**3GPP TSG-SA3 Meeting #103-e *S3-212104***

**e-meeting, 17 - 28 May 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1138** | **rev** | **-** | **Current version:** | **16.6.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Handling of KAUSF upon successful primary authentication  |
|  |  |
| ***Source to WG:*** | S3 |
| ***Source to TSG:*** | Samsung, NEC, Nokia, Nokia Shanghai Bell, Intel |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2020-12-23 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | <Release> |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA3 clarified in its LS to CT4 (S3-201350): - Only one KAUSF (latest one) is maintained in the AUSF and in the UE, as KAUSF is security association between the UE and the HPLMN.  - The AUSF in home PLMN never maintains two KAUSF, when a user is simultaneously registered in two Serving Networks via different access-types (3gpp and non-3gpp). - SA3 does not see the need for maintaining multiple KAUSF in the UE and in the HPLMN. Further keeping the old keys laying around in the network is not a good security practice.The above clarifications needs to be captured in the TS 33.501.Further, CT1 in its reply LS (C1-211518), indicated that mandating the AMF to initiate a security mode control procedure as soon as possible after a successful primary authentication and key agreement procedure to take the new partial native 5G NAS security context into use is feasible. So SA3 needs to capture that AMF performs NAS SMC procedure immediately after successful run of primary (re)authentication, as to keep the stored KAUSF aligned between the UE and home network. |
|  |  |
| ***Summary of change:*** | * UDM stores the authEvents for both serving networks in multiple registrations. UDM selects the AUSF reporting the most recent successful authentication result.
* When the UE having multiple registrations, while de-registers from the new serving network:
	+ AUSF and UE stores the latest KAUSF after UE deregistration;
	+ UDM, when deleting the authentication results for the new serving network, keeps the AUSF info in the authEvent.
* UDM selects the latest AUSF that served the UE and maintains the latest KAUSF, for SoRProtection and/or UPUProtection services.
* AUSF stores only the latest KAUSF upon successful authentication procedure and deletes any stored old KAUSF.
* UE stores only the latest KAUSF upon successful authentication procedure and deletes any stored old KAUSF.
* AMF initiates NAS SMC procedure immediately after successful run of primary (re)authentication.

During the execution of e.g. SoR/UPU procedures, the UDM selects the AUSF that stores the latest KAUSF. |
|  |  |
| ***Consequences if not approved:*** | UE and HN may store and use different versions of KAUSF leading to failure of SoRProtection and UPUProtection services. |
|  |  |
| ***Clauses affected:*** | 6.1.1.1, 6.1.3.1, 6.1.3.2.0, 6.1.4.1, 6.2.2.1, 6.2.2.2, 6.3.2.1, 6.4.2.1, 6.14.1,6.9.4.4, 6.14.2.1, 6.14.2.2, 6.14.2.3, 6.15.1, 6.15.2.1, 6.15.2.2, 10.2.2.2, 14.1.Y, B.2.1.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

**\*\*\*\* Start of Changes \*\*\*\***

#### 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 the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the KSEAF provided by the AUSF of the home network to the SEAF of the serving network.

Keys for more than one security context can be derived from the KSEAF without the need of a new authentication run. 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.

The anchor key KSEAF is derived from an intermediate key called the KAUSF. The KAUSF is an additional key established between the UE and HN resulting from the primary authentication procedure. The KAUSF may be securely stored in the AUSF based on the home operator's policy on using such key e.g. if the control plane solution for Steering of Roaming (see sections 6.14) or UE Parameter Update procedures (see sections 6.15) or AKMA are supported by the HPLMN.

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 1: This feature is an optimization that might 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]). The details of this feature are operator-specific and not in scope of this document.

NOTE 2: A subsequent authentication based on the KAUSF stored in the AUSF gives somewhat weaker guarantees than an authentication directly involving the ARPF and the USIM. It is rather comparable to fast re-authentication in EAP-AKA'.

NOTE 2a: Void.

UE and serving network shall support EAP-AKA' and 5G AKA authentication methods.

NOTE 2b: It is the home operator's decision which authentication method is selected.

The USIM shall reside on a UICC. The UICC may be removable or non-removable.

NOTE 3: For non-3GPP access networks USIM applies in case of terminal with 3GPP access capabilities.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA' and 5G AKA for non-3GPP access networks shall reside on the UICC.

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.

NOTE 5: For non-public network (NPN) security the Annex I of the present document provides details.

Upon successful completion of the primary authentication, the AMF shall initiate NAS security mode command procedure (see sub-clause 6.7.2) with the UE.

**\*\*\*\* 2A Change \*\*\*\***

6.1.3.1 Authentication procedure for EAP-AKA'

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

Editor’s Note: The reference to RFC 5448 will be superseded by the internet draft referred to in [67] when it becomes an RFC.

The selection of using EAP-AKA' is described in sub-clause 6.1.2 of the present document.

****

**Figure 6.1.3.1-1: Authentication procedure for EAP-AKA'**

The authentication procedure for EAP-AKA' works as follows, cf. also Figure 6.1.3.1-1:

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'.

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.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication in the Nudm\_UEAuthentication\_Get Response.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication in the Nudm\_UEAuthentication\_Get Response.

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.

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 by comparing the XRES and RES, 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. 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 NAS security Mode Command message. Upon receiving the EAP Success message in the valid NAS Security Mode Command message from the AMF, the UE shall consider the performed primary authentication as successful.

