6.0

When the UE is capable of connecting to 5GC and EPC and connected to an ng-eNB which is connected to both EPC and 5GC, the UE has the ability to select which core network to connect to as described in clause 4.8.4 in TS24.501[35]. If the UE selects the EPC, the UE shall use security procedure as in TS33.401[10].

6.1.1.1

NOTE A: For standalone non-public networks when an authentication method other than 5G AKA or EAP-AKA' is used, Annex I.2 applies.

NOTE 4: EAP-AKA' and 5G AKA are the only authentication methods that are supported in UE and serving network, hence only they are described in sub-clause 6.1.3 of the present document. For a private network using the 5G system as specified in [7] an example of how additional authentication methods can be used with the EAP framework is given in the informative Annex B.

6.1.1.2

The EAP framework is specified in RFC 3748 [27].

6.1.1.3

the KSEAF shall be cryptographically separate from the key KASME delivered from the home network to the serving network in earlier mobile network generations.

6.1.1.4.1

The serving network name is the concatenation of a service code and the SN Id with a separation character ":" such that the service code prepends the SN Id.

#### 8.1.1.2 Definition of Access Network Identities for Specific Access Networks

Table 8.1.1.2-1 specifies the list of Access Network Identities defined by 3GPP in the context of non-3GPP access to EPC.

Table 8.1.1.2-1: Access Network Identities in the context of non-3GPP access to EPC

|  |  |  |
| --- | --- | --- |
| Access Network Identity | | Type of Access Network |
| ANID Prefix | Additional ANID strings |  |
| "HRPD" constant character string, see NOTE 1 and NOTE 2 | No additional ANID string, see NOTE 2 and NOTE 6 | cdma2000® HRPD access network |
| "WIMAX" constant character string, see NOTE 1 | No additional ANID string, see NOTE 3 and NOTE 6 | WiMAX access network |
| "WLAN" constant character string, see NOTE 1 | No additional ANID string, see NOTE 4 and NOTE 6 | WLAN access network |
| "ETHERNET" constant character string, see NOTE 1 | No additional ANID string, see NOTE 5 and NOTE 6 | Fixed access network |
| All other character strings | Not applicable | Not defined, see NOTE 6 and Annex B |
| NOTE 1: The quotes are not part of the definition of the character string.  NOTE 2: The value of the ANID Prefix for cdma2000® HRPD access networks is defined in 3GPP2 X.S0057 [20]. 3GPP2 is responsible for specifying possible additional ANID strings applicable to the "HRPD" ANID Prefix.  NOTE 3: WiMAX Forum is responsible for specifying possible additional ANID strings applicable to the "WIMAX" ANID Prefix.  NOTE 4: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "WLAN" ANID Prefix.  NOTE 5: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "ETHERNET" ANID Prefix.  NOTE 6: Additional ANID Prefixes and ANID strings can be added to this table following the procedure described in the informative Annex B. | | |

Table 8.1.1.2-2 specifies the list of Access Network Identities defined by 3GPP in the context of access to 5GCN.

Table 8.1.1.2-2: Access Network Identities in the context of access to 5GCN

|  |  |  |
| --- | --- | --- |
| Access Network Identity | | Type of Access Network |
| ANID Prefix | Additional ANID strings |  |
| SNN-service-code, which is "5G" constant character string, see NOTE 1 and NOTE 2 | SNN-network-identifier, see NOTE 2 | N/A, see NOTE 3 |
| NOTE 1: The quotes are not part of the definition of the character string.  NOTE 2: Serving network name (SNN) specified in 3GPP TS 24.501 [76] is used as 5G Access Network Identity.  NOTE 3: Type of Access Network is not applicable for 5G Access Network Identity. | | |

6.1.2



The Nausf\_UEAuthentication\_Authenticate Request message shall contain either:

- SUCI, as defined in the current specification, or

- SUPI, as defined in TS 23.501 [2].

**Table F.2-1: 5G UE behaviour when receiving EAP identity requests**

|  |  |
| --- | --- |
| **REQUEST** | **5G UE RESPONSE** |
| EAP-Request/Identity | EAP-Response/Identity SUCI1) |
| EAP-Request/AKA-Identity  AT\_PERMANENT\_REQ | EAP-Response/AKA-Client-Error with the error code "unable to process packet" 2) |
| EAP-Request/AKA-Identity  AT\_FULLAUTH\_REQ | EAP-Response/AKA-Identity  AT\_IDENTITY=SUCI 3) |
| EAP-Request/AKA-Identity  AT\_ANY\_ID\_REQ | EAP-Response/AKA-Identity  AT\_IDENTITY=fast re-auth identity OR  AT\_IDENTITY=SUCI 4) |

F.3 Subscriber identity and key derivation

EAP-AKA' uses the subscriber identity (Identity) as an input to the key derivation when the key derivation function has value 1 ( i.e. MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)). RFC 4187 [21] clause 7 describes that the Identity is taken from the EAP-Response/Identity or EAP-Response/AKA-Identity AT\_IDENTITY attribute sent by the peer. This principle is not applied to the 5GS.

