**3GPP TSG-SA3 Meeting #104-e *S3-213149***

e-meeting, 16 - 27 August 2021

**Title: draft LS on 256-bit algorithm based on ZUC**

**Source: SA3**

**To: ETSI SAGE**

**Cc:**

**Contact person: Haimei Wang**

**wanghaimei@caict.ac.cn**

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

# 1 Overall description

In SA3#104e meeting, the deployment of ZUC is discussed in S3-212676. To meet the requirement of market, SA3 has come to the following conclusions:

When proposing 256-bit algorithm sets for future consideration, it is recommended that AES, SNOW and ZUC based 256-bit algorithms to be prepared to keep consistency.

# 2 Actions

**To ETSI SAGE**

**ACTION:** SA3 kindly asks ETSI SAGE to proceed with the evaluation and development of 256-bit encryption and integrity algorithm specifications based on ZUC-256, as one of potential algorithms.

# 3 Dates of next TSG SA WG 3 meetings

SA3#105 8 - 12 November 2021 Sophia Antipolis, FR

SA3#106 7 - 11 February 2022 TBC, EU