3GPP TSG SA WG 3 Meeting SA3#102e TDoc S3-210459-r3

Electronic meeting, Online, 18 - 29 January 2021

**Title: [draft]** Reply LS on Storage of KAUSF

**Response to:** LS S3-210005/C1-207764 on Reply LS on Storage of KAUSF from CT1

**Source:** SA3

**To:** CT1

**Cc:**

**Contact person:** Rajavelsamy Rajadurai

Rajvel@]Samsung.com

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

# 1 Overall description

SA3 thanks CT1 for their LS on Storage of KAUSF (S3-210005/C1-207764).

In SA3#101e meeting, SA3 started the discussion on the issue, when the new KAUSF is stored at the UE as part of alignment with the CT4 specification for Rel-16. SA3 continued the discussion and agreed on the attached CR S3-210460 in the SA3#102e meeting, particularly changes to the clause 6.2.2.2 is relevant to this issue.

SA3 is considering a solution, where only after identifying that the primary (re)authentication is successful in the network side, the UE shall store the KAUSF, KSEAF, SOR counter and UE parameter update counter on the USIM (or in the non-volatile memory of the ME, if no corresponding file is present on the USIM). The UE identifies that the primary (re)authentication is successful in the network side, upon receiving a valid NAS SMC message.

SA2 would like to summarise the following additional details in handling the newly derived KAUSF :

* The UE on receiving a valid NAS SMC procedure (corresponding to the partial context derived from the newly generated Kausf) shall store the newly generated KAUSF as the latest KAUSF or replace the old KAUSF with the latest KAUSF.
* After successful primary authentication and before receiving the NAS SMC message from the network, the UE will hold the newly derived KAUSF key.
* It is mandatory for the AMF to initiate the NAS SMC procedure with the UE, immediately after the primary re-authentication.
* At any point of time, UE will have one stored Kausf and only one newly derived Kausf key (from most recent authentication) on hold, irrespective of the access technology.
* On receiving Authentication failure, the newly derived key which is on-hold is deleted.
* When UE is about to power off, then the newly derived KAUSF key (if any) will be replacing the stored KAUSF key.

The solution under consideration mandates performing NAS SMC procedure, after the successful run of primary authentication. On this new mandatory requirement under consideration, SA3 would like to have feedback from CT1, on the feasibility to perform NAS SMC procedure immediately after successful run of primary authentication.

SA3 would like to inform CT1 that the procedure described in Annex C of TS 24.501 to store KAUSF, KSEAF, SoR counter and UE parameter counter on the USIM (or in the non-volatile memory of the ME) is not complete. Clause C.2 of 3GPP TS 24.501 needs also to take into account the scenarios where there is a USIM in UE operating in SNPN access mode and the network is using EAP-AKA’ or 5G-AKA, as specified in 3GPP TS 33.501 clause I.2.2 and 3GPP TS 23.122 clause 4.9.3.0.

# 2 Actions

**To CT1**

**ACTION:** SA3 would like to kindly ask CT1 to take the above into account and provide feedback on the feasibility to perform NAS SMC procedure immediately after successful run of primary authentication.

# 3 Dates of next TSG SA WG 3 meetings

SA3#102e-Bis 1 - 5 March 2021 Electronic meeting

SA3#103e 17 - 28 may 2021 Electronic meeting