**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211510-r2***

e-meeting, 17 - 28 May 2021

**Title: Draft LS on Security risk evaluation of using long term key for another key derivation than AKA**

**Response to:**

**Release: Rel-17**

**Work Item: FS\_AUTH\_ENH**

**Source:** **SA3**

**To: ETSI SAGE**

**Contact person: Ranga Dhanasekaran**

 **ranganathan.mavureddi\_dhanasekaran (at) nokia-bell-labs.com**

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

**Attachments:** none

# 1 Overall description

SA3 performs an ongoing study on Authentication Enhancements and the results have been recorded in 3GPP TR 33.846.

Solution #2.8 in clause 6.2.8 of 3GPP TR 33.846 proposes the usage of the long term key K during the KSUCI derivation to derive a new key. SA3 had lengthy discussions whether this approach imposes a security risk.

SA3 would like to request ETSI SAGE to evaluate whether there is a security risk to derive a new key from the long-term key K for any new purposes different from the ones already specified for the AKA procedure and, in particular, in the context of solution #2.8.

# 2 Actions

**To ETSI SAGE**

**ACTION:** SA3 asks ETSI SAGE to evaluate whether there is a security risk to derive a new key from the long-term key K and provide the results to SA3.

# 3 Dates of next TSG SA WG 3 meetings

SA3#103Bis-e 5 - 9 ~July 2021 Electronic meeting (TBC)

SA3#104-e 16 - 27 August 2021 Electronic meeting