**3GPP TSG-SA3 Meeting #115 *draft\_S3-240838-r1***

**Athens, Greece, 26th February -1st March 2024**

**Title:** ReplyLS on AEAD mode of ZUC-256 Algorithm

**Response to:** S3-240262 LIAISON STATEMENT ON AEAD mode of ZUC-256 Algorithm

**Release:** Release 19

**Work Item:** 256\_Algo

**Source:** 3GPP SA3

**To:** ETSI SAGE

**Cc:** CCSA Wireless Communications Technical Committee (TC5) Security Working Group (WG5)

**Contact Person:**

#### Name: Rong Wu

E-mail Address: raina.wu@huawei.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 256-bit algorithm work in the past years.

It’s observed that 256-NCA1 (SNOW-5G) and 256-NCA2 (AES-256) in SAGE specification share the same framework, i.e. MAC generation core, for AEAD mode, which is different from that of 256-NCA3 (ZUC-256). SA3 would like to ask ETSI SAGE whether there would be an advantage of having diversity in MAC generation cores of AEAD mode, i.e. using a different MAC core in different ciphers in case problems should arise out of use of the particular MAC mode. In case there are no benefits arising out of MAC generation core diversity, SA3 would like to request ETSI SAGE to revise 256-NIA3 and 256-NCA3 algorithms (ZUC-based algorithms) to re-use the same MAC generation core as in 256-NCA1 and 256-NCA2 algorithms. It’s believed that this alignment would be beneficial for the implementation and performance of 256-NCA3/NIA3.

**2. Actions:**

**To ETSI SAGE**

**ACTION:** ETSI SAGE is kindly requested to take the above information into account and provide a new version for ZUC-256 algorithm or advise 3GPP SA3 about the diversity benefits.

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

SA3#115AdHoc-e 15 - 19 April 2024 Electronic meeting

SA3#116 20 - 24 May 2024 Jeju (South Korea)

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)