

3GPP TS 33.501 V0.2.0 (2017-05)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System (Release 15)



The present document has been developed within the 3rd Generation Partnership Project (3GPPTM) and may be further elaborated for the purposes of 3GPP.. The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPPTM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Logos: Use exactly one of the above lines. Delete the others.

Use the top line for documents which are specific to GERAN technology only.

Use the second line for documents which are specific to UTRAN technology only or to GERAN and UTRAN technologies only.

*Use the third line for documents which relate to LTE technology (regardless of their applicability to GERAN or to UTRAN technologies) in Releases *prior to Release 10*.*

Keywords

<keyword[, keyword, ...]>

Use the fourth line for documents which relate to LTE technology (regardless of their applicability to GERAN or to UTRAN technologies) in Releases 10, 11 and 12.

Use the fifth line for documents which relate to LTE technology (regardless of their applicability to GERAN or to UTRAN technologies) in Release 13 onwards.

MCC selects keywords from stock list.

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.

© 2017, 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
Introduction	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations	6
3.1 Definitions	7
3.2 Symbols	7
3.3 Abbreviations.....	7
4 Overview of Security Architecture.....	7
5 Security Requirements and Features	7
5.1 Requirements on the UE	7
5.1.1 General	7
5.1.2 User data and signalling data confidentiality	7
5.1.2.1 Requirements on Support and Usage of Ciphering.....	7
5.1.3 User data and signalling data integrity	8
5.1.3.1 Requirements on Support and Usage of Integrity Protection	8
5.1.4 Secure storage and processing of subscription credentials.....	8
5.2 Requirements on the gNB.....	9
5.2.1 General	9
5.2.2 User data and signalling data confidentiality	9
5.2.2.1 Requirements on Support and Usage of Ciphering.....	9
5.2.3 User data and signalling data integrity	9
5.2.3.1 Requirements on Support and Usage of Integrity Protection	9
5.2.4 Requirements for gNB setup and configuration.....	9
5.2.5 Requirements for key management inside gNB	10
5.2.6 Requirements for handling User plane data for the gNB	10
5.2.7 Requirements for handling Control plane data for the gNB.....	10
5.2.8 Requirements for secure environment of the gNB	10
5.2.9 Requirements for gNB DU-CU interfaces	10
5.3 Requirements on the AMF.....	11
5.3.1 General	11
5.3.2 Signalling data confidentiality	11
5.3.2.1 Requirements on Support of Ciphering	11
5.3.3 Signalling data integrity	11
5.3.3.1 Requirements on Support of Integrity Protection	11
5.3 Visibility and configurability	11
5.3.1 Security indicators.....	11
5.3.2 Security configurability.....	11
6 Security Procedures between UE and 5G Core Network Functions	12
6.1 Primary authentication and key agreement.....	12
6.1.1 Authentication framework.....	12
6.1.1.1 General	12
6.1.1.2 EAP framework	12
6.1.1.3 Granularity of anchor key binding to serving network.....	12
6.1.2 Initiation of authentication	13
6.1.3 Authentication procedures.....	13
6.1.3.1 Authentication procedure for EAP-AKA'.....	13
6.1.3.2 Authentication procedure for EPS AKA*	15
6.1.4 Linking increased home control to subsequent procedures	17
6.1.4.1 Introduction	17
6.2 NAS security.....	17
6.3 Security negotiations.....	17
6.4 Security handling in state transitions	17

6.5	Security handling in mobility.....	17
6.6	Key hierarchy.....	17
6.7	Security contexts.....	18
6.7.1	General.....	18
6.7.2	Handling security contexts within the serving network.....	18
6.7.3	Distribution of security contexts.....	18
6.8	Subscriber identifier privacy.....	18
6.8.1	Subscriber permanent identifier.....	18
6.8.2	Subscriber temporary identifier.....	18
6.8.3	Subscriber identification procedure.....	18
7	Security Procedures between 5G Network Functions.....	18
7.1	Guidelines for protection of IP based interfaces.....	18
7.1.1	General.....	18
7.1.2	Implementation requirements.....	19
7.1.3	QoS considerations.....	19
7.2	Security procedures on N2.....	19
7.3	Security procedures on N3.....	19
7.4	Security messages over N12.....	19
7.5	Security messages over N13.....	20
7.6	Security procedures on N14.....	21
7.7	Security procedures on Xn.....	21
8	Security Procedures between UE and 5G Access Network Functions.....	21
8.1	Security negotiations.....	21
8.2	Security handling in state transitions.....	21
8.3	Security handling in mobility.....	21
8.4	Security handling in radio link failure.....	21
8.5	Dual Connectivity.....	21
9	Security of Interworking.....	21
10	Security Aspects of IMS Emergency Session Handling.....	21
11	Security for non-3GPP access to the 5G Core network.....	22
12	Security Procedures between UE and external data networks via the 5G Network.....	22
12.1	EAP based secondary authentication by an external DN-AAA server.....	22
12.1.1	General.....	22
12.1.2	Procedure.....	22
Annex A (normative): Key derivation functions.....		24
Annex B (informative): Using additional EAP methods for primary authentication.....		25
B.1	Introduction.....	25
B.2	Primary authentication and key agreement.....	25
B.2.1	Security Procedures with EAP TLS.....	25
B.3	Key derivation.....	25
Annex <X> (informative): Change history.....		25

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.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the 5G System and the 5G Core, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio.

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"
- [3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".
- [5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".
- [6] RFC 4301: "Security Architecture for the Internet Protocol".
- [7] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".
- [8] 3GPP TS 23.502: "Procedures for the 5G System"
- [9] 3GPP TS 33.102: "3G security; Security architecture"
- [10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture"
- [11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses"
- [12] IETF RFC 5488: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"
- [13] 3GPP TS 24.301: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"
- [x] <doctype> <#>[([up to and including][yyyy[-mm]]V<a[b[c]]>[onwards])]: "<Title>".

3 Definitions, symbols and abbreviations

Editor's Note: Delete from the above heading those words which are not applicable. Clause numbering depends on applicability and should be renumbered accordingly.