NOTE 4: Void.

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.

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

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

If AUSF and SEAF determine that the authentication was successful, then the SEAF provides the ngKSI and the KAMF to the AMF.

**\*\*\*\* 2B Change \*\*\*\***

##### 6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.



Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

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.

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 after deconcealment of SUCI by SIDF.

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 and 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 parameter 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.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values 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 5G AV has expired. If the 5G 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.

13. If the AUSF indicates that the authentication was successful from the home network point of view, then the AMF shall initiate NAS security mode command procedure (see sub-clause 6.7.2) with the UE, to take the newly generated partial native 5G NAS security context into use. Upon receiving the valid NAS Security Mode Command message from the AMF, the UE shall consider the performed primary authentication as successful. The AMF may, based on policy, decide not to send a new KgNB to initiate AS key re-keying procedure after running NAS Security Mode Command procedure whenever activating a partial native 5G security context, for example, when primary authentication is triggered by NAS COUNT wrap-around.If the authentication was successful, the key KSEAF received in the Nausf\_UEAuthentication\_Authenticate Response message shall 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 KSEAF and SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.

**\*\*\*\* 3rd Change \*\*\*\***

6.1.4.1 Introduction

The 5G authentication and key agreement protocols provide increased home control. Compared to EPS AKA in EPS, this provides better security useful in preventing certain types of fraud as explained in more detail below.

This increased home control comes in the following forms in 5GS:

- 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. sub-clause 6.1.3.1 of the present document.

- In the case of 5G AKA, the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the authentication confirmation received by the AUSF in Nausf\_UEAuthentication\_Authenticate Request message has been successfully verified, cf. sub-clause 6.1.3.2 of the present document.

When 3GPP credentials are used in above cases, the result is reported to the UDM. Details are described in clause 6.1.4.1a.

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.

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

But informative guidance is given in sub-clause 6.1.4.2 as to what measures an operator could usefully take. Such guidance may help avoiding a proliferation of different solutions.

The feature of increased home control is also used to allow the UDM to keep track of the AUSF that stores the KAUSF to be used during e.g. the control plane solution for Steering of Roaming or UE Parameter Update procedures; i.e. the AUSF that stores the latest KAUSF generated after successful completion of the latest primary authentication reported to the UDM.

After the UDM is informed that the UE has been successfully (re-)authenticated, the UDM shall store the AUSF instance which reported the successful authentication. If the UDM has been previously informed that the UE was authenticated by a different AUSF instance, the UDM may request the old AUSF to clear the stale security parameters (KAUSF, SOR counter and UE parameter update counter). If the UDM determines to delete the security parameters in the old AUSF, then the UDM shall use the Nausf\_UEAuthentication\_deregister service operation (see clause 14.1.Y) to send the indication to the old AUSF to clear the old KAUSF.

**\*\*\*\* 4th Change \*\*\*\***

6.2.2.1 Keys in network entities

***Keys in the ARPF***

The ARPF shall process the long-term key K and any other sensitive data only in its secure environment. The key K shall be 128 bits or 256 bits long.

During an authentication and key agreement procedure, the ARPF shall derive CK' and IK' from K in case EAP-AKA' is used and derive KAUSF from K in case 5G AKA is used. The ARPF shall forward the derived keys to the AUSF.

The ARPF holds the Home Network Private Key that is used by the SIDF to deconceal the SUCI and reconstruct the SUPI. The generation and storage of this key material is out of scope of the present document.

***Keys in the AUSF***

In case EAP-AKA' is used as authentication method, the AUSF shall derive a key KAUSF from CK' and IK' for EAP-AKA' as specified in clause 6.1.3.1. In case that 5G AKA is used as authentication method, the UDM/ARPF shall generate the KAUSF as specified in clause 6.1.3.2.

The KAUSF may be stored in the AUSF between two subsequent authentication and key agreement procedures.

When the AUSF stores the KAUSF, the AUSF shall store the latest KAUSF generated after successful completion of the latest primary authentication. The authentication is considered as successful and the AUSF shall store the latest KAUSF or replace the old KAUSF with the new KAUSF (if the AMF(s) end up selecting the same AUSF instance for (re)authentication of the UE) when:

 - in case 5G AKA is used as authentication method, when the RES\* and the XRES\* are equal (see clause 6.1.3.2.0).

 - in case EAP-AKA' is used as authentication method, when the AUSF sends an EAP-Success message to the SEAF (see clause 6.1.3.1).

The AUSF shall generate the anchor key, also called KSEAF, from the authentication key material received from the ARPF during an authentication and key agreement procedure.

***Keys in the SEAF***

The SEAF receives the anchor key, KSEAF, from the AUSF upon a successful primary authentication procedure in each serving network.

The SEAF shall never transfer KSEAF to an entity outside the SEAF. Once KAMF is derived KSEAF shall be deleted.

The SEAF shall generate KAMF from KSEAF immediately following the authentication and key agreement procedure and hands it to the AMF.

NOTE 1: This implies that a new KAMF, along with a new KSEAF, is generated for each run of the authentication and key agreement procedure.

NOTE 2: The SEAF is co-located with the AMF.

***Keys in the AMF***

The AMF receives KAMF from the SEAF or from another AMF.

The AMF shall, based on policy, derive a key KAMF' from KAMF for transfer to another AMF in inter-AMF mobility. The receiving AMF shall use KAMF' as its key KAMF.

