**3GPP TSG-SA3 Meeting #115 *draft-S3-240999***

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

**Title: LS on AEAD modes**

**Response to:**

**Source: 3GPP** **SA3**

**To:** **ETSI SAGE**

**Cc: -**

**Contact person: Alf Zugenmaier**

**zugenmai@hm.edu**

**company: NTT DOCOMO**

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

**Attachments:** none

# 1 Overall description

In the context of standardizing 256 bit algorithms, SA3 would like to understand which security properties are guaranteed by the AEAD mode(s) used in the algorithm specification and which prerequisites need to be fulfilled.

# 2 Actions

**To ETSI SAGE**

**ACTION: 3GPP SA3 would kindly request ETSI SAGE to respond to the above question.**

# 3 Dates of next TSG SA WG 3 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)