**3GPP TSG-SA3 Meeting #115 *draft\_S3-240989-r1***

**Athens, Greece, 26th February – 1st March 2024 merger of** **S3‑240298,** **S3‑240492, S3‑240571, S3‑240769**

**Source: Huawei, HiSilicon**

**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

This contribution proposes a new key issue for enabling the use of the new 256-bit algorithms. The scope of this key issue includes the new algorithm identifiers, the input key to the algorithm interface, etc.

# 4 Detailed proposal

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

## 5.X Key Issue #X: Introducing 256-bit algorithms in 5G system

### 5.X.1 Key issue details

Currently, 5G system supports the use of 128-bit algorithms for encryption and integrity protection in AS and NAS layer. Supporting 256-bit cryptographic algorithms without using a 256-bit root key is pointless. Though current 5G architecture supports both 128-bit and 256-bit root key provisions, for the remainder of present document, it is assumed that both UE and the network are provisioned with shared symmetric 256-bit root keys and that AKA is based on 256-bit keys. To realize the standardized ciphering and integrity algorithms, the specific identifiers are assigned in the UE security capabilities. This will facilitate the selection on the network side once the security capabilities are received. The identifiers, are also used as yet another separation parameter when deriving the lower and final level keys.

Furthermore, while the 5G system supports already the derivation and transport of 256-bit keys, the keys that are input to the currently supported algorithms are truncated to 128 bits. The issue is whether to use the entire 256-bit keys or the least significant n (i.e., 128) bits of keys in the actual ciphering and integrity protection.

The scope of this key issue is to identify the necessary requirements and enhancements in order to enable the selection and usage of the new 256-bit algorithms in a similar manner to how it is currently done for the 128-bit algorithms.

### 5.X.2 Threats

**There are no threats related to this key issue since the transition from 128-bit algorithms to 256-bit algorithms does not mean that 128-bit algorithms are broken.**

### 5.X.3 Potential security requirements

The 5G system should support the means to select and use the new 256-bit algorithms in AS and NAS layers.

NOTE: whether the 256 algorithms are mandatory or optional to support is not in the scope of this key issue.

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