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].

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> <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].

<ACRONYM>	<Explanation>
5GC	5G Core Network
5G-AN	5G Access Network
5G-RAN	5G Radio Access Network
AMF	Access and Mobility Management Function
AMF	Authentication Management Field

NOTE: If it is not clear from the context, which meaning the acronym AMF has, it is spelled out.

IKE	Internet Key Exchange
NAS	Non Access Stratum
QoS	Quality of Service
SEG	Security Gateway
UE	User Equipment
UPF	User Plane Function

4 Overview of Security Architecture

5 Security Requirements and Features

5.1 Requirements on the UE

5.1.1 General

5.1.2 User data and signalling data confidentiality

5.1.2.1 Requirements on Support and Usage of Ciphering

The UE shall support ciphering of user data between the UE and gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

The UE may implement the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

Confidentiality protection of the user data between the UE and gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.1.3 User data and signalling data integrity

5.1.3.1 Requirements on Support and Usage of Integrity Protection

The UE shall support integrity protection of user data between the UE and the gNB.

The UE shall support integrity protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

The UE may implement the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

Integrity protection of the user data between the UE and gNB is optional to use.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

Editor's note: The list of exceptions is FFS.

5.1.4 Secure storage and processing of subscription credentials

The following requirements apply for the storage and processing of the subscription credentials used to access the 5G network:

- The subscription credential(s) shall be integrity protected within the NG-UE using a tamper resistant secure hardware component.
- The long-term key(s) of the subscription credential(s) (e.g., K in EPS AKA) shall be confidentiality protected within the NG-UE using a tamper resistant secure hardware component.
- The long-term key(s) of the subscription credential(s) shall never be available in the clear outside of the tamper resistant secure hardware component.
- The authentication algorithm(s) that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.
- It shall be possible to perform a security evaluation / assessment according to the respective security requirements of the tamper resistant secure hardware component.

Editor's Note: It is FFS whether such a security assurance scheme to be used for evaluation of the credentials and identifier storage and processing is within the scope of 3GPP and if so, the requirements related to it.

Editor's note: The above requirements need to be updated with the agreed terminology for e.g. long-term key.

5.2 Requirements on the gNB

5.2.1 General

The security requirements given in this section apply to all types of gNBs. More stringent requirements for specific types of gNBs may be defined in other 3GPP specifications.

Editor's Note: The content may need to be updated after RAN decisions on split deployments of the gNB.

5.2.2 User data and signalling data confidentiality

5.2.2.1 Requirements on Support and Usage of Ciphering

The gNB shall support ciphering of user data between the UE and the gNB.

The gNB shall support ciphering of RRC-signalling.

The gNB shall implement the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

The gNB may implement the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

Confidentiality protection of user data between the UE and gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.2.3 User data and signalling data integrity

5.2.3.1 Requirements on Support and Usage of Integrity Protection

The gNB shall support integrity protection of user data between the UE and the gNB.

The gNB shall support integrity protection of RRC-signalling.

The gNB shall implement the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

The gNB may implement the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

Integrity protection of the user data between the UE and gNB is optional to use.

Integrity protection of the RRC-signalling and NAS-signalling is mandatory to use, except in the following cases:

Editor's note: The list of exceptions is FFS.

5.2.4 Requirements for gNB setup and configuration

Editor's Note: This clause will include the requirement on the gNB setup and configuration based on TS 33.401.

5.2.5 Requirements for key management inside gNB

The 5GC provides subscription specific session keying material for the gNBs, which also hold long term keys used for authentication and security association setup purposes. Protecting all these keys is important.

1. Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment except when done in accordance with this or other 3GPP specifications.

5.2.6 Requirements for handling User plane data for the gNB

Editor's Note: Backhaul and sidehaul security requirements are FFS

1. Any part of a gNB deployment that stores or processes user plane data in cleartext shall be protected from physical attacks. If not the whole entity is placed in a physically secure location, then user plane data in cleartext shall be stored and processed in a secure environment.

5.2.7 Requirements for handling Control plane data for the gNB

Editor's Note: Backhaul and sidehaul security requirements are FFS

1. Any part of a gNB deployment that stores or processes control plane data in cleartext shall be protected from physical attacks. If not the whole entity is placed in a physically secure location, then control plane data in cleartext shall be stored and processed in a secure environment.

5.2.8 Requirements for secure environment of the gNB

Editor's Note: The definition and the usage of the secure environment is FFS.

The secure environment is logically defined within the gNB and is a composition of functions for the support of sensitive operations.

1. The secure environment shall support secure storage of sensitive data, e.g. long term cryptographic secrets and vital configuration data.
2. The secure environment shall support the execution of sensitive functions, e.g. en-/decryption of user data and the basic steps within protocols which use long term secrets (e.g. in authentication protocols).
3. Sensitive data used within the secure environment shall not be exposed to external entities.
4. The secure environment shall support the execution of sensitive parts of the boot process.
5. The secure environment's integrity shall be assured.
6. Only authorised access shall be granted to the secure environment, i.e. to data stored and used within, and to functions executed within.

5.2.9 Requirements for gNB DU-CU interfaces

1. Due to split deployments, signalling traffic or user plane data may be sent on gNB-internal interfaces. Signalling traffic sent on gNB-internal interfaces shall be integrity, confidentiality and anti-replay protected.
2. User plane data sent on gNB-internal interfaces shall be confidentiality protected.

5.3 Requirements on the AMF

5.3.1 General

5.3.2 Signalling data confidentiality

5.3.2.1 Requirements on Support of Ciphering

The AMF shall support ciphering of NAS-signalling.

The AMF shall support the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

The AMF may support the following ciphering algorithms:

Editor's note: The list of supported ciphering algorithms is FFS.

Confidentiality protection of the RRC-signalling and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.3.3 Signalling data integrity

5.3.3.1 Requirements on Support of Integrity Protection

The AMF shall support integrity protection of NAS-signalling.

The AMF shall support the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

The AMF may support the following integrity protection algorithms:

Editor's note: The list of supported integrity protection algorithms is FFS.

