**3GPP TSG-CT WG1 Meeting #137-eC1-22XXXX**

**E-meeting, 18th – 26th Aug 2022 revision of C1-224989**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4620** | **rev** | **1** | **Current version:** | **17.7.1** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Resolving EN on KSEAF derivation indicator in USIM | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-07-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | The following EN will be addressed in CT6 (see CR 0963 to TS 31.102) and is therefore no more needed:  *Editor’s Note [WI: eNPN, CR#4412]: The indication to use MSK requires extension of the related elementary file in USIM subject to CT6 agreement.* | | | | | | | | |
| ***;*** | |  | | | | | | | | |
| ***Summary of change:*** | | Remove EN [WI: eNPN, CR#4412].  Backward compatibility analysis  Backward compatible as only UE internal operation is impacted | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.1.2.2.3, 5.4.1.2.2.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS 31.102 CR 0963 | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Revision 1   * Set “Other spec affected” to Y * Additional editorial fixes in 5.4.1.2.2.3 | | | | | | | | |

\*\*\* First change \*\*\*

5.4.1.2.2.3 UE successfully authenticates network

If a USIM is present and the SNN check is successful, the UE shall handle the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40]. The USIM shall derive CK and IK and compute the authentication response (RES) using the 5G authentication challenge data received from the ME, and pass RES to the ME. The ME shall derive CK' and IK' from CK and IK, and if the UE operates in SNPN access operation mode and the credentials in the USIM contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then derive MSK from CK' and IK' otherwise derive EMSK from CK' and IK'.

Furthermore, if the UE operates in SNPN access operation mode and the credentials in the USIM contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then the ME may generate a new KAUSF from the MSK otherwise the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request/AKA'-challenge message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request/AKA'-challenge message in subclause 5.4.1.2.4.2 in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context, and shall send an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

NOTE: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

The ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

If the EAP-request/AKA'-challenge message contains AT\_RESULT\_IND attribute, the UE may include AT\_RESULT\_IND attribute in the EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

\*\*\* Next change \*\*\*

5.4.1.2.2.8 UE handling EAP-success message

Upon receiving an EAP-success message, the ME shall:

a) delete the valid KAUSF and the valid KSEAF, if any;

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context as described in subclause 5.4.1.2.2.3:

1) if the UE operates in SNPN access operation mode and the credentials in the USIM contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the new KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) consider the new KAUSF to be the valid KAUSF, and the new KSEAF to be the valid KSEAF, reset the SOR counter and the UE parameter update counter to zero, and store the valid KAUSF, the valid KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and use the valid KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received.

The UE shall consider the procedure complete.

\*\*\* End of changes \*\*\*