NOTE 3: The precise rules for key handling in inter-AMF mobility can be found in clause 6.9.3.

The AMF shall generate keys KNASint and KNASenc dedicated to protecting the NAS layer.

The AMF shall generate access network specific keys from KAMF. In particular,

- the AMF shall generate KgNB and transfer it to the gNB.

- the AMF shall generate NH and transfer it to the gNB, together with the corresponding NCC value.
The AMF may also transfer an NH key, together with the corresponding NCC value, to another AMF, cf. clause 6.9.

- the AMF shall generate KN3IWF and transfer it to the N3IWF when KAMF is received from SEAF, or when KAMF' is received from another AMF.

***Keys in the NG-RAN***

The NG-RAN (i.e., gNB or ng-eNB) receives KgNB and NH from the AMF. The ng-eNB uses KgNB as KeNB.

The NG-RAN (i.e., gNB or ng-eNB) shall generate all further access stratum (AS) keys from KgNB and /or NH.

***Keys in the N3IWF***

The N3IWF receives KN3IWF from the AMF.

The N3IWF shall use KN3IWF as the key MSK for IKEv2 between UE and N3IWF in the procedures for untrusted non-3GPP access, cf. clause 11.

Figure 6.2.2-1 shows the dependencies between the different keys, and how they are derived from the network nodes point of view.

**Figure 6.2.2-1: Key distribution and key derivation scheme for 5G for network nodes**

NOTE 4: The key derivation and distribution scheme 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.

**\*\*\*\* 5th Change \*\*\*\***

6.2.2.2 Keys in the UE

For every key in a network entity, there is a corresponding key in the UE.

Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.

**Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE**

***Keys in the USIM***

The USIM shall store the same long-term key K that is stored in the ARPF.

During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME.

If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI.

***Keys in the ME***

The ME shall generate the KAUSF from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3.

When 5G AKA is used, the generation of RES\* from RES shall be performed by the ME.

The UE shall store the latest KAUSF or replace the old KAUSF with the latest KAUSF, after successful completion of the latest primary authentication. If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME.

In case 5G AKA is used as an authentication method, upon receiving the valid NAS Security Mode Command message from the AMF (to take the corresponding partial context derived from the newly generated KAUSF into use), the UE shall consider the performed primary authentication as successful and the UE shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.

In case of any key generating EAP method in TS 33.501 (EAP-AKA', EAP-TLS in Annex B, EAP methods in Annex I) is used as the authentication method for the primary (re)authentication, upon receiving the EAP-Success message in the valid NAS Security Mode Command message from the AMF, the primary authentication shall be considered as successful and the UE shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.

The ME shall perform the generation of KSEAF from the KAUSF. If the USIM supports 5G parameters storage, KSEAF shall be stored in the USIM. Otherwise, KSEAF shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of KAMF. If the USIM supports 5G parameters storage, KAMF shall be stored in the USIM. Otherwise, KAMF shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of all other subsequent keys that are derived from the KAMF.

Any 5G security context, KAUSF and KSEAF that are stored at the ME shall be deleted from the ME if:

a) the USIM is removed from the ME when the ME is in power on state;

b) the ME is powered up and the ME discovers that the USIM is different from the one which was used to create the 5G security context;

c) the ME is powered up and the ME discovers that there is no USIM is present at the ME.

NOTE 1: The key derivation and distribution scheme 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.

**\*\*\*\* 6th Change \*\*\*\***

6.3.2.1 Multiple registrations in different PLMNs

The UE shall independently maintain and use two different 5G security contexts, one per PLMN's serving network. Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

The ME shall store the two different 5G security contexts on the USIM if the USIM supports the 5G parameters storage. If the USIM does not support the 5G parameters storage, then the ME shall store the two different 5G security contexts in the ME non-volatile memory. Both of the two different 5G security contexts are current 5G security context.

The latest KAUSF result of the successful completion of the latest primary authentication shall be used by the UE and the HN regardless over which access network type (3GPP or non-3GPP) it was generated.

The HN shall keep the latest KAUSF generated during successful authentication over a given access even if the UE is deregistered from that access, but the UE is registered via another access.

**\*\*\*\* 7th Change \*\*\*\***

6.4.2.1 Multiple active NAS connections with different PLMNs

TS 23.501 [2] has a scenario when the UE is registered to a VPLMN's serving network via 3GPP access and to another VPLMN's or HPLMN's serving network via non-3GPP access at the same time. When the UE is registered in one PLMN's serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN's serving network over another type of access (e.g. non-3GPP), then the UE has two active NAS connections with different AMF's in different PLMNs. As described in clause 6.3.2.1, the UE shall independently maintain and use two different 5G security contexts, one per PLMN serving network. The 5G security context maintained by the UE shall contain the full set of 5G parameters, including NAS context parameters for 3GPP and non-3GPP access types per PLMN. In case of connection to two different PLMNs, it is necessary to maintain a complete 5G NAS security context for each PLMN independently, each with all associated parameters (such as two pairs of NAS COUNTs, i.e. one pair for 3GPP access and one pair for non-3GPP access).

Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

If UE receives more than one authentication requests via different access types simultaneously (e.g. initial registration after UE powers on, UE initiate the service request procedures simultaneously via both NAS connections), the UE shall process the authentication challenges in sequence. The UE shall respond to the second authentication challenge after completion of the first authentication procedure. In case if the first authentication procedure is 5G-AKA, then after sending the Authentication Response message to the network the UE shall respond to the second authentication challenge and in case if the first authentication procedure is EAP-AKA', then after receiving EAP Success/Failure from the network the UE shall respond to the second authentication challenge.