Integrity protection of the user data between the UE and gNB is optional to use.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

Editor's note: The list of exceptions is FFS.

5.3 Visibility and configurability

5.3.1 Security indicators

5.3.2 Security configurability

...

6 Security Procedures between UE and 5G Core Network Functions

6.1 Primary authentication and key agreement

6.1.1 Authentication framework

6.1.1.1 General

The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key provided by the AUSF to the SEAF.

Keys for more than one security context can be derived from the anchor key without the need of a new authentication run. As a concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

In addition, the 5G security architecture also supports the feature that an authentication run also may result in a key left at the AUSF based on the home operator's policy on using such a key.

NOTE: This feature is an optimization that may be useful, for example, when a UE registers to different serving networks for 3GPP-defined access and untrusted non-3GPP access. (This is possible according to TS 23.501 [2].)

NOTE: In the present release, EAP-AKA' and EPS AKA* are the only authentication methods that are mandatory to support in UE and serving network, hence only they are described in clause 6.1.3. An example of how additional authentication methods can be used with the EAP framework is given in the informative Annex B.

Editor's note: EPS AKA* refers to variants of EPS AKA that is being discussed for use over 5G (see TR 33 899 for one variant of it) – it may be renamed to a more 5G sounding name.

6.1.1.2 EAP framework

Editor's Note: This clause is meant to explain what support for the EAP framework means for the various functional entities in the 5G system.

6.1.1.3 Granularity of anchor key binding to serving network

The primary authentication and key agreement procedures support the binding of the anchor key to the serving network. This prevents one serving network from claiming to be a different serving network, and thus provides implicit serving network authentication to the UE.

Furthermore, the anchor key provided to the serving network is also specific to the authentication having taken place between the UE and a 5G core network, i.e. the anchor key is cryptographically separate from the key delivered from the home network to the serving network in earlier mobile network generations.

Editor's Note: The exact inputs used to bind the key provided to the serving network are FFS

Editor's Note: This is a new topic that has not been raised so far, but is essential to address in phase 1. It is about binding the anchor key to an identity of the serving network. This should be done in a uniform way for 3GPP access and non-3GPP access. It is ffs, which input should be used for the anchor key derivation to achieve the uniform binding. Candidates for input parameters are (a combination of): VPLMN-Id (as in 3GPP access to 4G), access network type (e.g. the string "WLAN", as in non-3GPP access to 4G), the string "5G" to distinguish anchor keys for 4G (i.e. KASME) from those for 5G.

6.1.2 Initiation of authentication

The SEAF may initiate an authentication with the UE at any time, according to the SEAF's policy.

The SEAF shall send an Authentication Initiation Request (5G-AIR) to the AUSF whenever the SEAF wishes to initiate an authentication with the UE with the following exception:

- The SEAF does not need to send a 5G-AIR if it has an authentication vector for EPS AKA* available and wishes to initiate an authentication with the UE over 3GPP access.

Editor's Note: It is ffs whether more than one authentication vector is allowed to be sent to the SEAF at a time.

NOTE: In EPS, the acronym AIR stands for Authentication Information Request.

The 5G-AIR shall contain a subscriber identifier, from which the AUSF can derive the UE's subscriber permanent identifier (SUPI), as defined in TS 23.501 [2].

Editor's Note: Depending on the decisions on security area #7 in TR 33.899, the subscriber identifier contained in the 5G-AIR may be a concealed SUPI, e.g. in the form of a pseudonym or a public-key encrypted SUPI. Furthermore, the subscriber identifier may be in the form of a NAI, depending on the decisions in SA2, CT1, and CT4. It is also ffs how the AUSF can determine whether the SUPI is in cleartext or in concealed form.

The 5G-AIR shall furthermore contain an indication of whether the authentication is meant for 3GPP access or non-3GPP access. The 5G-AIR shall also contain the serving network name, as defined in clause 6.1.1.3.

Upon receiving the 5G-AIR, the AUSF shall determine the SUPI from the subscriber identifier in the 5G-AIR and select the authentication method based on local policy.

NOTE: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs. The AUSF is limited in selecting the authentication methods in as far as EPS AKA* can only be selected for 3GPP access.

After selecting the authentication method, the AUSF starts the authentication procedure for the selected method, according to clause 6.1.3.

6.1.3 Authentication procedures

6.1.3.1 Authentication procedure for EAP-AKA'

EAP-AKA' is specified in RFC 5448 [12].

EAP-AKA' is applied within the 5G authentication framework as follows, cf. also Fig. 6.1.3.1-1:

A pre-condition is that the AUSF has received a 5G-AIR from the SEAF, cf. clause 6.1.2, and has selected EAP-AKA' as the authentication method.

Then the AUSF checks that the requesting SEAF in the serving network is entitled to use the serving network name received in the 5G-AIR.

The AUSF requests one or more authentication vectors (AVs) from the ARPF in an AV-Req including the serving network name and an indication that the authentication vector is for EAP-AKA'. The ARPF generates an authentication vector with AMF separation bit = 1, where AMF = Authentication Management Field as defined in TS 33.102 [9]. The ARPF then transforms this authentication vector into a new authentication vector by computing CK' and IK' as per the Normative Annex x with the value of <serving network name> being one of the input parameters, and replacing CK and IK by CK' and IK'. The ARPF then sends this transformed authentication vector to the AUSF in an AV-Resp. The choice of the value of <serving network name> shall follow the rules set in clause 6.1.1.3 on "Granularity of anchor key binding to serving network".

NOTE: The exchange of an AV-Req and an AV-Resp between AUSF and ARPF described in the preceding paragraph is the same as for trusted access using EAP-AKA' described in TS 33.402 [11], clause 6.2, step 10, except for the input parameter to the key derivation, which is the value of <network name>. "network name" is a concept from RFC 5448 [12]; it is carried in the AT_KDF_INPUT attribute in EAP-AKA'. The value of <network name> is defined not in RFC 5448 [12], but in 3GPP specifications. For EPS, it is defined in TS 24.302 [13] and is called "access network identity", while, for 5G, it is defined in clause 6.1.1.3 of the present specification and in TS 24.yyy [xx], with a re-direction from TS 24.302 [13] to TS 24.yyy, and is called "serving network name".