If the AT\_KDF\_INPUT parameter contains the prefix "5G:", the AT\_KDF parameter has the value 1 and the authentication is not related to fast re-authentication, then the UE shall use SUPI as the Identity for key derivation. This principle applies to all full EAP-AKA' authentications, even if the UE sent SUCI in NAS protocol or if the UE sent SUCI in the respose to the EAP identity requests as described in Table F.2-1 or if no identity was sent because the network performed re-authentication. The only exception is fast re-authentication when the UE follows the key derivation as described in RFC 5448 [12] for fast re-authentication.

NOTE 1: The fast re-authentication is not supported in 5GS.

NOTE 2: The prefix "5G:" is part of serving network name as specified in clause 6.1.1.4.

## 2.2 Composition of IMSI

IMSI is composed as shown in figure 1.



Figure 1: Structure of IMSI

IMSI is composed of three parts:

1) Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscription;

2) Mobile Network Code (MNC) consisting of two or three digits for 3GPP network applications. The MNC identifies the home PLMN of the mobile subscription. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two and three digit MNC codes within a single MCC area is not recommended and is outside the scope of this specification.

3) Mobile Subscriber Identification Number (MSIN) identifying the mobile subscription within a PLMN.

## 2.2A Subscription Permanent Identifier (SUPI)

The SUPI is a globally unique 5G Subscription Permanent Identifier allocated to each subscriber in the 5G System. It is defined in clause 5.9.2 of 3GPP TS 23.501 [119].

The SUPI is defined as:

- a SUPI type: in this release of the specification, it may indicate an IMSI or a network specific identifier; and

- dependent on the value of the SUPI type:

- an IMSI as defined in clause 2.1;

- a network specific identifier, taking the form of a Network Access Identifier (NAI) as defined in clause 28.7.2;

- for an FN-CRG a Global Cable Identifier (GCI) which includes the HFC Identifier and an operator identifier, as defined in clause 28.15.2;

- for an FN-BRG a Global Line Identifier (GLI) which includes a Line Id and an operator identifier, as defined in clause 28.16.2.

NOTE: Depending on the protocol used to convey the SUPI, the SUPI type can take different formats.

## 2.2B Subscription Concealed Identifier (SUCI)

The SUCI is a privacy preserving identifier containing the concealed SUPI. It is defined in clause 6.12.2 of 3GPP TS 33.501 [124].



Figure 2.2B-1: Structure of SUCI

The SUCI is composed of the following parts:

1) SUPI Type, consisting in a value in the range 0 to 7. It identifies the type of the SUPI concealed in the SUCI. The following values are defined:

- 0: IMSI

- 1: Network Specific Identifier

- 2 to 7: spare values for future use.

2) Home Network Identifier, identifying the home network of the subscriber.

When the SUPI Type is an IMSI, the Home Network Identifier is composed of two parts:

- Mobile Country Code (MCC), consisting of three decimal digits. The MCC identifies uniquely the country of domicile of the mobile subscription;

- Mobile Network Code (MNC), consisting of two or three decimal digits. The MNC identifies the home PLMN of the mobile subscription.

When the SUPI type is a Network Specific Identifier, the Home Network Identifier consists of a string of characters with a variable length representing a domain name as specified in clause 2.2 of IETF RFC 7542 [126].

3) Routing Indicator, consisting of 1 to 4 decimal digits assigned by the home network operator and provisioned in the USIM, that allow together with the Home Network Identifier to route network signalling with SUCI to AUSF and UDM instances capable to serve the subscriber.

Each decimal digit present in the Routing Indicator shall be regarded as meaningful (e.g. value "012" is not the same as value "12"). If no Routing Indicator is configured on the USIM, this data field shall be set to the value 0 (i.e. only consist of one decimal digit of "0").

4) Protection Scheme Identifier, consisting in a value in the range of 0 to 15 (see Annex C.1 of 3GPP TS 33.501 [124]). It represents the null scheme or a non-null scheme specified in Annex C of 3GPP TS 33.501 [124] or a protection scheme specified by the HPLMN;

5) Home Network Public Key Identifier, consisting in a value in the range 0 to 255. It represents a public key provisioned by the HPLMN and it is used to identify the key used for SUPI protection. This data field shall be set to the value 0 if and only if null protection scheme is used;

6) Scheme Output, consisting of a string of characters with a variable length or hexadecimal digits, dependent on the used protection scheme, as defined below. It represents the output of a public key protection scheme specified in Annex C of 3GPP TS 33.501 [124] or the output of a protection scheme specified by the HPLMN.

