**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 in dual connectivity scenarios**

**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 on different cryptographic key lengths in dual connectivity.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Different cryptographic key lengths in dual connectivity scenarios

### 5.X.1 Key issue details

The transition to 256-bit cryptographic algorithms may lead to network deployments that only partially support 256-bit cryptographic algorithms. In the context of dual connectivity, this means that there may be cases where not all RAN Nodes support cryptographic algorithms using 256-bit keys, e.g., because some of them have not been upgraded to a sufficiently recent Release, yet.

In these situations, there is a risk of inconsistent key sizes being used to protect different communication paths associated to a single subscriber session when using dual connectivity. Specifically, one can envisage a scenario in which the UE is connected to both a Master Node (MN) or Primary RAN and Secondary Node (SN) or Secondary RAN. Assuming a mixed deployment in which the MN already supports 256-bit cryptographic algorithms, but the SN only supports 128-bit cryptographic algorithms (or vice versa), the UE connection is protected with cryptographic keys of different length via the MN and SN.

This poses the question: In such a scenario, what is the expected behavior if consistent use of 256-bit security cannot be ensured?

### 5.X.2 Threats

The use of cryptographic algorithms with inconsistent key lengths could lead to different levels of protection on AS layer.

### 5.X.3 Potential security requirements

The 5G system should be able to ensure uniform cryptographic key lengths in dual connectivity scenarios.

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