**3GPP TSG-SA3 Meeting #103-e *Draft r1 S3-211497***

e-meeting, 17 - 28 May 2021

**Title: DRAFT Response LS on 256-bit algorithms based on SNOW 3G or SNOW V**

**Response to: LS S3-211407 / SAGE (20) 14**

**Source: SA3 (Vodafone, Ericsson, AT&T, BT plc, Deutsche Telekom AG)**

**To: ETSI SAGE**

**Cc:**

**Contact person: Tim Evans**

**Tim.evans1@vodafone.com**

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

**Attachments:**

# 1 Overall description

SA3 thanks ETSI SAGE for their LS on 256-bit algorithms based on SNOW 3G or SNOW V, and the accompanying prototype algorithm specifications. SA3 has discussed the points raised and has come to the following conclusions:

* SA3 agrees that there is value in designing the integrity algorithm so that it can deliver at least a 64-bit MAC, even if that is not used straight away in 5G.
* SA3 notes SAGE’s advice that:
  + there are sound reasons to introduce at least two 256-bit algorithm sets at the same time, e.g. one based on AES and one based on a SNOW algorithm;
  + existing research on SNOW 3G shows that its security against some types of attack is significantly below the 256-bit level;
  + an independent analysis of SNOW V suggests that it comfortably resists known 256‑bit attack types
  + the partial reuse of AES building blocks in SNOW V is not a cause for concern
* SA3 believes that it is much more feasible to achieve the highest 5G speeds with SNOW V than with SNOW 3G; specifically, SA3 prefers 256-bit algorithms that achieve 20 Gbps peak rates both when implemented in hardware or software on commodity CPUs as stated as a performance aspect in TR 33.841
* SA3 therefore agrees with SAGE’s recommendation to proceed with the development of 256‑bit algorithm specifications based on SNOW V.

# 2 Actions

**To ETSI SAGE**

**ACTION:** SA3 kindly asks ETSI SAGE to proceed with the development of 256-bit encryption and integrity algorithm specifications based on SNOW V.

# 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