Figure 2.2B-2 defines the scheme output for the null protection scheme.



Figure 2.2B-2: Scheme Output for the null protection scheme

The Mobile Subscriber Identification Number (MSIN) as defined in clause 2.2 or the username identifies the mobile subscription within the Home Network. The scheme output is formatted as a variable length of characters as specified for the username in clause 2.2 of IETF RFC 7542 [126].

NOTE: If the null protection scheme is used, the NFs can derive SUPI from SUCI when needed. The AMF derives SUPI used for AUSF discovery from SUCI when the Routing-Indicator is zero and the protection scheme is null.

Figure 2.2B-3 defines the scheme output for the Elliptic Curve Integrated Encryption Scheme Profile A.



Figure 2.2B-3: Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile A

The ECC ephemeral public key is formatted as 64 hexadecimal digits, which allows to encode 256 bits.

The ciphertext value is formatted as a variable length of hexadecimal digits.

The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Editor's Note: clause C.3.2 of TS 33.501 specifies that the scheme output may contain other parameters (not further defined in the specification). It is FFS how to format these parameters.

Figure 2.2B-4 defines the scheme output for the Elliptic Curve Integrated Encryption Scheme Profile B.



Figure 2.2B-4: Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile B

The ECC ephemeral public key is formatted as 66 hexadecimal digits, which allows to encode 264 bits.

The ciphertext value is formatted as a variable length of hexadecimal digits.

The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Editor's Note: clause C.3.2 of TS 33.501 specifies that the scheme output may contain other parameters (not further defined in the specification). It is FFS how to format these parameters.

Figure 2.2B-5 defines the scheme output for HPLMN proprietary protection schemes.



Figure 2.2B-5: Scheme Output for HPLMN proprietary protection schemes

The HPLMN defined scheme output is formatted as a variable length of hexadecimal digits. Its format is not further defined in 3GPP specifications.

As examples, assuming the IMSI 234150999999999, where MCC=234, MNC=15 and MSISN=0999999999, the Routing Indicator 678, and a Home Network Public Key Identifier of 27:

- the SUCI for the null protection scheme is composed of: 0, 234, 15, 678, 0, 0 and 0999999999

- the SUCI for the Profile <A> protection scheme is composed of: 0, 234, 15, 678, 1, 27, <EEC ephemeral public key value>, <encryption of 0999999999> and <MAC tag value>

28.7.3 NAI format for SUCI

When the SUPI is defined as a Network Specific Identifier, the SUCI shall take the form of a Network Access Identifier (NAI). In this case, the NAI format of the SUCI shall have the form username@realm as specified in clause 2.2 of IETF RFC 7542 [126], where the realm part shall be identical to the realm part of the Network Specific Identifier.

When the SUPI is defined as an IMSI, the SUCI in NAI format shall have the form username without a realm part as specified in clause 2.2 of IETF RFC 7542 [126].

The username part of the NAI shall take one of the following forms:

a) for the null-scheme:

type<supi type>.rid<routing indicator>.schid<protection scheme id>.userid<MSIN or Network Specific Identifier SUPI username>

b) for the Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile A and Profile B:

type<supi type>.rid<routing indicator>.schid<protection scheme id>.hnkey<home network public key id>.ecckey<ECC ephemeral public key value>.cip<ciphertext value>.mac<MAC tag value>

c) for HPLMN proprietary protection schemes:

type<supi type>.rid<routing indicator>.schid<protection scheme id>.hnkey<home network public key id>. out<HPLMN defined scheme output>

See clause 2.2B for the definition and format of the different fields of the SUCI.

Examples:

Assuming the IMSI 234150999999999, where MCC=234, MNC=15 and MSISN=0999999999, the Routing Indicator 678, and a Home Network Public Key Identifier of 27, the NAI format for the SUCI takes the form:

- for the null-scheme:

type0.rid678.schid0.userid0999999999

- for the Profile <A> protection scheme:

type0.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of 0999999999>.mac<MAC tag value>

Assuming the Network Specific Identifier user17@example.com, the Routing Indicator 678, and a Home Network Public Key Identifier of 27, the NAI format for the SUCI takes the form:

- for the null-scheme:

type1.rid678.schid0.useriduser17@example.com

- for the Profile <A> protection scheme:

type1.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of user17>.mac<MAC tag value>@example.com

6.1.3.1

EAP-AKA' is specified in RFC 5448 [12]. The 3GPP 5G profile for EAP-AKA' is specified in the normative Annex F.

