**3GPP TSG-SA WG3 Meeting #101e *S3-203006-r4***

**E-meeting, 9-20 November 2020**

**Title: Draft LS to CT6 on clarification of NAS COUNTs storage in USIM**

**Release: R16**

**Work Item: 5G\_Ph1\_Sec**

**Source:** SA3

**To:** CT6

**Cc:**

**Contact Person:**

#### **Name:** Ivy Guo

E-mail Address: ivy\_guo@apple.com

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

**Attachments: S3-20xxxx (security requirement agreed by SA3)**

**1. Overall Description:**

SA3 identified a security issue resulting from storage of NAS COUNTs on USIM as specified in TS 31.102.

When UE has 2 accesses (3GPP access and non-3GPP access) in two different PLMNs simultaneously, SA3 requires that for each PLMN the UE is connected to, both NAS COUNT pairs (one pair for 3GPP access and another pair for non-3GPP access) for each NAS security context shall be stored in the USIM.

This is because even if a UE is currently not connected to one PLMN over non-3GPP access, the NAS COUNTs for that access may be non-zero from a previous use of the security context on that access. NAS COUNTs shall not be reset without rekeying, as otherwise keystream will be reused. A figure discussed in SA3 is quoted below for clarity, and not for any implementation guidance.



**Figure xxx: Full set of 5G NAS parameters on UE side and AMF side for an example PLMN-X**

SA3 clarified the security requirement in the attached CR S3-20xxxx.

Please also note that TS 23.501 Clause 5.3.2.4 ‘Support of a UE registered over both 3GPP and Non-3GPP access’ specifies how an AMF associates multiple access-specific RM contexts for an UE using a 5G-GUTI that is common to both 3GPP and Non-3GPP accesses.

SA3 kindly requests CT6 to check the TS 31.102 to align with the above GUTI storage requirement and take care about any backward compatibility that may arise due to the change.

**2. Actions:**

**ACTION**: SA3 kindly asks CT6 to take action on the above request and provide feedback accordingly.

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#101bis-e 12 – 16 January 2020 online

SA3#102-e 22 Feb– 5 March 2020 online