**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241310-r6***

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.

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