Editor's Note: The content of clause 6.1.1.3 is ffs. The number of the stage 3 specification TS 24.yyy [xx] is ffs.

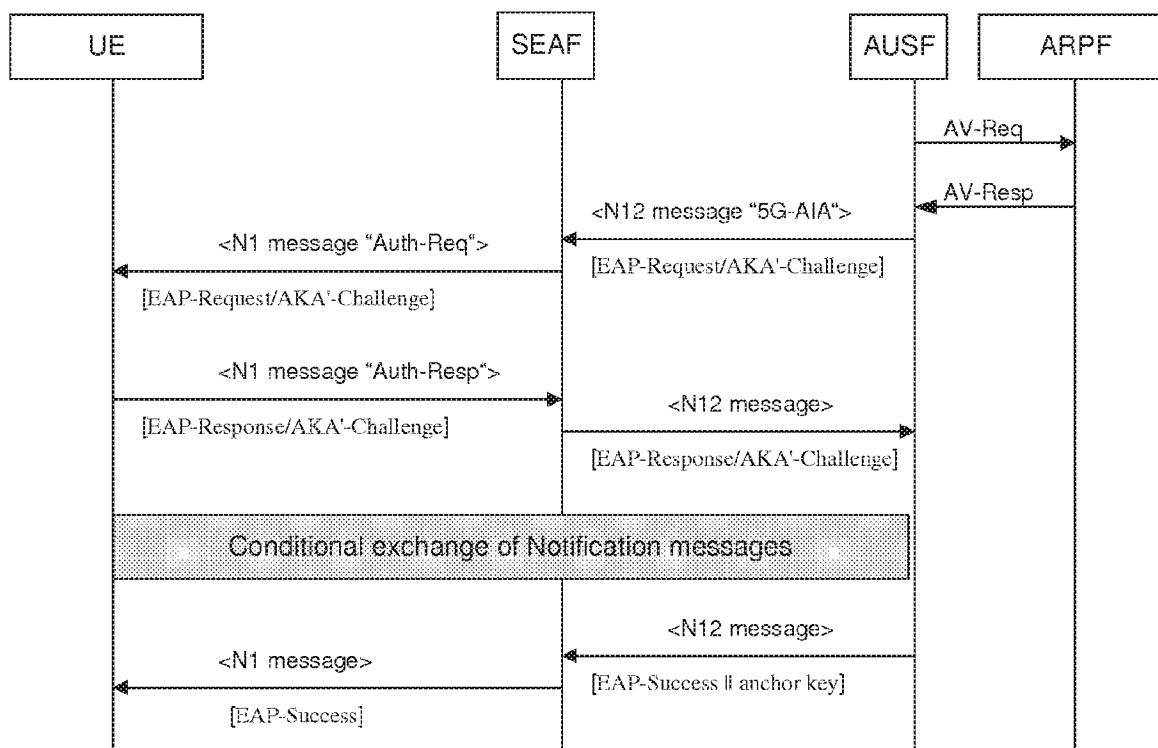


Fig. 6.1.3.1-1 Authentication procedure for EAP-AKA'

The AUSF and the UE then proceed as described in RFC 5448 [12].

The AUSF sends the EAP-Request/AKA'-Challenge message to the SEAF in a 5G Authentication Initiation Answer (5G-AIA) message over N12. The SEAF understands from the 5G-AIA that the authentication method used is an EAP method.

The SEAF transparently forwards the EAP-Request/AKA'-Challenge to the UE in a NAS message Auth-Req.

The UE sends the EAP-Response/AKA'-Challenge to the SEAF in a NAS message Auth-Resp.

The SEAF transparently forwards the EAP-Response/AKA'-Challenge to the AUSF in a message over N12. If the AUSF has successfully verified this message it continues as follows:

The AUSF and the UE conditionally exchange EAP-Request/AKA'-Notification and EAP-Response/AKA'-Notification messages, that are transparently forwarded by the SEAF.

The AUSF sends an EAP Success message to the SEAF, which forwards it transparently to the UE. The EAP Success message is contained in a message over N12 that also contains the anchor key, as computed in RFC 5448 [12].

The key received in the N12 message shall become the anchor key in the sense of the key hierarchy in clause 6.6.

The further steps taken by the AUSF upon receiving a successfully verified EAP-Response/AKA'-Challenge message are described in clause 6.1.4.

If the EAP-Response/AKA'-Challenge message is not successfully verified the AUSF acts according to the home network's policy.

Editor's Note: Error cases are typically handled in stage 3 specifications and should be elaborated jointly by SA3 and CT4.

Editor's Note: Steps in figure and text should be numbered.

Editor's Note: It is ffs whether the anchor key is the MSK or a key derived from the EMSK.

6.1.3.2 Authentication procedure for EPS AKA*

EPS AKA* enhances EPS AKA, as defined in TS 33.401 [10] with providing an Authentication Confirmation message from the visited network to the home network that confirms successful authentication of the UE such that the message cannot be spoofed by the visited network with a reasonable probability. The solution leaves the authentication exchange between the UE and the visited network unchanged, compared to using EPS AKA (except for the means to transport authentication messages over N1 and a modified authentication response).

EPS AKA* is applied within the 5G authentication framework as follows, cf. also Fig. 6.1.3.2-1:

When the AUSF has received a 5G-AIR from the SEAF, cf. clause 6.1.2, and has selected EPS AKA* as the authentication method, the AUSF checks that the requesting SEAF in the serving network is entitled to use the serving network name received in the 5G-AIR.

The AUSF requests one or more authentication vectors (AVs) from the ARPF in an AV-Req including the serving network name and an indication that the authentication vector is for EPS AKA*. The ARPF generates an authentication vector according to TS 33.401 [10] with AMF separation bit = 1, where AMF = Authentication Management Field as defined in TS 33.102 [9]. The ARPF then transforms the authentication vector into a new authentication vector by replacing KASME with KASME* and XRES with XRES*.