8.1. Message Format

As specified in [RFC3748], EAP packets begin with the Code,

Identifiers, Length, and Type fields, which are followed by

EAP-method-specific Type-Data. The Code field in the EAP header is

set to 1 for EAP requests, and to 2 for EAP Responses. The usage of

the Length and Identifier fields in the EAP header is also specified

in [RFC3748]. In EAP-AKA, the Type field is set to 23.

Identifier

The Identifier field is one octet and aids in matching Responses

with Requests.

Length

The Length field is two octets and indicates the length, in

octets, of the EAP packet including the Code, Identifier, Length,

and Data fields. Octets outside the range of the Length field

should be treated as Data Link Layer padding and MUST be ignored

upon reception. A message with the Length field set to a value

larger than the number of received octets MUST be silently

discarded.

In EAP-AKA, the Type-Data begins with an EAP-AKA header that consists

of a 1-octet Subtype field, and a 2-octet reserved field. The

Subtype values used in EAP-AKA are defined in Section 11. The

formats of the EAP header and the EAP-AKA header are shown below.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Code | Identifier | Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Type | Subtype | Reserved |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

The rest of the Type-Data, immediately following the EAP-AKA header,

consists of attributes that are encoded in Type, Length, Value

format. The figure below shows the generic format of an attribute.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Attribute Type | Length | Value...

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Attribute Type

Indicates the particular type of attribute. The attribute type

values are listed in Section 11.

Length

Indicates the length of this attribute in multiples of 4 bytes.

The maximum length of an attribute is 1024 bytes. The length

includes the Attribute Type and Length bytes.

Value

The particular data associated with this attribute. This field

is always included and it is two or more bytes in length. The

type and length fields determine the format and length of the

value field.



The input parameters and their lengths shall be concatenated into a string S as follows:

1. The length of each input parameter measured in octets shall be encoded into a two octet-long string:

a) express the number of octets in input parameter Pi as a number k in the range [0, 65535].

b) Li is then a 16-bit long encoding of the number k, encoded as described in clause B.2.1.

2. String S shall be constructed from n+1 input parameters as follows:

S = FC || P0 || L0 || P1 || L1 || P2 || L2 || P3 || L3 ||... || Pn || Ln

where

FC is used to distinguish between different instances of the algorithm and is either a single octet or consists of two octets of the form FC1|| FC2 where FC1 = 0xFF and FC2 is a single octet,

P0 ... Pn are the n+1 input parameter encodings, and

L0 ... Ln are the two-octet representations of the length of the corresponding input parameter encodings P0.. Pn.

In this specification the following restriction applies to P0: P0 is a static ASCII-encoded string.

This restriction is not part of the KDF definition and does not apply to the KDF when used by other 3GPP specifications unless explicitly stated so in those specifications.

3. The final output, i.e. the derived key is equal to the KDF computed on the string S using the key, denoted Key. The present document defines the following KDF:

derived key = HMAC-SHA-256 ( Key , S )

as specified in [22] and [23].

1. The UDM/ARPF shall first generate an authentication vector with Authentication Management Field (AMF) separation bit = 1 as defined in TS 33.102 [9]. The UDM/ARPF shall then compute CK' and IK' as per the normative Annex A and replace CK and IK by CK' and IK'.

Usage of the AMF

The 16 bits in the AMF are numbered from "0" to "15" where bit "0" is the most significant bit and bit "15" is the least significant bit (see subclause 3.4)

Bit "0" is called the "AMF separation bit". It is used for the purposes of EPS (Evolved Packet System) and is specified in

- TS 33.401 [28] for E-UTRAN access to EPS;

- TS 33.402 [29] for non-3GPP access to EPS;

- TS 33.501 [42] for 5G-RAN access to 5G System.

Bits "1" to "7" are reserved for future standardization use. Bits "1" to "7" shall be set to 0 while not yet specified for a particular use.

Bits "8" to "15" can be used for proprietary purposes. See Annex F for examples usages.

A.2 Function for the derivation of CK’, IK’ from CK, IK

When deriving CK’, IK’ from CK, IK and the access network identity as defined in clause 6 of this specification , the following parameters shall be used to form the input S to the KDF.

- FC = 0x20,

- P0 = value of access network identity, as defined in 3GPP TS 24.302 [22],

- L0 = length of value of access network identity (variable, depending on access network type),

- P1 = SQN  AK

- L1 = length of SQN  AK (i.e. 0x00 0x06)

If AK is not used, AK shall be treated in accordance with TS 33.102, i.e. as 000…0.

The access network identity is defined separately for each access network type. For each access network type, the access network identity is documented in TS 24.302 [22] to ensure that UE and HSS use the same access network identities as input for key derivation.

