**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241310-r1***

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

**Source: Huawei, HiSilicon, Xiaomi**

**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 \*\*\*

## 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. 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.

AES based 256-bits algorithm set [x], Snow 5G based 256-bits algorithm set [y], and ZUC based 256-bits algorithm set [z] are planned to be used to protect the NAS/AS messages. Moreover, each algorithm set includes three categories of algorithm identities (i.e. encryption algorithm, integrity protection algorithm, authenticated encryption algorithm). The following issues need to be addressed.

1. How to indicate UE support of 256-bit algorithms (including encryption, integrity protection, and authenticated encryption algorithm).
2. Whether enhancements are needed on how to select the 256-bit algorithm on the network side.
3. How to indicate the selected 256-bit algorithm.

Authenticated encryption (AE) supports authentication and integrity protection simultaneously. The following AE-related issues need to be addressed.

1. According to TS 33.501 [3], 128-bit integrity/encryption algorithms used for NAS/AS protection are negotiated via NAS/AS SMC message, which is only integrity protected.If the AE is selected, the AE may encrypt the whole NAS/AS SMC message. How to negotiate NAS/AS algorithms using authenticated encryption algorithm in 5GS is not clear.
2. How to handle the case if the RRC selects an authenticated encryption algorithm, but UP protection only activates encryption or 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

**N/A.**

### 5.X.3 Potential security requirements

The 5G system should support the means to select and use the new 256-bit algorithms (including encryption, integrity protection, and authenticated encryption algorithm) in AS and NAS layers.

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

NOTE yy: the impact of long-term key’s length is not in the scope of this key issue.

\*\*\* 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 \*\*\*