KASME* is computed as per the Normative Annex A with CK, IK, $SQN \oplus AK$, and the value of < serving network name> being the input parameters. The choice of the value of < serving network name> shall follow the rules set in clause 6.1.1.3 on "Granularity of anchor key binding to serving network".

Editor's Note: It is ffs whether the outcome of the discussion on the granularity of serving network authentication, cf. clause 6.1.1.3, will result in the computation of a KASME* different from KASME as computed in EPS.

XRES* is computed as per the Normative Annex x with CK, IK, RES, RAND, and the value of < serving network name> being the input parameters. XRES* shall have a length of 128 bits.

The ARPF then returns the requested number of transformed AVs to the AUSF in an AV-Resp.

The AUSF stores XRES* temporarily until a protocol timer expires.

Editor's Note: The protocol timer is to be defined by CT4.

The AUSF then generates HXRES* from XRES* by computing

$HXRES* = \text{SHA-256}(XRES* \parallel \text{RAND})$, truncated to 128 bits.

Editor's Note: It is ffs whether HXRES* should be computed in the ARPF.

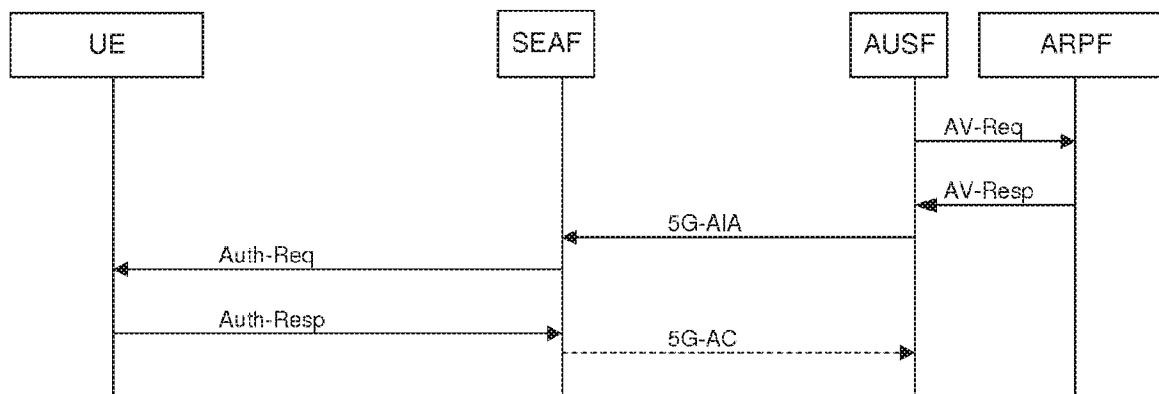


Fig. 6.1.3.2-1 Authentication procedure for EPS AKA*

The AUSF then returns one or more authentication vectors AV* to the SEAF in a 5G Authentication Initiation Answer (5G-AIA). The only difference between AV* and the transformed AV received from the ARPF is that AV* contains HXRES* while the transformed AV contains XRES*.

The SEAF understands from the 5G-AIA that the authentication method used is EPS AKA* and that the included authentication vector is of type AV*, not AV.

Editor's Note: It is to be defined by CT4 how the SEAF can learn this from the 5G-AIA.

Furthermore, the AUSF tells the SEAF whether a confirmation message is required.

NOTE 1: The AUSF may have a policy to always require a confirmation message, or adopt a more fine-grained policy depending on the trust in the roaming partner. The AUSF may learn from a database of roaming partners whether a confirmation message is required.

Editor's Note: It is whether the AUSF should also include the value of the timer in the message to the SEAF if the AUSF requires a confirmation message so that the SEAF can know within which period it has to use the received authentication vector.

If the AUSF requests a confirmation message from the SEAF then the AUSF shall send only one authentication vector AV* to the SEAF at a time.

The SEAF sends RAND, AUTN to the UE, as described for EPS AKA in TS 33.401 [10], in a NAS message Auth-Req. The USIM returns RES, CK, IK to the ME, as described for EPS AKA in TS 33.401 [10]. The ME then computes RES* from RES in the same way as the ARPF computed XRES* from XRES and returns RES* to the SEAF in a NAS message Auth-Resp.

The SEAF then computes HRES* from RES* in the same way as the AUSF computed HXRES* from XRES* and compares HRES* and HXRES*. If they coincide the SEAF considers the authentication successful. If not the SEAF rejects the authentication.

If the authentication was successful, the key KASME* received in AV* shall become the anchor key in the sense of the key hierarchy in clause 6.6.

If the authentication was successful, and if a confirmation message is required, the SEAF sends RES*, as received from the UE, in a newly defined 5G Authentication Confirmation (5G-AC) message (containing the subscriber identifier and the serving network name) to the AUSF.

When the 5G-AC message was received in response to an 5G-AIA and was received before the protocol timer above has expired the AUSF compares the received RES* with the stored XRES*. If they coincide the AUSF considers the confirmation message as successfully verified.

The further steps taken by the AUSF upon receiving a successfully verified confirmation message are described in clause 6.1.4.

If the confirmation message is not successfully verified the AUSF acts according to the home network's policy.

Editor's Note: Error cases are typically handled in stage 3 specifications and should be elaborated jointly by SA3 and CT4. It is ffs whether the AUSF sends a Cancel Location message, with suitable cause values, if the subscriber had already been registered and either the timer was up or the received RES* was incorrect.

Editor's Note: It is ffs how this authentication method can leave a key at the AUSF after authentication.

Editor's Note: The use of normative language needs to be checked.

Editor's Note: It is ffs whether the RES* could optionally be computed on the USIM.

6.1.4 Linking increased home control to subsequent procedures

6.1.4.1 Introduction

The authentication and key agreement protocols mandated to support in the present release all provide increased home control, compared to EPS AKA in 4G. This increased home control comes in the following forms in 5G:

- In the case of EAP-AKA', the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the EAP-Response/AKA'-Challenge received by the AUSF has been successfully verified, cf. clause 6.1.3.1.
- In the case of EPS AKA*, the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the Authentication Confirmation message received by the AUSF has been successfully verified, cf. clause 6.1.3.2.