The input key shall be the concatenation CK || IK of CK and IK.

The KDF returns a 256-bit output, where the 128 most significant bits are identified with CK' and the 128 least significant bits are identified with IK'.

9.12.1 Serving network name (SNN)

The serving network name (SNN) is used:

- in the Network name field of the AT\_KDF\_INPUT attribute defined in IETF RFC 5448 [40];

- in KAUSF derivation function as specified in 3GPP TS 33.501 [24] annex A; and

- in RES\* and XRES\* derivation function as specified in 3GPP TS 33.501 [24] annex A.

SNN shall contain a UTF-8 string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-service-code and SNN-network-identifier, delimited by a colon.

SNN-network-identifier identifies the serving PLMN or the serving SNPN.

MCC and MNC in the SNN-PLMN-ID are MCC and MNC of the serving PLMN. If the MNC of the serving PLMN has two digits, then a zero is added at the beginning.

MCC and MNC in the SNN-SNPN-ID are MCC and MNC of the serving SNPN. If the MNC of the serving SNPN has two digits, then a zero is added at the beginning.

SNN-NID contains an NID in hexadecimal digits.

ABNF syntax of SNN is specified in table 9.12.1.1

Table 9.12.1.1: ABNF syntax of SNN

SNN = SNN-service-code ":" SNN-network-identifier

SNN-service-code = %x35.47 ; "5G"

SNN-network-identifier = SNN-PLMN-ID / SNN-SNPN-ID

SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string ; applicable when not operating in SNPN access mode.

SNN-SNPN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string ":" SNN-NID ; applicable when operating in SNPN access mode.

SNN-mnc-digits = DIGIT DIGIT DIGIT ; MNC of the PLMN ID

SNN-mcc-digits = DIGIT DIGIT DIGIT ; MCC of the PLMN ID

SNN-mnc-string = %x6d.6e.63 ; "mnc" in lower case

SNN-mcc-string = %x6d.63.63 ; "mcc" in lower case

SNN-3gppnetwork-string = %x33.67.70.70.6e.65.74.77.6f.72.6b ; "3gppnetwork" in lower case

SNN-org-string = %x6f.72.67 ; "org" in lower case

SNN-NID = x SNN-hexadecimal-digit ; NID in hexadecimal digits

SNN-hexadecimal-digit = DIGIT / %x41 / %x42 / %x43 / %x44 / %x45 / %x46

NOTE: SNN-service-code allows for distinguishing of ANID specified in 3GPP TS 24.302 [16] and SNN as either of SNN or ANID can be carried in the AT\_KDF\_INPUT attribute.

EXAMPLE 1: In case of a PLMN, if PLMN ID contains MCC = 234 and MNC = 15, SNN is 5G:mnc015.mcc234.3gppnetwork.org.

EXAMPLE 2: In case of an SNPN, if SNPN ID contains a PLMN ID of MCC = 234 and MNC = 15 and an NID of 123ABH, SNN is 5G:mnc015.mcc234.3gppnetwork.org:123AB.

Editor's note (WID: Vertical\_LAN, CR#1511): size of NID is FFS

2. The UDM shall subsequently send this transformed authentication vector AV' (RAND, AUTN, XRES, CK', IK') to the AUSF from which it received the Nudm\_UEAuthentication\_Get Request together with an indication that the AV' is to be used for EAP-AKA' using a Nudm\_UEAuthentication\_Get Response message.

NOTE: The exchange of a Nudm\_UEAuthentication\_Get Request message and an Nudm\_UEAuthentication\_Get Response message between the AUSF and the UDM/ARPF described in the preceding paragraph is the same as for trusted access using EAP-AKA' described in TS 33.402 [11], sub-clause 6.2, step 10, except for the input parameter to the key derivation, which is the value of <network name>. The "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> parameter is not defined in RFC 5448 [12], but rather in 3GPP specifications. For EPS, it is defined as " access network identity " in TS 24.302 [71], and for 5G, it is defined as "serving network name" in sub-clause 6.1.1.4 of the present document.

In case SUCI was included in the Nudm\_UEAuthentication\_Get Request, UDM will include the SUPI in the Nudm\_UEAuthentication\_Get Response.

The AUSF and the UE shall then proceed as described in RFC 5448 [12] until the AUSF is ready to send the EAP-Success.

3. The AUSF shall send the EAP-Request/AKA'-Challenge message to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response message. 4. The SEAF shall transparently forward the EAP-Request/AKA'-Challenge message to the UE in a NAS message Authentication Request message. The ME shall forward the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM. This message shall include the ngKSI and ABBA parameter. In fact, SEAF shall include the ngKSI and ABBA parameter in all EAP-Authentication request message. ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. During an EAP authentication, the value of the ngKSI and the ABBA parameter sent by the SEAF to the UE shall not be changed.

