**3GPP TSG-SA3 Meeting #115** ***S3-241008***

**Athens, Greece, 26 February - 1 March 2024 revision of S3-240320**

**Source: KDDI Corporation**

**Title: Scope definition 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

[x] -

# 3 Rationale

This contribution proposes content for the scope section of the TR documenting the study on enabling a cryptographic algorithm transition to 256-bits.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

# Scope

This study aims to address key requirements for introducing support for 256-bit symmetric algorithms into the 5G System as well as the coexistence of 128-bit and 256-bit cryptographic algorithms. Considering findings and conclusions from preceding work, the following points should be addressed as part of this study:

- Studying key issues and candidate solutions concerning the negotiation (selection) of key sizes between UE and network, including:

- Potential risks and impacts to the current system when supporting both 128-bit and 256-bit algorithms in parallel and the adoption of 256-bit algorithms in existing deployments where 128 bits is already supported, e.g. handover scenarios within 5G system

- How to prioritise the use of 256-bit algorithms and mitigate bidding-down attacks when negotiating key sizes;

- How to ensure 256-bit security is achieved concerning varying levels of support for 256-bit algorithms by different UEs and within the network; potential dependencies in key-length selection of AS and NAS layers

- Study the implications and requirements for the key hierarchies to support 256-bit cryptographic algorithms

- Study the implications and requirements to AKA procedures.

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