**3GPP TSG-SA3 Meeting #116 *S3-24xxxx***

**Jeju, Korea 20 - 24 May 2024**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Discussion on the way forward**

**Document for: Discussion**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is proposed to discuss and agree on the proposed addition to the SID on 256-bit algorithms ([1]).***

# 2 References

[1] SP-231717, SID on enabling a cryptographic algorithm transition, FS\_CAT256.

[2] SP-231159, WID on Addition of 256-bit Algorithms

[3] TS 33.501, System Architecture

[4] TR 33.700-41, Study on enabling a cryptographic algorithm transition to 256-bits, Release 19

# 3 Rationale

As part of the initial SA3 discussions on the study to enable a cryptographic algorithm transition in Rel-19 ([1]), several specific aspects of the introduction of algorithms with a key length of 256-bit were discussed. Among them, the deployment and operational implications caused by the introduction of these new algorithms into an existing 5G system, that currently only supports 128-bit algorithms, were tackled.

We should consider that the introduction and the deployment of the 256-bit algorithms can only take place gradually in affordable steps:

- In a first step, we have specified the 256-bit algorithms [2].

- In a further step, we should study all the implications of the new introduced 256-bit algorithms in [2], and we should document them in a technical report [4]. One of those implications is the introduced 256-AEAD algorithm as base of 256-bit algorithms, such as 256-NEAx, 256-NIAx, 256-NCAx.

- In a final step, we should address the specific 256-bit deployment aspects in the specifications, such as the security architecture and procedures for 5G system [3].

In order to proceed with the study of the implications of the introduction of the new algorithms, we propose to look first at the distinctive features of the new 256-bit algorithms:



Figure 1: Clustering of Distinctive Features (example)

# 4 Detailed proposal

**Proposal#1:** Addition of a NOTE to the SID ([1]):

An addition should be inserted, which could read as follows:

“NOTE x: This study is intended to analyse and document the implications of the introduction of the 256-bit algorithms, but is not necessarily intended to lead to the introduction and the deployment of the 256-bit algorithms into the 3GPP specifications.”

**Proposal#2:** Update the SID with the adaptation of 256-AEAD algorithm.

**Proposal#3:** Reorganize the contents of the study to cover the distinctive features in an ordered and systematic approach. A proposal of clustering of features is provided as a concrete proposal.