## A.7.1 ABBA parameter values

ABBA parameter is provided to the UE from SEAF and shall be used as an input parameter for KAMF derivation. To support flexible set of security features ABBA parameter is defined when security features change. To ensure forward compatibility, the ABBA parameter is a variable length parameter.

The SEAF shall set the ABBA parameter to 0x0000. The UE shall use the ABBA parameter provided by the SEAF in the calculation of KAMF.

The following values have been defined for this parameter.

|  |  |
| --- | --- |
| **ABBA parameter value** | **Description** |
| 0x0000 | Initial set of security features defined for 5GS. |

Table A.7.1-1: ABBA parameter definitions

NOTE 1: The SEAF needs to understand that the authentication method used is an EAP method by evaluating the type of authentication method based on the Nausf\_UEAuthentication\_Authenticate Response message.

5. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME shall derive CK' and IK' according to Annex A.3.

If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3. 3.

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

7. The SEAF shall transparently forward the EAP-Response/AKA'-Challenge message to the AUSF in Nausf\_UEAuthentication\_Authenticate Request message.

8. The AUSF shall verify the message, and if the AUSF has successfully verified this message it shall continue as follows, otherwise it shall return an error to the SEAF. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for details on linking authentication confirmation).

9. The AUSF and the UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the SEAF. The SEAF shall transparently forward these messages.

NOTE 2: EAP Notifications as described in RFC 3748 [27] and EAP-AKA Notifications as described in RFC 4187 [21] can be used at any time in the EAP-AKA exchange. These notifications can be used e.g. for protected result indications or when the EAP server detects an error in the received EAP-AKA response.

10. The AUSF derives EMSK from CK’ and IK’ as described in RFC 5448[12] and Annex F.

AT\_KDF set to 1

In this case, MK is derived and used as follows:

MK = PRF’(IK’|CK’,"EAP-AKA’"|Identity)

K\_encr = MK[0..127]

K\_aut = MK[128..383]

K\_re = MK[384..639]

MSK = MK[640..1151]

EMSK = MK[1152..1663]

Arkko, et al. Informational [Page 10]

RFC 5448 EAP-AKA’ May 2009

Here [n..m] denotes the substring from bit n to m. PRF’ is a new

pseudo-random function specified in Section 3.4. The first 1664 bits

from its output are used for K\_encr (encryption key, 128 bits), K\_aut

(authentication key, 256 bits), K\_re (re-authentication key, 256

bits), MSK (Master Session Key, 512 bits), and EMSK (Extended Master

Session Key, 512 bits). These keys are used by the subsequent

EAP-AKA’ process. K\_encr is used by the AT\_ENCR\_DATA attribute, and

K\_aut by the AT\_MAC attribute. K\_re is used later in this section.

MSK and EMSK are outputs from a successful EAP method run [RFC3748].

The AUSF uses the most significant 256 bits of EMSK as the KAUSF and then calculates KSEAF from KAUSF as described in clause A.6. The AUSF shall send an EAP Success message to the SEAF inside Nausf\_UEAuthentication\_Authenticate Response, which shall forward it transparently to the UE. Nausf\_UEAuthentication\_Authenticate Response message contains the KSEAF. If the AUSF received a SUCI from the SEAF when the authentication was initiated (see sub-clause 6.1.2 of the present document), then the AUSF shall also include the SUPI in the Nausf\_UEAuthentication\_Authenticate Response message.

NOTE 3: For lawful interception, the AUSF sending SUPI to SEAF is necessary but not sufficient. By including the SUPI as input parameter to the key derivation of KAMF from KSEAF, additional assurance on the correctness of SUPI is achieved by the serving network from both, home network and UE side.

11. The SEAF shall send the EAP Success message to the UE in the N1 message. This message shall also include the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

NOTE 4: Step 11 could be NAS Security Mode Command or Authentication Result.

NOTE 5: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

The key received in the Nausf\_UEAuthentication\_Authenticate Response message shall become the anchor key, KSEAF in the sense of the key hierarchy in sub-clause 6.2 of the present document. The SEAF shall then derive the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7 and send it to the AMF. On receiving the EAP-Success message, the UE derives EMSK from CK’ and IK’ as described in RFC 5448 and Annex F. The ME uses the most significant 256 bits of the EMSK as the KAUSF and then calculates KSEAF in the same way as the AUSF. The UE shall derive the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 6: As an implementation option, the UE creates the temporary security context as described in step 11 after receiving the EAP message that allows EMSK to be calculated. The UE turns this temporary security context into a partial security context when it receives the EAP Success. The UE removes the temporary security context if the EAP authentication fails.

