**3GPP TSG-SA3 Meeting #98e *S3-200386***

**e-meeting, 2 – 6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0768** | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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 | **x** | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarifications on authentication methods selection and key derivation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Interdigital | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Vertical\_LAN\_SEC | | | | |  | ***Date:*** | | | 6.3.2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **D** |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The referencing to Annex I for NPN has not been consequently applied in clause 6. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Modification of editor’s note to provide clear guidance for normative reference and example. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misleading specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | I.2.2, I.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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

### I.2.2 EAP framework, selection of authentication method, and EAP method credentials

The EAP authentication framework is supported by the 5GS as described in clause 6.1.1.2.

The UE and the serving network may support 5G AKA, EAP-AKA', or any other key-generating EAP authentication method.

Selection of the authentication methods is dependent on NPN configuration.

NOTE 1: For EAP-AKA' (as well as 5G AKA)- the selection is described in clause 6.1.2. For authentication that is not using EAP-AKA' (or 5G AKA), the selection is NPN operator deployment-specific and out of scope of this specification.

When an EAP authentication method other than EAP-AKA' is selected, the chosen method determines the credentials needed in the UE and network. These credentials, called the EAP-method credentials, shall be used for authentication.

NOTE 2: How credentials for EAP methods other than EAP-AKA' are stored and processed within the UE are out of the scope for standalone non-public networks.

NOTE 3: Storage and processing of credentials for EAP-AKA' (as well as 5G AKA) is described in clause 6 of the present document.

### I.2.3 Key hierarchy, key derivation and key distribution

The text in clauses 6.2.1 and 6.2.2 cannot apply directly for an EAP authentication method other than EAP-AKA' as these clauses assume that an AKA-based authentication method is used. The major differences are the way in which KAUSF is calculated and that the UDM/ARPF is not necessarily involved in the key derivation or distribution.

Depending on the selected authentication method, the KAUSF is generated as follows:

- For 5G AKA and EAP-AKA' refer to clause 6.2.1.

- When using a key-generating EAP authentication method other than EAP-AKA', the key derivation of KAUSF is based on the EAP-method credentials in the UE and AUSF and shall be done as shown in Figure I.2.3-1.

NOTE: For EAP authentication methods other than EAP-AKA', this key derivation replaces clauses 6.2.1 and 6.2.2 for the generation of KAUSF .



Figure I.2.3-1: KAUSF derivation for key-generating EAP authentication methods other than EAP-AKA'

KAUSF shall be derived by the AUSF and UE from the EMSK created by the EAP authentication as for EAP-AKA'.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the KAUSF downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from KAUSF (e.g. KSEAF, KAMF, KgNB etc) apply without modification.

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