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

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

**Source: KDDI Corporation**

**Title: DRAFT New Key Issue on different cryptographic key lengths on AS and NAS layer**

**Document for: Approval**

**Agenda Item: TBD**

# 1 Decision/action requested

***Approve the pCR to TR 33.700***

# 2 References

None

# 3 Rationale

This contribution proposes a new key issue related to different cryptographic key lengths on AS and NAS layer.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Different cryptographic key lengths on AS and NAS layer

### 5.X.1 Key issue details

As the 5G system transitions to 256-bit cryptographic algorithms, the situation may arise that a network deployment only partially supports 256-bits cryptographic algorithms, depending on the individual operators’ deployment status and configuration policy. That is, certain network elements are already upgraded to support 256-bit cryptographic algorithms, while others do not support them, yet, or will never support them.

In these scenarios, there is a risk of different key sizes being used for AS and NAS security in a single UE session, depending on the gNB and AMF the UE is connected to.Assuming a deployment in which the AMF already supports 256-bit cryptographic algorithms, but the gNB only supports 128-bit cryptographic algorithms (or vice versa), the UE connection is protected with cryptographic keys of different length on AS and NAS layer. This example poses a challenge to the UE and the network: What is the expected behaviour in such a mixed deployment scenario?

Additionally, this issue may also occur in 5G NSA deployments. While it is expected that the 5G System will transition to 256-bit cryptography at some point in time, the same may not be true for 4G/LTE. Hence, in 5G NSA deployments the situation arises that only the Radio Access Network supports 256-bits, while the Core Network does not (i.e., option 3, 3a, 3x) or vice versa (i.e., option 4, 4a, 7, 7a, 7x). For these scenarios, too, it is necessary to specify how network and UE are to behave.

### 5.X.2 Threats

**Unless gNB and AMF both support** 256-bit cryptographic algorithms, AS and NAS security may be protected with cryptographic keys of different length. Such discrepancies are undesirable from a security point of view.

### 5.X.3 Potential security requirements

The 5G System should be able to ensure uniform cryptographic key lengths for AS and NAS security.

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