6.1.3.2.0



1. For each Nudm\_Authenticate\_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [9]. The UDM/ARPF shall then derive KAUSF (as per Annex A.2) and calculate XRES\* (as per Annex A.4). Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES\*, and KAUSF.

# A.2 KAUSF derivation function

This clause applies to 5G AKA only.

When deriving a KAUSF from CK, IK and the serving network name when producing authentication vectors, and when the UE computes KAUSF during 5G AKA, the following parameters shall be used to form the input S to the KDF:

- FC = 0x6A;

- P0 = serving network name;

- L0 = length of the serving network name (variable length as specified in 24.501 [35]);

- P1 = SQN ⊕ AK,

- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06).

The XOR of the Sequence Number (SQN) and the Anonymity Key (AK) is sent to the UE as a part of the Authentication Token (AUTN), see TS 33.102. If AK is not used, AK shall be treated in accordance with TS 33.102, i.e. as 000…0.

The serving network name shall be constructed as specified in clause 6.1.1.4.

The input key KEY shall be equal to the concatenation CK || IK of CK and IK.





### 6.3.7 Length of authentication parameters

The authentication key (K) shall have a length of 128 bits or 256 bits.

NOTE: Examples of algorithm set for 3GPP authentication and key agreement functions allow either an authentication key K with only a length of 128 bits, or an authentication key K with a length of 128 bits or 256 bits. Depending on the chosen algorithm set, the operator may have the choice of the length of the authentication key K (128 bits or 256 bits).

The random challenge (RAND) shall have a length of 128 bits.

Sequence numbers (SQN) shall have a length of 48 bits.

The anonymity key (AK) shall have a length of 48 bits.

The authentication management field (AMF) shall have a length of 16 bits.

The message authentication codes MAC in AUTN and MAC‑S in AUTS shall have a length of 64 bits.

The cipher key (CK) shall have a length of 128 bits.

The integrity key (IK) shall have a length of 128 bits.

The authentication response (RES) shall have a variable length of 4‑16 octets.

2. The UDM shall then return the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G-AKA in a Nudm\_UEAuthentication\_Get Response. In case SUCI was included in the Nudm\_UEAuthentication\_Get Request, UDM will include the SUPI in the Nudm\_UEAuthentication\_Get Response.

3. The AUSF shall store the XRES\* temporarily together with the received SUCI or SUPI. 4. The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES\* from XRES\* (according to Annex A.5) and KSEAF from KAUSF(according to Annex A.6), and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G HE AV.

5. The AUSF shall then remove the KSEAF return the 5G SE AV (RAND, AUTN, HXRES\*) to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response.

6. The SEAF shall send RAND, AUTN to the UE in a NAS message Authentication -Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA paremeter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM.

NOTE 2: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the 5G AV by checking whether AUTN can be accepted as described in TS 33.102[9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES\* from RES according to Annex A.4. The ME shall calculate KAUSF from CK||IK according to clause A.2. The ME shall calculate KSEAF from KAUSF according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.

NOTE 3: This separation bit in the AMF field of AUTN cannot be used anymore for operator specific purposes as described by TS 33.102 [9], Annex F.

8. The UE shall return RES\* to the SEAF in a NAS message Authentication Response.

9. The SEAF shall then compute HRES\* from RES\* according to Annex A.5, and the SEAF shall compare HRES\* and HXRES\*. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in sub-clause 6.1.3.2.2. If the UE is not reached, and the RES\* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.

10. The SEAF shall send RES\*, as received from the UE, in a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF.

11. When the AUSF receives as authentication confirmation the Nausf\_UEAuthentication\_Authenticate Request message including a RES\* it may verify whether the AV has expired. If the AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF shall store the KAUSF. AUSF shall compare the received RES\* with the stored XRES\*. If the RES\* and XRES\* are equal, the AUSF shall consider the authentication as successful from the home network point of view.AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for linking with the authentication confirmation).

12. The AUSF shall indicate to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the KSEAF shall be sent to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response. In case the AUSF received a SUCI from the SEAF in the authentication request (see sub-clause 6.1.2 of the present document), and if the authentication was successful, then the AUSF shall also include the SUPI in the Nausf\_UEAuthentication\_Authenticate Response message.

If the authentication was successful, the key KSEAF received in the Nausf\_UEAuthentication\_Authenticate Response messageshall become the anchor key in the sense of the key hierarchy as specified in sub-clause 6.2 of the present document. Then the SEAF shall derive the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7. The SEAF shall provide the ngKSI and the KAMF to the AMF.

If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and KAMF to the AMF after it has received the Nausf\_UEAuthentication\_Authenticate Response message containing SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

6.1.3.3.1

in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [9]) to the ME.