All the NAS and AS security mechanisms defined for single registration mode are applicable independently on each access using the corresponding 5G security context.

NOTE: The UE belongs to a single HPLMN.

**\*\*\*\* 8th Change \*\*\*\***

#### 6.9.4.4 AS key re-keying

The KgNB/KeNB re-keying procedure is initiated by the AMF. It may be used under the following conditions:

- after a successful AKA run with the UE as part of activating a partial native 5G security context; or

- as part of synchronizing the NAS and the AS security contexts as a part of handover procedure, if a handover is occuring; or

- as part of re-activating a non-current full native 5G security context after handover from E-UTRAN according to clause 8.4; or

- to create a new KgNB from the current KAMF.

The AMF may, based on policy, decide not to send a new KgNB to initiate AS key re-keying procedure after running primary authentication following a NAS Security Mode Command procedure whenever activating a partial native 5G security context, for example, when primary authentication is triggered by NAS COUNT wrap-around.

NOTE 1: To perform a key change on-the-fly of the entire key hierarchy, the AMF has to change the 5G NAS security context before changing the 5G AS security context.

In order to be able to re-key the KgNB, the AMF requires a fresh uplink NAS COUNT from a successful NAS SMC procedure with the UE. In the case of creating a new KgNB from the current KAMF a NAS SMC procedure shall be run first to provide this fresh uplink NAS COUNT. This NAS SMC procedure does not have to change other parameters in the current EPS NAS security context. The AMF derives the new KgNB using the key derivation function as specified in Annex A.9 using the KAMF and the uplink NAS COUNT used in the most recent NAS Security Mode Complete message. The derived new KgNB is sent to the gNB/ng-eNB in an NGAP UE CONTEXT MODIFICATION REQUEST message triggering the gNB/ng-eNB to perform the AS key re-keying. The gNB/ng-eNB runs the key change on-the-fly procedure with the UE. During this procedure the gNB/ng-eNB shall indicate to the UE that a key change on-the-fly is taking place. The procedure used is based on an intra-cell handover, and hence the same KgNB derivation steps shall be taken as in a normal handover procedure. The gNB/ng-eNB shall indicate to the UE to change the current KgNB in intra-cell handover during this procedure. Network-side handling of AS key re-keying that occur as a part of Xn and N2 handovers are described is defined in clauses 6.9.2.3.2 and 6.9.2.3.3 of the present document.

When the UE receives an indication that the procedure is a key change on-the-fly procedure, the UE shall derive a temporary KgNB by applying the key derivation function as specified in Annex A.9 using the KAMF from the current 5G NAS security context and the uplink NAS COUNT in the most recent NAS Security Mode Complete message. UE-side handling of AS key re-keying that occur as a part of Xn and N2 handovers is described in clause 6.9.2.3.4 of the present document.

From this temporary KgNB the UE shall derive the KNG-RAN\* as normal (see Annex A.11/A.12). The gNB/ng-eNB shall take the KgNB it received from the AMF, which is equal to the temporary KgNB, as basis for its KNG-RAN\* derivations. From this step onwards, the key derivations continue as in a normal handover.

If the AS level re-keying fails, then the AMF shall complete another NAS security mode procedure before initiating a new AS level re-keying. This ensures that a fresh KgNB is used.

The NH parameter shall be handled according to the following rules:

- The UE, AMF, and gNB/ng-eNB shall delete any old NH upon completion of the context modification.

- The UE and AMF shall use the KAMF from the currently active 5G NAS security context for the computation of the fresh NH. The computation of NH parameter value sent in the Namf\_Communication\_CreateUEContext Request, NGAP HANDOVER REQUEST, and NGAP PATH SWITCH REQUEST ACKNOWLEDGE messages shall be done according to clauses 6.9.2.3.2 and 6.9.2.3.3.

**\*\*\*\* 9th Change \*\*\*\***

6.14.1 General

This clause describes the security functions necessary to support steering of the UE in the VPLMN during registration procedure and also after registration as described in TS 23.122 [53] Annex C. The security functions are described in the context of the functions supporting the control plane solution for steering of roaming in 5GS.

If the control plane solution for Steering of Roaming is supported by the HPLMN, the AUSF shall store the latest KAUSF after the completion of the latest primary authentication.

The content of the Steering List as well as the conditions for sending it to the UE are described in TS 23.122 [53] Annex C. The Steering List includes either a list of preferred PLMN/access technology combinations, a secured packet or the HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'.

NOTE: The Steering of Roaming Information is defined in clause 1.2 of TS 23.122 [53]. It contains thus the ACK indication, the Steering List and the integrity protection information.

**\*\*\*\* 10th Change \*\*\*\***

6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case where the UE registers with VPLMN AMF is described below in figure 6.14.2.1-1:

**Figure 6.14.2.1-1: Procedure for providing list of preferred PLMN/access technology combinations** **during registration in VPLMN**

1) The UE initiates registration by sending Registration Request message to the VPLMN AMF.

2-3) The VPLMN AMF executes the registration procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]. As part of the registration procedure, the VPLMN AMF executes primary authentication of the UE and then initiates the NAS SMC procedure, after the authentication is successful.

