3GPP TSG SA WG 3 Meeting SA3#102e TDoc S3-210459-r1

Electronic meeting, Online, 18 - 29 January 2021

**Title:** 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**

**Attachments:** S3-210460.

# 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.

The guideline from SA3 is, 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.

SA3 discussed the following additional details in handling the newly derived KAUSF, and would like to share these details with CT1:

* 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.
* UE will hold only one newly derived key which is from the last authentication, irrespective of the access technology.
* On receiving Authentication failure, the newly derived key which is on-hold is deleted.
* The AMF performs the NAS SMC procedure after the primary re-authentication as soon as possible.
* If any partial context exist for the UE, then the AMF performs NAS SMC procedure before sending the DL NAS Transport message carrying the UPU/SOR transparent container.
* When UE is about to power off, then the newly derived KAUSF key (if any) will be replacing the old KAUSF key.

# 2 Actions

**To CT1**

**ACTION:** SA3 would like to kindly ask CT1 to take the above guidance into account. Further SA3 kindly request CT1 to provide any feedback if needed.

# 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