**3GPP TSG-CT WG3 Meeting #113eC3-210abc**

**E-Meeting, 25th – 29th January 2021**

**Title: LS on Lifetime expiry of AKMA application key**

**Response to: N/A**

**Release: Rel-17**

**Work Item: CT3 aspects of AKMA (AKMA-CT)**

**Source:** **CT3**

**To: SA3**

**Cc: CT1, CT4**

**Contact person: Narendranath Durga Tangudu**

 **n.tangudu@samsung.com**

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

**Attachments:** DP?

# 1 Overall description

As per Clause 6.4.1 of TS 33.535,

 *KAKMA shall be re-keyed by running a successful primary authentication as described in clause 6.1.*

When the KAF key life time expires, to refresh the KAF key using AKMA procedures, a new KAKMA needs to be used to generate a fresh KAF. To generate new KAKMA key, running a successful primary authentication is pre-requisite. It not clear how the AAnF can generate new KAKMA key when the KAUSF hasn’t changed.

CT3 has discussed further in the discussion paper C3-210186, on the possible solutions to address the above mentioned issue. In this context, CT3 would like to ask SA3 following questions:

Question 1): If Ua\* protocol doesn’t support KAF refresh, how the KAF is refreshed at KAF lifetime expiry, when the KAUSF did not change?

Question 2): Does SA3 see any security issue, if the UE or the Application Function provide information to the network to provide new KAF, which may trigger primary authentication if the KAUSF hasn’t changed?

# 2 Actions

**To SA3**

**ACTION:** 3GPP TSG CT WG3 asks SA3 to answer the above questions.

# 3 Dates of next TSG CT WG 3 meetings

3GPP TSG CT3#114e 24th February –5th March 2021 E-Meeting

3GPP TSG CT3#115e 14th -23rd April 2021 E-Meeting