the UDM.

5 Services offered by the AUSF

5.1 Introduction

The AUSF offers to NF Service Consumers (e.g. AMF) the following services:

- Nausf_UEAuthentication
- Nausf_SoRProtection
- Nausf_UPUProtection

5.2 Nausf_UEAuthentication Service

5.2.1 Service Description

The AUSF is acting as NF Service Producer. It provides UE authentication service to the requester NF. The NF Service Consumer is the AMF.

For this service, the following service operations are defined:

- Authenticate

This service permits to authenticate the UE and to provide one or more master keys which are used by the AMF to derived subsequent keys.

5.2.2 Service Operations

5.2.2.1 Introduction

The service operation defined for the Nausf_UEAuthentication is as follows:

- Authenticate: It allows the AMF to authenticate the UE.

5.2.2.2 Authenticate

5.2.2.2.1 General

The service operation "Authenticate" permits the requester NF to initiate the Authentication of the UE by providing the following information to the AUSF:

- UE id (e.g. SUPI)
- Serving Network Name

The AUSF retrieves the UE's subscribed authentication method from the UDM and depending on the information provided by the UDM, the AUSF enters in one of the following procedures:

- 5G-AKA
- EAP-based authentication'

For those two different procedures a new resource is generated by the AUSF. The content of the resource will depend on the procedure and will be returned to the AMF.

5.2.2.2.2 5G AKA

In this procedure, the NF Service Consumer (AMF) requests the authentication of the UE by providing UE related information and the serving network name and the 5G AKA is selected. The NF Service Consumer (AMF) shall then return to the AUSF the result received from the UE:

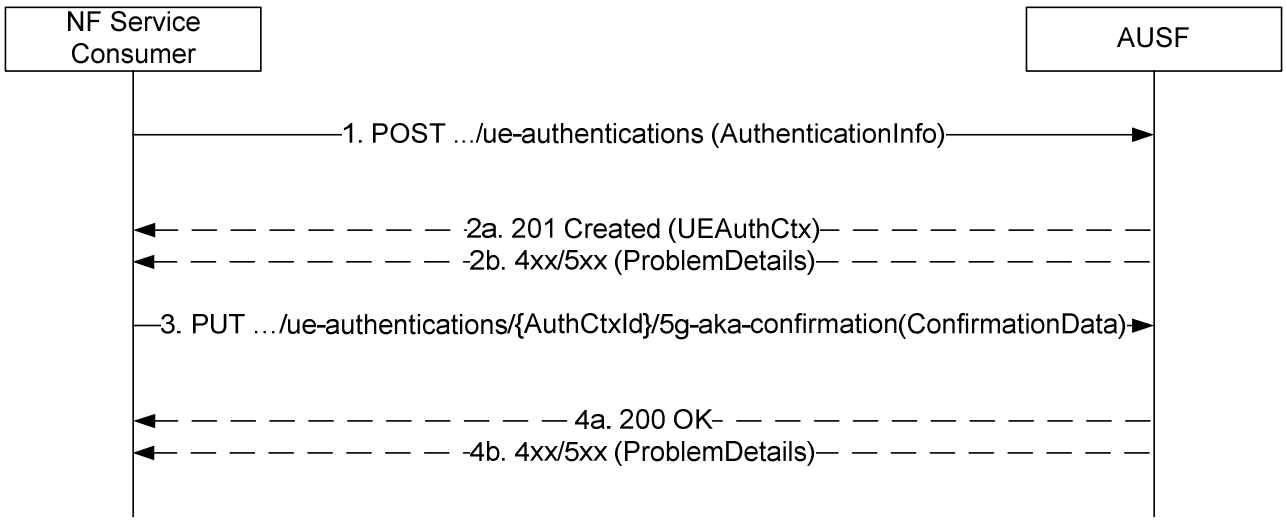

Figure 5.2.2.2.2-1: 5G AKA

1. The NF Service Consumer (AMF) shall send a POST request to the AUSF. The payload of the body shall contain at least the UE Id and the Serving Network Name.

2a. On success, "201 Created" shall be returned. The payload body shall contain the representation of the resource created and the "Location" header shall contain the URI of the created resource (e.g.

.../v1/ue_authentications/{authCtxId}). The AUSF generates a sub-resource "5g-aka-confirmation". The AUSF shall provide an hypermedia link towards this sub-resource in the payload to indicate to the AMF where it shall send a PUT for the confirmation.

