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

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

**Source: KDDI Corporation**

**Title: DRAFT New Key Issue on biddown attacks during negotiation of cryptographic algorithms and key lengths**

**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 the secure negotiation of cryptographic algorithms and key lengths.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Biddown attacks during negotiation of cryptographic algorithms and key sizes

### 5.X.1 Key issue details

With the introduction of 256-bit cryptographic algorithms in the 5G System –in addition to the 128-bit algorithms currently used– it is expected that different cryptographic key lengths will need to be supported in parallel, both in UE and in the network. While 128-bit cryptographic algorithms are considered secure at the time of this study, it is prudent to consider future bid-down potential and study the secure negotiation of key lengths between the UE and the network.

*Note: The 5G System defines the Anti-bidding down Between Architectures (ABBA) parameter to prevent bidding down attacks between the network and the UE. However, for this parameter to be effective, dedicated values would need to be defined.*

### 5.X.2 Threats

Without negotiation of cryptographic algorithms and key length to be used for AS and NAS security, UE and network may each use different keys. If the UE and the network use different keys, connection establishment will fail.

If the algorithm negotiation between the UE and the network is not secured, the risk of bid-down attacks arises. If a bid down attack is successful, a UE and network supporting 256-bit security may agree on using 128-bit cryptographic algorithms, resulting in weaker cryptographic protection than available.

### 5.X.3 Potential security requirements

The UE and the gNB shall be able to securely negotiate cryptographic algorithms and key sizes to be used for AS security.

The UE and the AMF shall be able to securely negotiate cryptographic algorithms and key sizes to be used for NAS security.

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