**3GPP TSG-SA3 Meeting #115** ***S3-240321***

**Athens, Greece, 26 February - 1 March 2024**

**Source: KDDI Corporation**

**Title: Assumptions for TR 33.700-41**

**Document for: Approval**

**Agenda Item: 5.5 New Study on enabling a cryptographic algorithm transition to 256-bits**

# 1 Decision/action requested

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

# 2 References

[1] 3GPP TS 33.501

# 3 Rationale

This contribution lays out the security architecture assumptions for developing key issues related to the introduction of the 256-bit cryptographic algorithms into TS 33.501 [1]. It aims to present the assumed security architecture as well as analyze which potential threats can play a role and how these can be captured in key issues.

# 4 Detailed Proposal

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

# 4 Assumptions

## 4.1 Basis of the assumptions

All security architecture assumptions made in this document are based TS 33.501 [1] and the description of how the procedures work according to TS 33.501 [1]. The main purpose of the assumptions is to create a delta compared to TS 33.501 [1] that can be used to understand what threats are relevant for TS 33.501 for affected procedures.

## 4.2 Terminology

We introduce the following terminology:

* Legacy ME: A Release 18 (or earlier Release) UE.
* Updated ME: A higher than Release 18 UE.

## 4.3 Security Architecture Assumptions

### 4.3.1 Assumptions related to the introduction of 256-bit algorithms into the specifications

The assumptions below describe a ‘naïve’ introduction of the 256-bit algorithms in the specification. It is characterized by the minimum change to normative text in TS 33.501. This results in opportunistic use of 256-bit cryptographic algorithms.

Assumption 1: The 256-bit algorithms are added in the respective capability lists of the gNB, AMF, and UE when those algorithms are supported.

Assumption 2: The 128-bit algorithms is mandatory and 256-bit algorithms is optional in Release 19.

Assumption 4: No changes are made to the procedure to how UE security capabilities are communicated.

Assumption 5: No changes are made to how the gNB or AMF select the highest priority algorithm.

Assumption 6: Support for Legacy UEs and legacy gNBs and AMFs remains.

Assumption 7: The security architecture of the AS and NAS layer do not change.

Assumption 8: Operators will have the control over what algorithm prioirites should be applied to the system.

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