The feature of increased home control is useful in preventing certain types of fraud, e.g. fraudulent Update Location request for subscribers that are not actually present in the visited network. But an authentication protocol by itself cannot provide protection against such fraud. The authentication result needs to be linked to subsequent procedures, e.g. the location update procedure in some way to achieve the desired protection.

The actions taken by a home network to link authentication confirmation (or the lack thereof) to subsequent procedures are subject to operator policy and are not standardized.

6.2 NAS security

Editor's Note: This clause is meant to contain, among other things, contents corresponding to 33.401 [10], clause 8 "Security mechanisms for non-access stratum signalling and data via MME" and clause 6.5 "Handling of NAS COUNTs".

6.3 Security negotiations

6.4 Security handling in state transitions

6.5 Security handling in mobility

6.6 Key hierarchy

Editor's Note: This clause is meant to contain an overall description of all the keys in the 5G key hierarchy, also comprising keys shared between UE and access network that are defined only below in clause 8.

6.7 Security contexts

6.7.1 General

Editor's Note: 33.401 contains an elaborate set of definitions of different levels of security contexts. These definitions may be further explained here. If the definitions in clause 3 are sufficient, this subclause may be quite short.

6.7.2 Handling security contexts within the serving network

Editor's Note: The content of this clause is meant to correspond to 33.401, clause 6.4, which is about handling security contexts at certain events like removal of the UICC, new authentication, state transitions, and about the respective roles of MME and UICC in handling security contexts.

6.7.3 Distribution of security contexts

Editor's Note: The content of this clause is meant to correspond to 33.401, clauses 6.1.4, 6.1.5, 6.1.6, which are about distributing security contexts in and between security domains.

6.8 Subscriber identifier privacy

Editor's Note: The content of this clause depends on the decisions on security area #7 in TR 33.899.

6.8.1 Subscriber permanent identifier

6.8.2 Subscriber temporary identifier

NOTE: This subclause is about the temporary subscription identifier shared between UE and core network. RAN level identifiers are handled in clause 7.

6.8.3 Subscriber identification procedure

Editor's Note: The content of this clause is meant to correspond to 33.401, clause 6.1.3, which is about the Identity request/response procedure between serving network and UE invoked in case the SN is unable to resolve the temporary identifier.

7 Security Procedures between 5G Network Functions

7.1 Guidelines for protection of IP based interfaces

7.1.1 General

Editor's Note: Whether to include management interfaces here is FFS.

Editor's Note: The security of the FI interface is FFS.

The protection of IP based interfaces for 5GC and 5G-AN shall be done according to NDS/IP as specified in TS 33.210 [3]. Traffic on interfaces carrying control plane signalling shall be integrity protected according to NDS/IP. In addition to the mandatory integrity protection, traffic carrying subscriber specific sensitive data, e.g. cryptographic keys, shall be also confidentiality protected according to NDS/IP.

NOTE 1: According to TS 33.210 [3] and TS 33.310 [5], in case control plane interfaces are trusted (e.g. physically protected), there is no need to use protection.

7.1.2 Implementation requirements

Whenever IPsec ESP is required, then it shall be implemented according to RFC 4303 [4] as profiled by TS 33.210 [3]. For IPsec implementation, tunnel mode is mandatory to implement while transport mode is optional.

Editor's Note: Whether IPsec support is mandatory or optional for 5G CN entities is FFS.

Whenever IKEv2 certificates based authentication is required, then it shall be implemented according to TS 33.310 [5]. The certificates shall be implemented according to the profile described by TS 33.310 [5]. IKEv2 shall be implemented conforming to the IKEv2 profile described in TS 33.310 [5].

7.1.3 QoS considerations

If the sender of IPsec traffic uses DiffServ Code Points (DSCPs) to distinguish different QoS classes, either by copying DSCP from the inner IP header or directly setting the encapsulating IP header's DSCP, the resulting traffic may be reordered to the point where the receiving node's anti-replay check discards the packet. If different DSCPs are used on the encapsulating IP header, then to avoid packet discard under one IKE SA and with the same set of traffic selectors, distinct Child-SAs should be established for each of the traffic classes (using the DSCPs as classifiers) as specified in RFC 4301 [6].

Editor's Note: This might need to be revised depending on the progress on the QoS architecture in other working groups.

7.2 Security procedures on N2

Editor's Note: includes equivalent of S1-MME messages, like key transport to base station, as well as message protection, i.e. backhaul link security.

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates based authentication as specified in clause 7.1.2. IPsec is mandatory to implement on the gNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

Editor's Note: The implementation requirement on the 5G-RAN side in general and the gNB in particular is FFS.

7.3 Security procedures on N3

N3 is the reference point between the 5G-AN and UPF. It is used to carry user plane data from the UE to the UPF.

In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificates based authentication as specified in clause 7.1.2 with confidentiality, integrity and replay protection. IPsec is mandatory to implement on the gNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

Editor's Note: The implementation requirement on the 5G-RAN side in general and the gNB in particular is FFS.

QoS related aspects are further described in clause 7.1.3.

7.4 Security messages over N12

This subclause lists the security-related messages that are run over the N12 interface between the AMF and the AUSF. The N12 interface is defined in TS 23.501 [2].

In the present release of this specification, the AMF is co-located with the SEAF.

The messages listed here are used in procedures that are described in clause 6.

NOTE: The names of messages used here are specific to the present specification and may be different in other 3GPP specifications.

*List of messages:***Authentication Initiation Request (5G-AIR):**

This message sent from SEAF to AUSF is described in clause 6.1.2 of the present specification. The content of this message is independent of any authentication method.

5G Authentication Initiation Answer (5G-AIA):

This message sent from AUSF to SEAF is described in clause 6.1.3 of the present specification. This message contains the first authentication message sent by the AUSF. The content of this message is hence dependent on the authentication method selected by the AUSF.