4-5) The VPLMN AMF invokes the Nudm\_UECM\_Registration message to the UDM and registers access with the UDM as per step 14a in sub-clause 4.2.2.2.2 of 3GPP TS 23.502[8].

6) The VPLMN AMF invokes Nudm\_SDM\_Get service operation message to the UDM to get amongst other information the Access and Mobility Subscription data for the UE (see step 14b in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]).

7) The UDM decides to send the Steering of Roaming Information, and obtains a list of preferred PLMN/access technology combinations or a secured packet list as described in TS 23.122 [53].

 If the UDM determines that the UE is configured to not expect to receive Steering of Roaming Information at initial registration and if the UDM determines that no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed, then the UDM may not piggyback Steering of Roaming Information at all in the Nudm\_SDM\_Get response and hence the following steps are omitted.

8-9) The UDM shall invoke Nausf\_SoRProtection service operation message to the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE. If the HPLMN decides that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf\_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-IUE, as specified in sub-clause 14.1.3 of this document.

NOTE: At reception of Nausf\_SoRProtection\_Protect request from the UDM, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and list of preferred PLMN/access technology combinations or secured packet (if provided).

The details of the CounterSoR are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SoR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the received Steering of Roaming Information is not tampered with or removed by the VPLMN. The expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering of Roaming Information.

10) The UDM responds to the Nudm\_SDM\_Get service operation to the VPLMN AMF, which shall include the ACK Indication, the list of preferred PLMN/access technology combinations or secured packet (if provided), SoR-MAC-IAUSF and CounterSoR within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-IUE.

11) The VPLMN AMF shall construct the SOR header based on the ACK Indication and the list of preferred PLMN/access technology combinations or secured packet (if provided) received from the UDM and include it in the SOR transparent container as specified in clause 9.11.3.51 of TS 24.501 [35]. The resulting Steering of Roaming Information, also including SoR-MAC-IAUSFand CounterSoR(both also received from the UDM), is conveyed to the UE in the Registration Accept message;

12) On receiving the Registration Accept message with Steeringof Roaming Information the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the received Steering of Roaming Information, including the CounterSoR and the SoR header, and verifies whether it matches the SoR-MAC-IAUSF value received in the Registration Accept message. Based on the SoR-MAC-IAUSF verification outcome, the behaviour of the UE is specified in TS 23.122 [53].

13) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering of Roaming Information received in step 11 has been provided by the HPLMN, then the UE shall send the Registration Complete message to the serving AMF. The UE shall generate the SoR-MAC-IUE as specified in Annex A.18 and includes the generated SoR-MAC-IUE in a SOR transparent container in the Registration Complete message.

14) The AMF sends a Nudm\_SDM\_Info request message to the UDM. If a transparent container with the SoR-MAC-IUE was received in the Registration Complete message, the AMF shall include the SoR-MAC-IUEin the Nudm\_SDM\_Info request message.

15) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information in step 10, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 10.

**\*\*\*\* 11th Change \*\*\*\***

6.14.2.2 Procedure for steering of UE in VPLMN or HPLMN after registration

The security procedure for the steering of UE in VPLMN after registration is described below in figure 6.14.2.2-1:

**Figure 6.14.2.2-1: Procedure for providing list of preferred PLMN/access technology combinations** **after registration**

1) The UDM decides to notify the UE of the changes to the Steering of Roaming Information by the means of invoking Nudm\_SDM\_Notification service operation.

2-3) The UDM shall invoke Nausf\_SoRProtection service operation message by including the ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packetto the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf\_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-IUE, as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

NOTE: At reception of Nausf\_SoRProtection\_Protect request from the UDM, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packet.

The details of the CounterSoR are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SOR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the Steering of Roaming Information received is not tampered with or removed by the VPLMN. The inclusion of these information in the calculation of the expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering of Roaming Information.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which contains optionally the list of preferred PLMN/access technology combinations or secured packet,the ACK Indication, SoR-MAC-IAUSF, and CounterSoR within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-IUE.

5) Upon receiving the Nudm\_SDM\_Notification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the SOR transparent container (including the SOR header) constructed as specified in clause 9.11.3.51 of 3GPP TS 24.501 [35] based on the ACK Indication, the Steering List, SoR-MAC-IAUSF and CounterSoR received from the UDM.

6) On receiving the DL NAS Transport message, the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the received Steering of Roaming Information, including the CounterSoR and the SoR header and verify whether it matches the SoR-MAC-IAUSF value received in the DL NAS Transport message.

7) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering Information has been provided by the HPLMN, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the SoR-MAC-IUE as specified in Annex A.18 and includes the generated SoR-MAC-IUE in a SOR transparent container in the UL NAS Transport message.

8) The AMF shall send a Nudm\_SDM\_Info request message to the UDM. If a SOR transparent container with the SoR-MAC-IUE was received in the UL NAS Transport message, the AMF shall include the SoR-MAC-IUE in the Nudm\_SDM\_Info request message.

9) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 4.

**\*\*\*\* 12th Change \*\*\*\***

6.14.2.3 SoR Counter

The AUSF and the UE shall associate a 16-bit counter, CounterSoR, with the key KAUSF.

The UE shall initialize the CounterSoR to 0x00 0x00 when the newly derived KAUSF is stored (see clause 6.2.2.2). The UE shall store the SoR counter. If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterSoR shall be stored in the USIM. Otherwise, CounterSoR shall be stored in the non-volatile memory of the ME.

