**3GPP TSG-SA3 Meeting #102e *S3-210146***

**e-meeting, 18 – 29 January 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **1030** | **rev** | **-** | **Current version:** |  |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | f |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 11 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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:*** | The discussion paper S3-210144 discusses and highlight the issues for the scenario when a UE is registered to two different PLMNs via 3GPP access and non-3GPP access and the UE and the AUSF maintains a single Kausf for both accesses. This Kausf is used to protect SoR and UPU.  |
|  |  |
| ***Summary of change:*** | It is proposed to maintain Kausf and CounterSoR per serving PLMN when a UE is registered to two different PLMNs over 3GPP access and non-3GPP access. |
|  |  |
| ***Consequences if not approved:*** | The SoR and UPU transmission procedure will fail. |
|  |  |
| ***Clauses affected:*** | 6.1.2, 6.1.3.1, 6.1.3.2.0, 6.14.2.1, 6.14.2.2 and 6.15.2.1 |
|  |  |
|  | **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:*** |  |

**\*\*\*\* 1st CHANGE \*\*\*\***

#### 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, if the control plane solution for Steering of Roaming or UE Parameter Update procedures are supported by the HPLMN (see sections 6.14 and 6.15).

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.

**\*\*\*\* Next CHANGE \*\*\*\***

### 6.1.2 Initiation of authentication and selection of authentication method

The initiation of the primary authentication is shown in Figure 6.1.2-1.



Figure 6.1.2-1: Initiation of authentication procedure and selection of authentication method

The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

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].

The SEAF shall include the SUPI in the Nausf\_UEAuthentication\_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf\_UEAuthentication\_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf\_UEAuthentication\_Authenticate Request shall furthermore contain:

- the serving network name, as defined in sub-clause 6.1.1.4 of the present document.

NOTE 2: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs.

Upon receiving the Nausf\_UEAuthentication\_Authenticate Request message, the AUSF shall check that the requesting SEAF in the serving network is entitled to use the serving network name in the Nausf\_UEAuthentication\_Authenticate Request by comparing the serving network name with the expected serving network name. The AUSF shall store the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF shall respond with "serving network not authorized" in the Nausf\_UEAuthentication\_Authenticate Response.

The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;

- the serving network name;

Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

Based on SUPI, the UDM/ARPF shall choose the authentication method.

NOTE 3: The Nudm\_UEAuthentication\_Get Response in reply to the Nudm\_UEAuthentication\_Get Request and the Nausf\_UEAuthentication\_Authenticate Response message in reply to the Nausf\_UEAuthentication\_Authenticate Request message are described as part of the authentication procedures in clause 6.1.3.

### 6.1.3 Authentication procedures

#### 6.1.3.1 Authentication procedure for EAP-AKA'

EAP-AKA' is specified in RFC 5448 [12]. 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, 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 store KAUSF andthe SN Name, if Kausf is required by the operator for e.g, UPU and SoR. 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 store KAUSF andthe SN Name. 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.

**\*\*\*\* Next CHANGE \*\*\*\***

#### 6.1.3.2 Authentication procedure for 5G AKA

##### 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.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication 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 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. The UE shall store Kausf and SN-Name.

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 and the SN-Name, if Kausf is required by the operator for e.g. UPU or SoR. 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 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.

**\*\*\*\* Next 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. 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. The UDM shall include the SN-Name over which the UDM wants to send SoR. The AUSF shall use the KAUSF corresponding to the SN-Name to calculate SoR-MAC-IAUSF and SoR-MAC-IUE.

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.

**\*\*\*\* Next 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 include the SN-Name over which the UDM wants to send SoR. The AUSF shall use the KAUSF corresponding to the SN-Name to calculate SoR-MAC-IAUSF and SoR-MAC-IUE.

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.

**\*\*\*\* Next 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. 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 UDM includes the SN-name over which the UDM decided to send the UPU Data. The AUSF shall use KAUSF associated with the SN-name to calculate UPU-MAC-IAUSF.

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.

**\*\*\*\* CHANGE ENDS\*\*\*\***