For EAP-AKA', this message contains the EAP-Request/AKA'-Challenge, as described in clause 6.1.3.1.

For EPS AKA*, this message contains the EPS AKA* authentication vector(s), as described in clause 6.1.3.2.

EAP-AKA' challenge response:

This message sent from SEAF to AUSF is described in clause 6.1.3.1 of the present specification. It contains the EAP-Response/AKA'-Challenge.

EAP-AKA' Notification request:

This conditional message sent from AUSF to SEAF is described in clause 6.1.3.1 of the present specification. It contains the EAP-Request/AKA'-Notification.

EAP-AKA' Notification response:

This conditional message sent from SEAF to AUSF is described in clause 6.1.3.1 of the present specification. It contains the EAP-Response/AKA'-Notification.

EAP-AKA' Success:

This message sent from AUSF to SEAF is described in clause 6.1.3.1 of the present specification. It contains the EAP-Success message. It also contains the anchor key.

5G Authentication Confirmation (5G-AC) message:

This message sent from SEAF to AUSF is described in clause 6.1.3.2 of the present specification

Editor's Note: messages relating to sequence number synchronisation failures need to be taken into account.

7.5 Security messages over N13

This subclause lists the security-related messages that are run over the N13 interface between the AUSF and the ARPF inside the UDM. The N13 interface is defined in TS 23.501 [2].

The messages listed here are used in procedures that are described in clause 6.

NOTE: The names of messages used here are specific to the present specification and may be different in other 3GPP specifications.

*List of messages:***Authentication Vector Request (AV-Req):**

This message sent from AUSF to ARPF is described in clause 6.1.3 of the present specification. For EAP-AKA', the description of the content of AV-Req can be found in clause 6.1.3.1. For EPS AKA*, the description of the content of AV-Req can be found in clause 6.1.3.2.

Authentication Vector Response (AV-Resp):

This message sent from ARPF to AUSF is described in clause 6.1.3 of the present specification. For EAP-AKA', the description of the content of AV-Resp can be found in clause 6.1.3.1. For EPS AKA*, the description of the content of AV-Resp can be found in clause 6.1.3.2.

Editor's Note: messages relating to sequence number synchronisation failures need to be taken into account

7.6 Security procedures on N14

7.7 Security procedures on Xn

Xn is the interface connecting 5G-RAN nodes. It is used to carry signalling and user plane data.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificates based authentication as specified in clause 7.1.2 with confidentiality, integrity and replay protection.

QoS related aspects are further described in clause 7.1.3.

8 Security Procedures between UE and 5G Access Network Functions

8.1 Security negotiations

8.2 Security handling in state transitions

8.3 Security handling in mobility

8.4 Security handling in radio link failure

8.5 Dual Connectivity

Editor's note: more subheadings from 33.401 clause 7 or 33.899 sec are all 4?

9 Security of Interworking

Editor's Note: This clause covers security of interworking with LTE systems

10 Security Aspects of IMS Emergency Session Handling

Editor's Note: This clause covers emergency session aspects.

11 Security for non-3GPP access to the 5G Core network

Editor's Note: This clause covers untrusted non-3GPP access.

12 Security Procedures between UE and external data networks via the 5G Network

Editor's Note: This clause covers, e.g. secondary authentication.12.1 EAP based secondary authentication by an external DN-AAA server

12.1.1 General

This clause specifies support for optional-to-use secondary authentication between the UE and an external data network (DN).

EAP shall be used for authentication between the UE and a DN-AAA server in the external data network. The SMF shall perform the role of the EAP Authenticator. It relies on an external DN-AAA server to authenticate and authorize the UE request for the establishment of a PDU sessions.

Between the UE and the SMF, EAP messages are sent in the SM NAS message. The SMF communicates with the external DN-AAA over N4 and N6 via the UPF.

12.1.2 Procedure

Editor's Note: modify to use proper normative language, 'shall', 'is' etc. 'shall' is to be used only for the security part.

Editor's Note: figure needs to be editable.

Editor's Note: text needs to make clear that figure shows non-authentication messages only for illustration, they are not part of the normative text in the present TS.