If 5G AKA is used: Upon receipt of an authentication failure message, the AMF/SEAF may initiate new authentication towards the UE. (see TS 24.501 [35]).

If EAP-AKA’ is used: The ME shall proceed as described in RFC 4187 [21] and RFC 5448 [12] for EAP-AKA’.

6.1.3.3.2

When the UDM/ARPF receives an Nudm\_UEAuthentication\_Get Request message with a "*synchronisation failure indication*" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC.

6.1.4.1

The feature of increased home control is useful in preventing certain types of fraud, e.g. fraudulent Nudm\_UECM\_Registration Request for registering the subscriber's serving AMF in UDM 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 Nudm\_UECM\_Registration procedure from the AMF in some way to achieve the desired protection.

6.1.4.1a



1. The AUSF shall inform UDM about the result and time of an authentication procedure with a UE using a Nudm\_UEAuthentication\_ResultConfirmation Request. This shall include the SUPI, a timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

NOTE: It may be sufficient for the purposes of fraud prevention to send only information about successful authentications, but this is up to operator policy.

2. The UDM shall store the authentication status of the UE (SUPI, authentication result, timestamp, and the serving network name).

3. UDM shall reply to AUSF with a Nudm\_UEAuthentication\_ResultConfirmation Response.

4. Upon reception of subsequent UE related procedures (e.g. Nudm\_UECM\_Registration\_Request from AMF) UDM may apply actions according to home operator’s policy to detect and achieve protection against certain types of fraud (e.g. as proposed in section 6.1.4.2).

6.2.1



The keys related to authentication (see Figure 6.2.1-1) include the following keys: K, CK/IK. In case of EAP-AKA', the keys CK', IK' are derived from CK, IK as specified in clause 6.1.3.1.

The key hierarchy (see Figure 6.2.1-1) includes the following keys: KAUSF, KSEAF, KAMF, KNASint, KNASenc, KN3IWF, KgNB, KRRCint, KRRCenc, KUPint and KUPenc.

Keys for AUSF in home network:

- KAUSF is a key derived

- by ME and AUSF from CK', IK' in case of EAP-AKA', CK' and IK' is received by AUSF as a part of transformed AV from ARPF; or,

- by ME and ARPF from CK, IK in case of 5G AKA, KAUSF is received by AUSF as a part of the 5G HE AV from ARPF.

- KSEAF is an anchor key derived by ME and AUSF from KAUSF. KSEAF is provided by AUSF to the SEAF in the serving network.

Key for AMF in serving network:

- KAMF is a key derived by ME and SEAF from KSEAF. KAMF is further derived by ME and source AMF when performing horizontal key derivation.

Keys for NAS signalling:

- KNASint is a key derived by ME and AMF from KAMF, which shall only be used for the protection of NAS signalling with a particular integrity algorithm.

- KNASenc is a key derived by ME and AMF from KAMF, which shall only be used for the protection of NAS signalling with a particular encryption algorithm.

Key for NG-RAN:

- KgNB is a key derived by ME and AMF from KAMF. KgNB is further derived by ME and source gNB when performing horizontal or vertical key derivation. The KgNB is used as KeNB between ME and ng-eNB.

Keys for UP traffic:

- KUPenc is a key derived by ME and gNB from KgNB, which shall only be used for the protection of UP traffic with a particular encryption algorithm.

- KUPint is a key derived by ME and gNB from KgNB, which shall only be used for the protection of UP traffic between ME and gNB with a particular integrity algorithm.

Keys for RRC signalling:

- KRRCint is a key derived by ME and gNB from KgNB, which shall only be used for the protection of RRC signalling with a particular integrity algorithm.

- KRRCenc is a key derived by ME and gNB from KgNB, which shall only be used for the protection of RRC signalling with a particular encryption algorithm.

Intermediate keys:

- NH is a key derived by ME and AMF to provide forward security as described in Clause A.10.

- KNG-RAN \* is a key derived by ME and NG-RAN (i.e., gNB or ng-eNB) when performing a horizontal or vertical key derivation as specified in Clause 6.9. 2.1.1 using a KDF as specified in Clause A.11/A.12.

- K'AMF is a key that can be derived by ME and AMF when the UE moves from one AMF to another during inter-AMF mobility as specified in Clause 6.9.3 using a KDF as specified in Annex A.13.

Key for the non-3GPP access:

- KN3IWF is a key derived by ME and AMF from KAMF for the non-3GPP access. KN3IWF is not forwarded between N3IWFs.

NOTE 1: The key hierarchy for standalone non-public networks when an authentication method other than 5G AKA or EAP-AKA' is used is given in Annex I.2.3.