2b. 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 serving network is not authorized, the AUSF shall use the SERVING_NETWORK_NOT_AUTHORIZED "cause".

3. Based on the relation type, the NF Service Consumer (AMF) deduces that it shall send a PUT containing the "RES*" provided by the UE to the URI provided by the AUSF or derived by itself. The NF Service Consumer (AMF) shall also send a PUT containing null value in the RES* to indicate the failure to the AUSF for the following cases:

   - if the UE is not reached, and the RES* is never received by the NF Service Consumer (AMF);
   - the comparation of the HRES* and HXRES* is unsuccessful in the NF Service Consumer (AMF);
   - the authentication failure is received from the UE, e.g. synchronization failure or MAC failure;

4a. On success, "200 OK" shall be returned. If the UE is not authenticated, e.g. the verification of the RES* was not successful in the AUSF, the AUSF shall set the value of AuthResult to AUTHENTICATION_FAILURE.

4b. 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.

5.2.2.2.3 EAP-based authentication method

5.2.2.2.3.1 General

In this procedure, the NF Service Consumer requests the authentication of the UE by providing UE related information and the serving network and the EAP-based authentication is selected (see IETF RFC 3748 [18]). EAP messages are exchanged between a UE acting as EAP peer, an NF Service Consumer (AMF/SEAF) acting as a pass-through authenticator and the AUSF acting as the EAP server.

5.2.2.2.3.2 EAP method: EAP-AKA'

EAP-AKA' is the EAP method used in this procedure

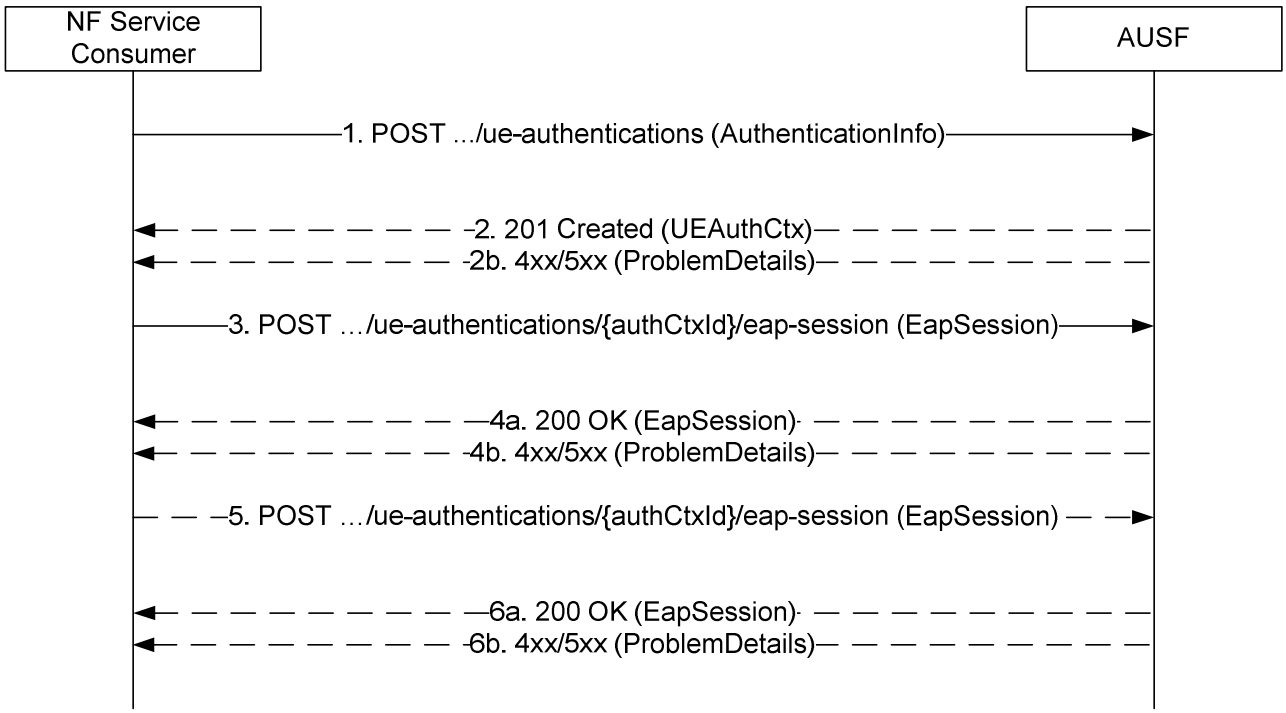

Figure 5.2.2.2.3-1: EAP-based authentication with EAP-AKA' method

1. The NF Service Consumer (AMF) shall send a POST request to the AUSF. The payload of the body shall contain at least the UE Id, Serving Network Name.

