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

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

**Source: KDDI Corporation**

**Title: DRAFT New Key Issue on insufficient long-term key length for 256-bit security**

**Document for: Approval**

**Agenda Item: TBD**

# 1 Decision/action requested

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

# 2 References

[1] 3GPP TS 31.102

# 3 Rationale

This contribution proposes a new key on insufficient long-term key length for 256-bit security.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Insufficient long-term key length for 256-bit security

### 5.X.1 Key issue details

According to TS 31.102 [1], it is still possible to provision current USIMs with long-term keys of 128-bit length. Regardless of their length, the long-term secret stored in the USIM and the UDM is used to derive CK an IK (and following child keys) of 256-bit length.

Assuming both sides support them, the UE and the network may agree on the use of 256-bit cryptographic algorithms for AS and/or NAS, even though the long-term secret is only 128 bits long. This creates an issue, because the long-term secret does not provide sufficient entropy. Thus, despite 256-bit keys being used on AS and/or NAS layer, the subscriber may not benefit from "true" 256-bit security.

### 5.X.2 Threats

256-bit cryptographic keys derived from a 128-bit secret do not provide "true" 256-bit security due to a lack of sufficient entropy.

### 5.X.3 Potential security requirements

256-bit cryptographic algorithms should be used only when the root keys are of 256-bit supported or higher.

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