To generate the SoR-MAC-IAUSF, the AUSF shall use the CounterSoR. The CounterSoR shall be incremented by the AUSF for every new computation of the SoR-MAC-IAUSF. The CounterSoR is used as freshness input into SoR-MAC-IAUSF and SoR-MAC-IUE derivations as described in the Annex A.17 and Annex A.18 respectively, to mitigate the replay attack. The AUSF shall send the value of the CounterSoR (used to generate the SoR-MAC-IAUSF) along with the SoR-MAC-IAUSF to the UE. The UE shall only accept CounterSoR value that is greater than stored CounterSoR value. The UE shall store the received CounterSoR, onlyif the verification of the received SoR-MAC-IAUSF is successful. The UE shall use the stored CounterSoR received from the HPLMN, when deriving the SoR-MAC-IUE for the SoR acknowledgement.

The AUSF and the UE shall maintain the CounterSoR for lifetime of the KAUSF.

The AUSF that supports the control plane solution for steering of roaming shall initialize the CounterSoR to 0x00 0x01 when the newly derived KAUSF is stored (see clause 6.2.2.1). The AUSF shall set the CounterSoR to 0x00 0x02 after the first calculated SoR-MAC-IAUSF, and monotonically increment it for each additional calculated SoR-MAC-IAUSF. The SoR Counter value of 0x00 0x00 shall not be used to calculate the SoR-MAC-IAUSF and SoR-MAC-IUE.

The AUSF shall suspend the SoR protection service for the UE, if the CounterSoR associated with the KAUSF of the UE, is about to wrap around. When a fresh KAUSF is generated for the UE, the CounterSoR at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume the SoR protection service for the UE.

**\*\*\*\* 13th Change \*\*\*\***

6.15.1 General

This clause describes the security functions necessary to update the UE parameters using the UDM control plane procedure specified in TS 23.502 [8]. The security functions are described in the context of the functions supporting the delivery of UE Parameters Update Data from the UDM to the UE after the UE has successfully registered to the 5G network.

If the control plane procedure for UE parameters update is supported by the UDM, the AUSF shall store the latest KAUSF after the completion of the latest primary authentication.

The content of UE Parameters Update Data and the conditions for sending it to the UE as well as how it is handled at the UE are specified in TS 24.501 [35].

NOTE : The home network relies on the serving network to deliver the UE parameters update.

**\*\*\*\* 14th Change \*\*\*\***

6.15.2.1 Procedure for UE Parameters Update

The UDM may decide to perform UE parameters update anytime after the UE has been successfully authenticated and registered to the 5G system. The security procedure for the UE parameters update is described below in figure 6.15.2.1-1:

****

**Figure 6.15.2.1-1: Procedure for UE Parameters Update**

1) The UDM decides to perform the UE Parameters Update (UPU) using the control plane procedure while the UE is registered to the 5G system. If the final consumer of any of the UE parameters to be updated (e.g., the updated Routing ID Data) is the USIM, the UDM shall protect these parameters using a secured packet mechanism (see 3GPP TS 31.115 [65]) to update the parameters stored on the USIM. The UDM shall then prepare the UE Parameters Update Data (UPU Data) by including the parameters protected by the secured packet, if any, as well as any UE parameters for which final consumer is the ME (see TS 24.501 [35]).

2-3) The UDM shall invoke Nausf\_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-IAUSF and CounterUPU as specified in sub-clause 14.1.4 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the UDM decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall set the corresponding indication in the UE Parameters Update Data (see TS 24.501 [35]) and include the ACK Indication in the Nausf\_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-IUE, as specified in sub-clause 14.1.4 of this document.

The details of the CounterUPU is specified in sub-clause 6.15.2.2 of this document. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-IUE allows the UDM to verify that the UE received the UE Parameters Update Data correctly.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which contains UE Parameters Update Data, UPU-MAC-IAUSF, CounterUPU within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected UPU-XMAC-IUE.

5) Upon receiving the Nudm\_SDM\_Notification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the transparent container received from the UDM.

6) On receiving the DL NAS Transport message, the UE shall calculate the UPU-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.19) on the received UE Parameters Update Data and the CounterUPU and verify whether it matches the UPU-MAC-IAUSF value received in the DL NAS Transport message. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is protected by secured packet (see 3GPP TS 31.115 [65]), the ME shall forward the secured packet to the USIM using procedures in 3GPP TS 31.111 [66]. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is not protected by secure packet, the ME shall update its stored parameters with the received parameters in UDM Updata Data.

7) If the UDM has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the UDM, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the UPU-MAC-IUE as specified in Annex A.20 and include the generated UPU-MAC-IUE in a transparent container in the UL NAS Transport message.

8) If a transparent container with the UPU-MAC-IUE was received in the UL NAS Transport message, the AMF shall send a Nudm\_SDM\_Info request message with the transparent container to the UDM.

9) If the UDM indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall compare the received UPU-MAC-IUE with the expected UPU-XMAC-IUE that the UDM stored temporarily in step 4.

**\*\*\*\* 15th Change \*\*\*\***

6.15.2.2 UE Parameters Update Counter

The AUSF and the UE shall associate a 16-bit counter, CounterUPU, with the key KAUSF.

