**3GPP TSG-SA3 Meeting #100e *S3-202035***

**e-meeting, 17 -28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0941** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Storage of KAUSF in the UE and AUSF |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2020-08-07 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The UE can be registered in two serving networks simultanously. Primary authentication will take place over both serving networks. In this use case there are two different scenarios, either: A: one AUSF will handle the two serving networks; or B: two different AUSF(s) will handle the two serving networks (i.e. one AUSF handles one serving network). The selection of the KAUSF to store affects procedures such as SoR or UPU. The agreement between SA3 and CT4 after an exchange of LSes is that the latest KAUSF is stored.  |
|  |  |
| ***Summary of change:*** | The following is proposed:* The AUSF shall store the latest KAUSF after successful completion of the latest primary authentication.
* The ME shall store the latest KAUSF after successful completion of the latest primary authentication
* The UE shall store the KAUSF on either USIM or in non-volatile memory at deregistration and/or ME power off. The storage of the KAUSF in the USIM or in the non-volatile memory of the ME, allows that the latest generated KAUSF is available in the ME after deregistration and/or ME power off.
* The UE shall keep the KAUSF at handover or idle mode mobility from 5GS to EPS. This is, the KAUSF remains stored in the UE when the UE moves to EPS so that when the UE comes back to 5GS at handover or idle mode mobility from EPS to 5GS reusing the security context from EPS, the KAUSF stored in the UE can be used in 5GS.
* The latest KAUSF result of the successful completion of the latest primary authentication shall be stored and used by the UE and the HN regardless over which access network type (3GPP or non-3GPP) it was generated.

During the execution of e.g. SoR/UPU procedures, the UDM selects the AUSF that stores the latest KAUSF. |
|  |  |
| ***Consequences if not approved:*** | Unclear/incomplete specification.UE and HN may store and use different versions of KAUSF causing interoperability problems. |
|  |  |
| ***Clauses affected:*** | 6.1.1.1; 6.1.4.1; 6.2.2.1; 6.2.2.2; 6.3.2.1; 6.3.2.X (new), 6.14.1; 6.14.2.1; 6.14.2.2; 6.15.1; 6.15.2.1, 14.1.2.1 and 14.2.1.Y (new) |
|  |  |
|  | **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 e.g. 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.

**\*\*\*\* 2nd 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.

This procedure 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 UDM.

**\*\*\*\* 3rd 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 AUSF 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. If AUSF has an old KAUSF generated before the latest successful primary authentication, the AUSF shall replace the old KAUSF if any, with the new KAUSF generated in the latest successful primary authentication after the AUSF receives the Result Confirmation Response from UDM as specified in 6.1.4.1a.

NOTE X: Multiple KAUSF for a given UE may exist in different AUSFs of the HN e.g. if subsequent primary authentication procedures for the UE are executed using different AUSF instances.

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 K'AMF from KAMF for transfer to another AMF in inter-AMF mobility. The receiving AMF shall use K'AMF 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 K’AMF 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.

**\*\*\*\* 4th 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 KAUSF . The UE shall store the latest KAUSF after successful completion of the latest primary authentication. If the UE has an old KAUSF generated before the latest successful primary authentication,

the UE shall replace the old KAUSF value with the latest KAUSF. The UE shall store the latest KAUSF or replace the old KAUSF with the latest KAUSF after UE receives EAP success message in the case of EAP-AKA’ or after expiry of a timer which is started after sending RES\* in the case of 5G AKA. 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.

NOTE X: The storage of the KAUSF in the USIM or in the non-volatile memory of the ME, allows that the latest generated KAUSF is available in the ME after deregistration and/or ME power off.

The UE shall keep the KAUSF at handover or idle mode mobility from 5GS to EPS. This is, the KAUSF remains stored in the UE when the UE moves to EPS so that when the UE comes back to 5GS at handover or idle mode mobility from EPS to 5GS reusing the security context from EPS, the KAUSF stored in the UE can be used in 5GS.

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.

**\*\*\*\* 5th 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.

Editor's Note: It is FFS to define the event(s) that triggers the storage of the key in the ME or in the USIM. Also, the appropriate clause needs to be considered.