2a. On success, "201 Created" shall be returned. The payload body shall contain the representation of the resource generated and the "Location" header shall contain the URI of the generated resource (e.g. .../v1/ue_authentications/{authCtxId}/eap-session). The AUSF generates a sub-resource "eap-session". The AUSF shall provide an hypermedia link towards this sub-resource in the payload to indicate to the AMF where it shall send a POST containing the EAP packet response. The body payload shall also contain the EAP packet EAP-Request/AKA'-Challenge.

2b. 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. In particular, if the serving network is not authorized, the AUSF shall use the "Cause" SERVING_NETWORK_NOT_AUTHORIZED.

3. Based on the relation type, the NF Service Consumer (AMF) shall send a POST request including the EAP-Response/AKA' Challenge received from the UE. The POST request is sent to the URI provided by the AUSF or derived by the NF Service Consumer (AMF).

4a. On success, and if the AUSF and the UE have indicated the use of protected successful result indications as in IETF RFC 9048 [17], the AUSF shall reply with a "200 OK" HTTP message containing the EAP Request/AKA' Notification and an hypermedia link towards the sub-resource "eap-session".

4b. 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.

NOTE: Steps 4 to 5 are optional.

5. The NF Service Consumer (AMF) shall send a POST request including the EAP Response/AKA' Notification received from the UE. The POST request is sent to the URI provided by the AUSF or derived by the NF Service Consumser (AMF).

6a. If the EAP authentication exchange is successfully completed (with or without the optional Notification Request/Response messages exchange), "200 OK" shall be returned to the NF Service Consumer (AMF). The

payload shall contain the result of the authentication, an EAP success/failure and the Kseaf if the authentication is successful. If the UE is not authenticated, the AUSF shall set the authResult to AUTHENTICATION_FAILURE.

6b. 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.

5.2.2.2.3.3 EAP method: EAP-TLS

The EAP-TLS method can be used in private networks as an EAP method (see 3GPP TS 33.501 [8] Annex B.1). The corresponding stage 3 implementation is described in Annex B.

5.3 Nausf_SoRProtection Service

5.3.1 Service Description

The AUSF is acting as NF Service Producer. It provides SoRProtection service to the NF Service Consumer.

This service permits to provide the NF Service Consumer (e.g. UDM) with the SoR-MAC-IAUSF and CounterSoR to protect the the Steering Information List from being tampered with or removed by the VPLMN.

NOTE: If the Steering Information List is not available or HPLMN determines that no steering of the UE is required, a SOR transparent container information element with an HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE' protected by SoR-MAC-IAUSF and CounterSoR is still sent to the UE during registration. The Steering Information List In such a case, the NF Service Consumer shall send an empty list to the AUSF when consuming the Nausf_SoRProtection Service.

In option this service also allows to provide the NF Service Consumer (e.g. UDM) with the SoR-XMAC-IUE that allows the NF Service Consumer (e.g. UDM) to verify that the UE received the Steering Information List.

5.3.2 Service Operations

5.3.2.1 Introduction

The service operation defined for the Nausf_SoRProtection is as follows:

- Protect

5.3.2.2 Protect

5.3.2.2.1 General

The Protect service operation is used in the following procedures:

- Procedure for steering of UE in VPLMN during registration (see clause 6.14.2.1 of 3GPP TS 33.501 [8]);
- Procedure for steering of UE in VPLMN after registration (see clause 6.14.2.2 of 3GPP TS 33.501 [8]).

The NF Service Consumer (e.g. UDM) uses this service operation to request the AUSF to compute the SoR-MAC-IAUSF and the CounterSoR by providing Steering Information List. The NF Service Consumer (e.g. UDM) may also request the AUSF to compute the SoR-XMAC-IUE by providing the indication that an acknowledgement is requested from the UE.