The UE shall initialize the CounterUPU to 0x00 0x00 when the newly derived KAUSF is stored (see clause 6.2.2.2). The UE shall store the UPU counter . If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterUPU shall be stored in the USIM. Otherwise, CounterUPU shall be stored in the non-volatile memory of the ME.

To generate the UPU-MAC-IAUSF, the AUSF shall use the CounterUPU. The CounterUPU shall be incremented by the AUSF for every new computation of the UPU-MAC-IAUSF. The CounterUPU is used as freshness input into UPU-MAC-IAUSF and UPU-MAC-IUE derivations as described in the Annex A.19 and Annex A.20 respectively, to mitigate the replay attack. The AUSF shall send the value of the CounterUPU (used to generate the UPU-MAC-IAUSF) along with the UPU-MAC-IAUSF to the UE. The UE shall only accept CounterUPU value that is greater than stored CounterUPU value. The UE shall update the stored CounterUPU with the received CounterUPU, onlyif the verification of the received UPU-MAC-IAUSF is successful. The UE shall use the CounterUPU received from the UDM, when deriving the UPU-MAC-IUE for the UE Parameters Upadate Data acknowledgement.

The AUSF and the UE shall maintain the CounterUPU for lifetime of the KAUSF.

The AUSF that supports the UE parameters update using control plane procedure shall initialize the CounterUPU to 0x00 0x01 when the newly derived KAUSF is stored (see clause 6.2.2.1). The AUSF shall set the CounterUPU to 0x00 0x02 after the first calculated UPU-MAC-IAUSF, and monotonically increment it for each additional calculated UPU-MAC-IAUSF. The UPU Counter value of 0x00 0x00 shall not be used to calculate the UPU-MAC-IAUSF and UPU-MAC-IUE.

The AUSF shall suspend the UE Parameters Update protection service for the UE, if the CounterUPU associated with the KAUSF of the UE, is about to wrap around. When a fresh KAUSF is generated for the UE, the CounterUPU at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume theUE Parameters Update protection service for the UE.

**\*\*\*\* 16th Change \*\*\*\***

10.2.2.2 UE sets up an IMS Emergency session with emergency registration

UEs that are in limited service state (LSM) request emergency services by initiating the Registration procedure with the indication that the registration is to receive emergency services, referred to as Emergency Registration.

UEs that had earlier registered for normal services but now cannot be authenticated by the serving network, shall initiate Emergency Registration procedure to request emergency services.

It shall be possible to configure whether the network allows or rejects an emergency registration request and whether it allows unauthenticated UEs to establish bearers for unauthenticated IMS emergency sessions or not.

The AMF may attempt to authenticate the UE after receiving the emergency registration request.

If authentication failed in the UE during an emergency registration request, the UE shall wait for a NAS SMC command to set up an unauthenticated emergency bearer.

If authentication failed in the serving network and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as with the normal initial registration requests. The AMF shall reject the unauthenticated emergency bearer setup request from the UE.

If authentication failed in the serving network and if the serving network policy allow unauthenticated IMS Emergency Sessions, then the AMF shall support unauthenticated emergency bearer setup and the behaviours of the UE and the AMF are as described below.

a) UE behaviour:

After sending Emergency Registration request to the serving network the UE shall know of its own intent to establish an unauthenticated IMS Emergency Session.

The UE shall proceed as specified for the non-emergency case in except that the UE shall accept a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF. If the UE accepts a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF as part of Emergency Registration request, then the primary authentication performed if any shall be considered as unsuccessful and the newly generated KAUSF is not stored.

NOTE: In case of authentication success the AMF will send a NAS SMC selecting algorithms with a non-NULL integrity algorithm, and the UE will accept it.

b) AMF behavior:

After receiving Emergency Registration request from the UE, the AMF knows of that UE's intent to establish an unauthenticated IMS Emergency Session.

- If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

- After the unsuccessful verification of the UE, the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

- If both, the Emergency Registration request and an AUTHENTICATION FAILURE message with error code as defined in 24.501 [35] clauses 5.4.1.2.4.5 (for EAP based authentication) or 5.4.1.3.7 (for 5G AKA based authentication) are received by the AMF from the UE, then the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

If the UE has initiated a PDU session establishment procedure to establish bearers for unauthenticated IMS emergency sessions and the AMF has indicated to the SMF that this is an unauthenticated emergency call, then the SMF shall indicate 'Not Needed' in the UP security policy for both UP confidentiality and UP integrity protection to the ng-eNB/gNB.

**\*\*\*\* 17th Change \*\*\*\***

14.1.Y Nausf\_UEAuthentication\_deregister service operation

**Service operation name:** Nausf\_UEAuthentication\_deregister

**Description:** Deletion of stale security parameters (KAUSF, SOR counter and UE parameter update counter) in AUSF. UDM uses this service operation to request the AUSF to clear the stale security parameters, after the UE has been successfully (re)authenticated in different AUSF Instance.

**Input, Required:** SUPI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

**\*\*\*\* 18th Change \*\*\*\***

B.2.1.1 Security procedures

EAP-TLS is a mutual authentication EAP method that can be used by the EAP peer and the EAP server to authenticate each other. It is specified in RFC 5216 [38] and draft-ietf-emu-eap-tls13 [76]. The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [3]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [5].

EAP-TLS supports several TLS versions, and the negotiation of the TLS version is part of EAP-TLS. The main principle of negotiation goes as follows. The EAP server indicates the support for EAP-TLS in the EAP-Request. If the peer chooses EAP-TLS, it responds with an EAP-Response indicating in the ClientHello message which TLS versions the peer supports. The EAP server chooses the TLS version, and indicates the chosen version in the ServerHello message.

