**3GPP TSG-SA3 Meeting #100-e *S3-201649***

**E-meeting, 17- 28 Aug 2020** Revision of S3-20xxxx

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | 883 | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Deletion of confusing text on KSEAF |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Huawei, HiSilicon, |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  5GS\_Ph1-SEC |  | ***Date:*** |  4-8-2020 |
|  |  |  |  |  |
| ***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:*** | TS 33.501 contains contradictory text, about deleting KSEAF immediately after the computation of KAMF, and also about transferring KSEAF during AMF context transfer. If KAMF, is derived, KSEAF should not be left undeleted. |
|  |  |
| ***Summary of change:*** | Delete the sentence “KSEAF shall not be forwarded to another AMF set. “ in clause 6.9.3 |
|  |  |
| ***Consequences if not approved:*** | Confusing specifications causes implementation mistakes. |
|  |  |
| ***Clauses affected:*** | 6.9.3 |
|  |  |
|  | **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 \*\*\*\***

### .9.3 Key handling in mobility registration update

The procedure shall be invoked by the target AMF after the receiving of a Registration Request message of type mobility registration update from the UE wherein the UE and the source AMF are identified by means of a temporary identifier 5G-GUTI.

The protocol steps for the source AMF and target AMF performing context transfer are as follows:

a) The target AMF sends a message to the source AMF, this message contains 5G-GUTI and the received Registration Request message.

b) The source AMF searches the data of the UE in the database and checks the integrity protection on the Registration Request message.

i) If the UE is found and the integrity check succeeds, when the source AMF does not change KAMF according to its local policy, the source AMF shall send a response back that:

- shall include the SUPI, and

- may include any current 5G security context it holds.

ii) If the UE is found and the integrity check succeeds, when the source AMF changes KAMF according to its local policy, the source AMF shall send a response back that:

- shall include the SUPI,

- keyAmfHDerivationInd, and

- may include a new 5G security context it derives from the current one it holds.

The source AMF subsequently deletes the 5G security context which it holds.

If the UE cannot be identified or the integrity check fails, then the source AMF shall send a response indicating that the temporary identifier 5G-GUTI cannot be retrieved.

c) If the target AMF receives a response with a SUPI, it creates an entry and stores the 5G security context that may have beenreceived .

If the target AMF receives a response indicating that the UE could not be identified, it shall initiate the subscription identification procedure described in clause 6.12.4 of the present document.

NOTE: Void.

NOTE X: The source AMF does not have KSEAF because it is deleted after KAMF derivation as per clause 6.2.2.1 and therefore the context transfer from the source AMF to the target AMF does not contain KSEAF.

At mobility registration update, the source AMF shall use local policy to determine whether to perform horizontal KAMF derivation. If the source AMF determines not to perform horizontal KAMF derivation, the source AMF shall transfer current security context to the target AMF. If the source AMF determines to perform horizontal KAMF derivation, the source AMF shall derive a new key KAMF from the currently active KAMF and the uplink NAS COUNT value in the received Registration Request message. The ngKSI for the newly derived KAMF key is defined such as the value field and the type field are taken from the ngKSI of the current KAMF. The source AMF shall transfer the new KAMF, the new ngKSI, the UE security capability, the keyAmfHDerivationInd to the target AMF. The key derivation of the new KAMF is specified in Annex A.13. If the source AMF has derived a new key KAMF, the source AMF shall not transfer the old KAMF to the target AMF and the source AMF shall in this case also delete any stored non-current 5G security context, and not transfer any non-current 5G security context to the target AMF.

When the target AMF receives the new KAMF together with the keyAmfHDerivationInd, then the target AMF shall decide whether to use the KAMF directly according to its local policy after receiving the response from the source AMF.

If the target AMF, according to its local policy, decides to not use the KAMF received from the source AMF, it can perform a re-authentication procedure to the UE to establish a new NAS security context.

If the target AMF decides to use the key KAMF received from source AMF (i.e., no re-authentication), it shall send the K\_AMF\_change\_flag set to 1 to the UE in the NAS SMC including replayed UE security capabilities, the selected NAS algorithms and the ngKSI for identifying the new KAMF from which the UE shall derive a new KAMF to establish a new NAS security context between the UE and target AMF.

The target AMF shall reset the NAS COUNTs to zero and derive new NAS keys (KNASint and KNASenc) from the new KAMF using the selected NAS algorithm identifiers as input. The target AMF shall integrity protect the NAS Security Mode Command message with the new KNASint key.

If the UE receives the  K\_AMF\_change\_flag set to 1 in the NAS Security Mode Command message, then the UE shall derive a new key KAMF from the current active KAMF identified by the received ngKSI in the NAS Security Mode Command message using the uplink NAS COUNT valuethat was sent in the Registration Request message. The UE shall assign the received ngKSI in the NAS Security Mode Command message to the ngKSI of the new derived KAMF. The UE shall derive new NAS keys (KNASint and KNASenc) from the new KAMF and integrity check the NAS Security Mode Command message using the new KNASint key.

The UE shall then derive a new initial KgNB from the new KAMF as specified in Annex A.9.

The UE shall associate the derived new initial KgNB with a new NCC value equal to zero and reset the NAS COUNTs to zero.

After the ongoing mobility registration procedure is successfully completed, the ME shall replace the currently stored KAMF and ngKSI values on both USIM and ME with the new KAMF and the associated ngKSI.

**\*\*\*\* END of CHANGE \*\*\*\***