**3GPP TSG-SA3 Meeting #116 *S3-*** ***242450-r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: KDDI Corporation**

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

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***For SA3 to accept the conclusions.***

# 2 References

# 3 Rationale

There was no progress in the past two meeting cycles of FS\_CAT256 study with no agreement on any key issues. Therefore, it is proposed to conclude the current study and enable the use of 256-bit cryptographic algorithms separately.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

# 7 Conclusions

During the study, the following aspects on introducing new 256-bit encryption and integrity protection algorithms were discussed:

- 256-bit security,

- relation with the long-term key and key hierarchy,

- impacts on Access Stratum (AS) and Non-Access Stratum (NAS) protocols,

- impacts on Dual Connectivity and Ultra-Reliable Low Latency Communications,

- impacts on RRC-Reconnection,

- impacts on handover and interworking mechanisms, and

* backward compatibility.

However, no key issues were agreed. It was concluded that there are currently no security threats to 128-NIA1,128-NIA2, 128-NIA3, 128-NEA1, 128-NEA2, 128-NEA3 specified in TS33.501[3] for the 5G System. The algorithm negotiation specified in TS33.501 already supports the adoption of new algorithms.

In future releases of the 3GPP system, the use of 256-bit keys will be supported. Additionally, AEAD mode may be supported as a new mechanism. This study does not conclude anything related to normative work for enabling the use of 256-bit keys. Moveover, the adoption of AEAD mode will be treated separately.

 \*\*\* End of 1st Change \*\*\*