In this case, since two independent successful primary authentication procedures with the Home PLMN are executed, two KAUSF are generated. However, the KAUSF is not bound to the 5G security context and therefore the latest KAUSF result of the successful completion of the latest primary authentication shall be stored and used by the UE and the HN regardless over which access network type (3GPP or non-3GPP) it was generated.

**\*\*\*\* 6th 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 Steering Information List as well as the conditions for sending it to the UE are described in TS 23.122 [53] Annex C and are not repeated below. For example, the Steering Information List may include a list of preferred PLMN/access technology combinations or 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'.

**\*\*\*\* 7th CHANGE \*\*\*\***

#### 6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case when 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

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 Information, and obtains the list as descirbed in TS 23.122 [53].

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 reported the latest successful Nudm\_UEAuthentication\_ResultConfirmation service operation after successful completion of the latest primary authentication.

If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering Information List, then the UDM shall set the corresponding indication in the SoR header (see TS 24.501 [35]) and include the ACK Indication 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 details of the CounterSoR is specified in sub-clause 6.14.2.3 of this document. In case, the Steering Information List is not available or HPLMN determines that no steering of the UE is required, then the List indication valuein the SoR header shall be set to null and list shall not be included. The inclusion of list of preferred PLMN/access technology combinations (if provided) and the SoR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the Steering Information List received is not tampered with or removed by the VPLMN and if the UDM requested an acknowledgement. The expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering Information List.

10) The UDM responds to the Nudm\_SDM\_Get service operation to the VPLMN AMF, which shall include the SoR header, Steering Information List, 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 include the Steering Information List, the SoR-MAC-IAUSF, CounterSoR and the SoR header to the UE in the Registration Accept message;

12) On receiving the Registration Accept message, if the USIM is configured with the indication that the UE shall receive the Steering Information List, then 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 information, 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 Information List has been provided by the HPLMN in step 11, 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 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 transparent container in 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 Information List 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.

**\*\*\*\* 8th CHANGE \*\*\*\***

#### 6.14.2.2 Procedure for steering of UE in VPLMN 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

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

2-3) The UDM shall invoke Nausf\_SoRProtection service operation message by including the SoR header and Steering Information List 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 reported the latest successful Nudm\_UEAuthentication\_ResultConfirmation service operation after successful completion of the latest primary authentication.

If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering Information List, then the UDM shall set the corresponding indication in the SoR header (see TS 24.501 [35]) and include the ACK Indication 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 details of the CounterSoR is specified in sub-clause 6.14.2.3 of this document. The inclusion of Steering Information List and the acknowledge indication in the calculation of SoR-MAC-IAUSF allows the UE to verify that the Steering Information List received is not tampered with or removed by the VPLMN and if the UDM requested an acknowledgement. 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 Information.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which contains the list of preferred PLMN/access technology combinations, SoR-MAC-IAUSF, CounterSoR within the Access and Mobility Subscription data and the SoR header. 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 transparent container 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 information, the CounterSoR and the SoR header and verifies 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 List 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 transparent container in the UL NAS Transport message.

8) The AMF shall send a Nudm\_SDM\_Info request message to the UDM. If a transparent container with the SoR-MAC-IUE was received in the UL NAS Transport message, the AMF shall include the transparent container 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 Information List, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 4.

**\*\*\*\* 9th 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.

**\*\*\*\* 10th 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 reported the latest successful Nudm\_UEAuthentication\_ResultConfirmation service operation after successful completion of the latest primary authentication.

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.

**\*\*\*\* 11th CHANGE \*\*\*\***

### 14.1.2 Nausf\_UEAuthentication service

#### 14.1.2.1 Nausf\_UEAuthentication\_Authenticate service operation

**Service operation name:** Nausf\_UEAuthentication\_authenticate.

**Description:** Authenticate the UE and provides related keying material.

**Input, Required:** One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.

2. In the subsequent authentication requests depending on the authentication method:

a. 5G AKA: Authentication confirmation message with RES\* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS).

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

**Input, Optional:** None.

**Output, Required:** One of the options below.

1. Depending on the authentication method:

a. 5G AKA: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

**Output, Optional:** SUPI if the authentication was initiated with SUCI.

**\*\*\*\* END OF CHANGES \*\*\*\***