**3GPP TSG-SA3 Meeting #115 *S3-241170***

**Electronic meeting, online, 16 April - 19 April 2024**

**Source: ZTE Corporation, Samsung**

**Title: New Key Issue on authentication parameters in AKA procedure**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is proposed to approve the key issue.***

# 2 References

[1] [S3‑235091](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_113_Chicago/docs/S3-235091.zip) New SID on study on enabling a cryptographic algorithm transition to 256 bits

[2] TS 33.501 Security architecture and procedures for 5G system.

[3] TS 33.102 3G Security; Security architecture (Release 17)

# 3 Rationale

Based on the objectives in [S3‑235091](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_113_Chicago/docs/S3-235091.zip) [1], it is proposed to study the implications and requirements to AKA procedures. According to TS 33.501 [2], in the current AKA procedure, both the authentication vector AV' for EAP-AKA' and 5G HE AV for 5G AKA are generated from AV (RAND || XRES || CK || IK || AUTN), where the length of each authentication parameter used in generating AV is specified in TS 33.102 [3]:

The random challenge (RAND) shall have a length of 128 bits.

Sequence numbers (SQN) shall have a length of 48 bits.

The anonymity key (AK) shall have a length of 48 bits.

The authentication management field (AMF) shall have a length of 16 bits.

The message authentication codes MAC in AUTN and MAC‑S in AUTS shall have a length of 64 bits.

The cipher key (CK) shall have a length of 128 bits.

The integrity key (IK) shall have a length of 128 bits.

The authentication response (RES) shall have a variable length of 4‑16 octets.

With the introduction of 256-bit long-term keys, the length of some parameters may be no longer suitable. For example, 128-bit CK and IK can not provide sufficient security strength when the long term key is 256 bits. How to revise the length of the authentication parameters to enhance the security strength and how to apply the authentication parameters with revised length in AKA procedures need to be further studied.

# 4 Detailed proposal

For SA3 to accept this proposal.

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

## 5.X Key Issue #X: Key Issue on authentication parameters in AKA procedure

### 5.X.1 Key issue details

According to TS 33.501, the long-term key could have a length of 128 bits or 256 bits. When the long-term key has a length of 256 bits, using the existing authentication parameters in AKA procedure can not achieve the desired security strength. It is necessary to determine the length of authentication parameters when 256-bit long-term key is used. For example, the CK and IK need to be 256-bit long to ensure sufficient entropy. Whether other parameters’ lengths need to be adjusted requires further study.

Meanwhile, the modification of parameter length will further influence the AKA procedures. For example, in the existing AKA procedure, the concatenation CK || IK of CK and IK is applied as the 256-bit input key to derive KAUSF. If CK and IK already have a length of 256 bits, whether the same mechanism can be applied to form the input key needs to be reconsidered.

### 5.X.2 Threats

N/A

### 5.X.3 Potential security requirements

The 5G System should support derivation of authentication parameters based on 256-bit long-term keys.

The 5G System should support key derivations in AKA procedures based on 256-bit long-term keys.

 \*\*\* End of 1st Change \*\*\*