**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241310-r5***

Electronic meeting, online, 15 - 19 April 2024 merger of S3-241310, S3-241275, S3-241390 and S3-241467

**Source: Huawei, HiSilicon, Xiaomi, Vivo, Ericsson**

**Title: Key Issue on introducing 256-bit algorithms in 5G system**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***Approve the pCR to TR 33.700-41.***

# 2 References

None

# 3 Rationale

Based on the discussion in SA3#115, there is no consensus on the length of long-term key impact. Thus, a note saying “the impact of long-term key’s length is not in the scope of this key issue” is added. The discussion on the long-term key can be treated separately.

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

# 4 Assumptions

The 5G System supports already procedures for the selection and activation of the AS and NAS security based on the UE security capabilities and network configuration. Using these procedures to negotiate the use of new 256-bit ciphering and integrity algorithms simply requires assigning an identity to these algorithms (which will then need to be reflected in other specifications).

The UE security capabilities IE is defined in TS 24.501 [4] clause 9.1.3.54. The IE includes already space for the introduction of new 5G algorithms, 4 for each type of algorithm (ciphering or integrity protection).

The NAS and AS SMC procedures described in TS 33.501 [3] in clauses 6.7.2 and 6.7.4 respectively enable the network and the UE to securely select and activate NAS and AS security based on the UE security capabilities and network configuration.

The UE security capabilities are sent to the network in an initial NAS message that can be unprotected. This is the reason why the 5G System supports a mechanism to protect against bidding down attacks by a man-in-the-middle tampering with the initial NAS message as pointed out in NOTE 1 of clause 6.7.2 of TS 33.501 [3]. This is the reason the UE security capabilities are replayed in the NAS SMC message.

Editor's Note: Further assumptions are ffs.

\*\*\* Start of 2nd Change \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[x] 3GPP TS 35.243: "Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G; Document 1: algorithm specification ".

[y] 3GPP TS 35.240: "Specification of the Snow 5G based 256-bits algorithm set: specification of the 256-NEA4 encryption, the 256-NIA4 integrity, and the 256-NCA4 authenticated encryption algorithm for 5G; Document 1: algorithm specification ".

[z] 3GPP TS 35.246: " Specification of the ZUC based 256-bits algorithm set: Specification of the 256-NEA6 encryption, the 256-NIA6 integrity, and the 256-NCA6 authenticated encryption algorithm for 5G; Document 1: algorithm specification".

\*\*\* End of 1st Change \*\*\*