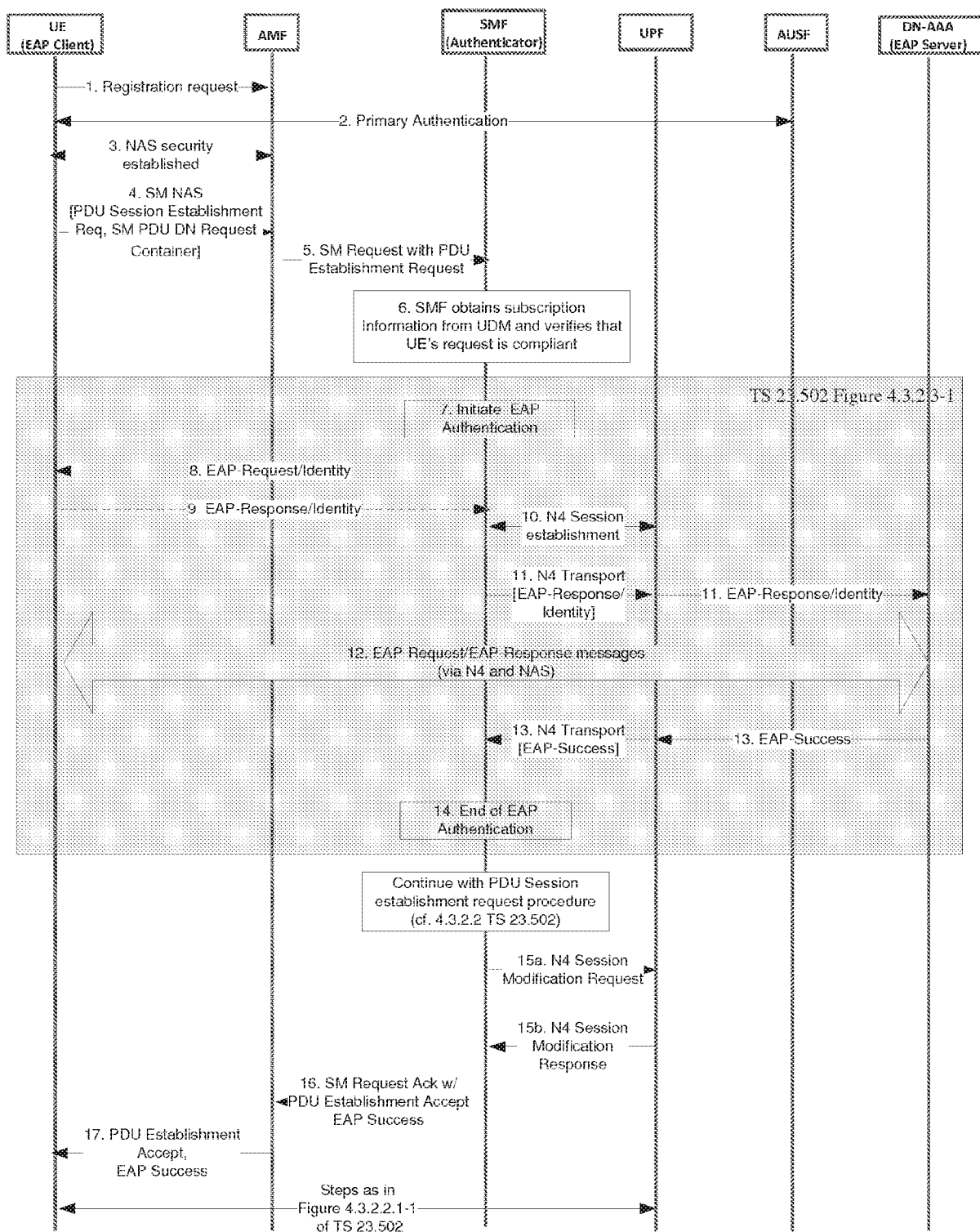


Figure 12.1.2-1 EAP Authentication with an external AAA server

The following procedure is based on clauses 4.3.2.2.1 and 4.3.2.3 in TS 23.502[8].

- 1-3 The NG-UE registers with the network performing primary authentication with AUSF/ARPF based on its network access credentials and establishes a NAS security context with the AMF.

4. The UE shall initiate establishment of a new PDU Session by sending a SM NAS message containing a PDU Session Establishment Request. The UE includes the service it would like to obtain (identified by S-NSSAI) and the PDN it would like to connect to (identified by DNN).

The NAS message may contain SM PDU DN Request Container containing information for the PDU session authorization by the external DN.

5. The AMF selects an SMF and sends a “SM Request” message with SM NAS as one of its payload. It also forwards the Permanent User ID and the received S-NSSAI, DNN.
6. The SMF obtains subscription data from UDM for the given Permanent User ID obtained from AMF in step 5. The SMF checks whether the UE request is compliant with the user subscription and with local policies. If not, the SMF will reject UE's request via SM-NAS signaling and skip rest of the procedure.
7. The SMF shall trigger EAP Authentication to obtain authorization from an external DN-AAA server.
8. The SMF shall send an EAP Request/Identity message to the UE.
9. The UE sends an EAP Response/Identity message. The UE includes its DN-specific identity complying with Network Access Identifier (NAI) format.

NOTE: Steps 8 and 9 are optional. To avoid this additional round-trip, the secondary authentication identity may be sent in step 4.

10. The SMF selects a UPF and initiates a N4 Session establishment procedure with it. The SM PDU DN Request Container, if provided by the UE, is forwarded to the UPF, which further relays it to the DN.

NOTE: Clause 4.3.2.3 in TS 23.502 [8] describes the transport mechanism for delivery of EAP messages between the UE and the external AAA server.

This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.

11. The UPF shall forward the EAP Response/Identity message to the DN AAA Server.
12. The DN AAA server and the UE shall exchange EAP messages as required by the EAP method.
13. After the completion of the authentication procedure, DN AAA server sends EAP Success message to the SMF.
14. This completes the authentication procedure at the SMF.

If the authorization is successful, PDU Session Establishment proceeds further starting step 6a of Figure 4.3.2.2.1-1 in TS 23.502 [8].

- 15a-15b. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 9.a and 9.b of Fig 4.3.2.2.1-1 in TS 23.502 [8].

16. The SMF sends “SM Request Ack” to AMF as in step 10 of Fig. 4.3.2.2.1-1 in TS 23.502[8]. This message shall include EAP Success to be sent to the UE within the NAS SM “PDU session establishment accept”.

17. The AMF forwards NAS SM “PDU session establishment accept” along with EAP Success to the UE as described in steps 11 and step 12 of Figure 4.3.2.2.1-1 in TS 23.502[8].

The UE-requested PDU Session Establishment proceeds further as described in clause 4.3.2.3 in TS 23.502[8].

In case of a Home Routed deployment, it is the SMF in the HPLMN that shall take the role of the authenticator.

Annex A (normative): Key derivation functions

Annex B (informative): Using additional EAP methods for primary authentication

B.1 Introduction

The present annex describes the usage of additional EAP methods for primary authentication within 5G system. Annex x is provided as an example on how the 5G authentication framework for primary authentication can be applied to other EAP methods than EAP AKA'. The additional EAP methods are assumed to be used in special use cases, such as in private networks or with IoT devices in isolated deployment scenarios as specified in TS 22.261 [y].

B.2 Primary authentication and key agreement

B.2.1 Security Procedures with EAP TLS

Editor's Note: This clause is meant to describe the security procedures with EAP TLS.

B.3 Key derivation

Editor's Note: The content of this clause is meant to describe how key derivation is done with additional EAP methods. The clause should take a stand e.g. on serving network binding or other key derivation related aspects.

Annex <X> (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
03-2017	SA3#86b	S3-170964				S3-170904 implemented	0.1.0
05-2017	SA3#87	S3-171524				S3-171491, 492, 493, 495, 496, 497, 499, 545, 501, 502, 503, 504, 505, 506 implemented	0.2.0