**3GPP TSG-SA3 Meeting #102-e *S3-21aabb***

**e-meeting, 18 - 29 January 2021, Online was S3-210415**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0963** | **rev** | **2** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Correcting notation used for inter-AMF mobility key derivation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | MediaTek Inc. | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2021-01-29 |
|  |  | | | |  | |  | | |  |
| ***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 can be 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:*** | | TS 33.501 is using two different notations for an intermediate AMF-key derived from KAMF/ KASME, hence it can be misunderstood that those intermediate key K'AMF and intermediate key KAMF' have different meaning e.g. different input parameters.  Terminology throughout 33.501 to be consistent. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Correcting notation of the intermediate AMF-key to be consistent KAMF'. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect notation used in the spec. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.2.1, 6.2.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

### 6.2.1 Key hierarchy

Requirements on 5GC and NG-RAN related to keys are described in clause 5.1.3. The following describes the keys of the key hierarchy generation in a 5GS in detail.:



Figure 6.2.1-1: Key hierarchy generation in 5GS

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

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

Keys for AUSF in home network:

- KAUSF is a key derived

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

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

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

Key for AMF in serving network:

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

Keys for NAS signalling:

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

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

Key for NG-RAN:

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

Keys for UP traffic:

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

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

Keys for RRC signalling:

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

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

Intermediate keys:

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

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

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

Key for the non-3GPP access:

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

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

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

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.