The TLS procedure described in the RFC 5216 [38] is applicable to TLS 1.2 defined in RFC 5246 [40]. The TLS procedure described in the draft-ietf-emu-eap-tls13 [76] is applicable to TLS 1.3 defined in RFC 8446 [77].

The procedure below is based on the unified authentication framework from the present document, procedures from TS 23.502 [8] and RFC 5216 [38]. The procedure for EAP-TLS with TLS 1.2 is presented here as an example, and other potential procedures are possible, e.g. if TLS resumption is used.



**Figure B.2.1.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial authentication**

1. The UE sends the Registration Request message to the SEAF, containing SUCI. If the SUPI is in NAI format, only the username part of the NAI is encrypted using the selected protection scheme and included in the SUCI, together with the realm part in the NAI needed for UDM routing.

Privacy considerations are described in Clause B.2.2.

2. The SEAF sends Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. The SUCI and the serving network name (as described in clause 6.1.1.4) are included in the message.

3. AUSF sends the the Nudm\_UEAuthentication\_Get Request, containing SUCI and the serving network name, to UDM. The general rules for UDM selection apply.

4. The SIDF located within the UDM de-conceals the SUCI to SUPI if SUCI is received in the message. The UDM then selects the primary authentication method.

5. If the UDM chooses to use EAP-TLS, it sends the SUPI and an indicator to choose EAP-TLS to AUSF in the Nudm\_UEAuthentication\_Get Response.

6. With the received SUPI and the indicator, the AUSF chooses EAP-TLS as the authentication method. The AUSF sends thea Nausf\_UEAuthentication\_Authenticate Response message containing EAP-Request/EAP-TLS [TLS start] message to the SEAF.

7. The SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the UE. This message also includes the ngKSI and the ABBA parameter. In fact, the SEAF shall always 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.

8. After receiving the EAP-TLS [TLS-start] message from SEAF, the UE replies with an EAP-Response/EAP-TLS [client\_hello] to the SEAF in the Authentication Response message. The contents of TLS client\_hello are defined in the TLS specification of the TLS version in use.

NOTE1: The EAP framework supports negotiation of EAP methods. If the UE does not support EAP-TLS, it should follow the rule described in RFC 3748 [27] to negotiate another EAP method. In 5G system, UDM typically knows which EAP method and credentials are supported by the subscriber, and consequently EAP based negotiation may never be used.

9. The SEAF forwards the EAP-Response/EAP-TLS [client hello] message to AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

10. The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf\_UEAuthentication\_Authenticate Response, which further includes information elements such as server\_hello, server\_certificate, server\_key\_exchange, certificate\_request, server\_hello\_done. These information elements are defined in the RFCs for the corresponding TLS version in use.

11. The SEAF forwards the EAP-Request/EAP-TLS message with server\_hello and other information elements to the UE through Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

12. The UE authenticates the server with the received message from step 11.

NOTE 2: The UE is required to be pre-configured with a UE certificate and also certificates that can be used to verify server certificates.

13. If the TLS server authentication is successful, then the UE replies with EAP-Response/EAP-TLS in Authentication Response message, which further contains information element such as client\_certificate, client\_key\_exchange, client\_certificate\_verify, change\_cipher\_spec, client\_finished etc. Privacy considerations are described in Clause B.2.1.2.

14. The SEAF forwards the message with EAP-Response/EAP-TLS message with client\_certificate and other information elements to the AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

15. The AUSF authenticates the UE based on the message received. The AUSF verifies that the client certificate provided by the UE belongs to the subscriber identified by the SUPI. If there is a miss-match in the subscriber identifiers in the SUPI, the AUSF does not accept the client certificate. If the AUSF has successfully verified this message, the AUSF continues to step 16, otherwise it returns an EAP-failure.

NOTE 2: The AUSF is required to be pre-configured with the root or any intermediary CA certificates that can be used to verify UE certificates. Deployment of certificate revocation lists (CRLs) and online certificate status protocol (OCSP) are described in clause B.2.2.

16. The AUSF sends EAP-Request/EAP-TLS message with change\_cipher\_spec and server\_finished to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response.

17. The SEAF forwards EAP-Request/EAP-TLS message from step 16 to the UE with Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

18. The UE sends an empty EAP-TLS message to the SEAF in Authentication Response message.

19. The SEAF further forwards the EAP-Response/EAP-TLS message to the AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

20. The AUSF uses the most significant 256 bits of EMSK as the KAUSF and then calculates KSEAF from KAUSF as described in Annex A.6. The AUSF sends an EAP-Success message to the SEAF together with the SUPI and the derived anchor key in the Nausf\_UEAuthentication\_Authenticate Response.

21. The SEAF forwards the EAP-Success message to the UE in the NAS Security Mode Command message (thereby initiates the NAS security mode command procedure (see sub-clause 6.7.2)) and the authentication procedure is finished.. Then the SEAF derives the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7, and provides the ngKSI and the KAMF to the AMF.

On receiving the EAP-Success message, the UE derives EMSK and 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 derives the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 3: Void.

NOTE 4: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

NOTE 5: As an implementation option, the UE creates the temporary security context as described in step 21 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.

**\*\*\*\* End of Changes \*\*\*\***