**3GPP TSG-SA3 Meeting #115 *S3-240698-r2***

Athens, Greece, 26th February - 1st March 2024

**Source: Samsung, KDDI, THALES, Xiaomi**

**Title: Key Issue on insufficient entropy due to permanent secret key length (K)**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is proposed to approve this key issue on long-term key K entropy to study potential solutions.***

# 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] 3GPP TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 18)

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

[4] 3GPP TS 33.501 Security architecture and procedures for 5G system (Release 18)

[5] S3‑211408 Choice of cryptographic algorithm in 256-bit Milenage

[6] S3‑234134 Specification of Milenage-256 finalized

[7] 3GPP TS 35.231 A second example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 1: Algorithm specification

[8] IETF RFC 2104 Keyed-Hashing for Message Authentication

# 3 Rationale

In SA3#113 meeting, a SID to study on enabling a cryptographic algorithm transition to 256 bits was agreed. 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 challenges in supporting both 128 bits and 256 bits key.

According to the below excerpt from TS 31.102 [2], it is evident that the USIM supports subscription with permanent secret key length of 128 bits or 256 bits.

## 6.1 Authentication and key agreement procedure

…………

A permanent secret key K is used in this procedure. This key K has a length of 128 bits or 256 bits and is stored within the USIM for use in the algorithms described below. Also more than one secret key K can be stored in the USIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

………….

Following are the length of authentication parameters as specified in TS 33.102 [3].

………….

### 6.3.7 Length of authentication parameters

The authentication key (K) shall have a length of 128 bits or 256 bits.

NOTE: Examples of algorithm set for 3GPP authentication and key agreement functions allow either an authentication key K with only a length of 128 bits, or an authentication key K with a length of 128 bits or 256 bits. Depending on the chosen algorithm set, the operator may have the choice of the length of the authentication key K (128 bits or 256 bits).

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.

………….

According to the above excerpt, before introducing 256-bit algorithms (e.g., MILENAGE 256-bit algorithm set) to 5GS, CK and IK shall have a length of 128 bits (combining gives 256 bits). Further based on the key derivation and distribution as specified in clause 6.2.2 in TS 33.501 [4], NAS and AS keys are truncated to 128 bits for 128 bits algorithm. If UE and network negotiate and agree to use 256 bits security algorithm, the derived NAS and AS keys would be used without truncation.

Following are the scenarios when a permanent key (K) in the USIM has 256 bits or 128 bits key length, respectively:

**Permanent key length (K) is 256 bits**

If UE and network negotiate and agree to use either 256 bits or 128 bits security algorithm, it provides sufficient entropy in both cases.

**Permanent key length (K) is 128 bits**

If UE and network negotiate and agree to use 128 bits security algorithm, it provides sufficient entropy.

But in case if UE and network negotiate and agree to use 256 bits security algorithm, it does not provide sufficient entropy.

**Observation:** The security algorithm negotiation between UE and the network to select either 128 bits or 256 bits security algorithm without considering the permanent key length will result in insufficient entropy in case when 128 bits K is used and 256 bit algorithm is selected.

MILENAGE 256-bit algorithm set or Tuak algorithm set may be used by 3GPP operators. According to S3‑211408 [5] and S3‑234134 [6], for candidate MILENAGE 256-bit algorithm set, i.e. MILENAGE-256-R, provided by SAGE, CK/IK can be 256-bit, The Tuak algorithm supporting 256-bit K may also generate 256-bit CK and 256-bit IK as specified in TS 35.231 [7].

If MILENAGE-256-R or Tuak algorithm set is selected, the USIM/UDM/ARPF will generate 256-bit CK and 256-bit IK. In the current 5GS, the traditional ME /UDM/ARPF derives the KAUSF/CK'/IK' using 128-bit CK and 128-bit IK. Moreover, the input key of HMAC-SHA-256 can be any key with length longer or equal to the length of the HMAC-SHA-256 output (i.e. 256 bits). The following statement is captured from the IETF RFC 2104 [8], in which the L is the length of the HMAC-SHA-256 output.

Keys longer than L bytes are acceptable but the extra length would not significantly increase the function strength. (A longer key may be advisable if the randomness of the key is considered weak.)

# The mechanism to enable the ME/UDM/ARPF to support 256-bit CK/IK is not clear. 4 Detailed proposal

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[xx] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

\*\*\* Start of 2nd Change \*\*\*

## 5.X Key Issue #X: Key Issue on permanent secret key length (K)

### 5.X.1 Key issue details

**Permanent secret key length issue**

As per TS 33.501 [xx], the long-term key K length could be either 128 bits or 256 bits long. If the long-term key K length is 128 bits, then only 128 bits entropy is achieved even though 256 bits algorithm is used. Strength of the NAS/AS encryption/Integrity protection algorithms depends on the entropy of the long-term key K. Therefore, when the long-term key has a length of 128 bits, it does not have much gain to use 256 bits algorithm from the security perspective.

According to TS 33.501 [xx], the NAS and AS keys are truncated to 128 bits for 128 bits algorithm. If UE and the network negotiate and agree to use 256 bits algorithm, the derived NAS and AS keys would be used without truncation.

Following are the possible scenarios when a permanent key (K) in the USIM has 128 bits or 256 bits key length, respectively:

**Permanent key length (K) is 256 bits:**

If UE and network negotiate and agree to use either 256 bits or 128 bits security algorithm, it provides sufficient entropy in both cases.

**Permanent key length (K) is 128 bits:**

If UE and network negotiate and agree to use 128 bits security algorithm, it provides sufficient entropy.

But in case if UE and network negotiate and agree to use 256 bits security algorithm, it does not provide sufficient entropy.

Therefore, if it is 128 bits long-term key K, then only 128 bits security algorithm to be used and if the key length is 256 bits, then either 128 bits or 256 bits algorithm can be used.

**Security capability indication issue caused by the key length**

Currently, 5GS only supports the negotiation of 128-bit security algorithms. Specifically, 5GS uses the NAS SMC procedure to negotiate 128-bit security algorithm (e.g., 128-NEA1) with the UE for NAS security [xx]. The negotiation of 128-bit security algorithm (e.g., 128-NEA1) for AS security is achieved via the AS SMC procedure [xx].

256-bit security algorithms are planned to be introduced to the 5GS. In other words, a mechanism that supports negotiation of 128-bit/256-bit security algorithm shall be developed. Compared to traditional scenarios that only apply 128-bit long-term key K and 128-bit security algorithms, the following four possible cases need to be considered in 256-bit scenarios.

* 128-bit long-term key K in UICC, the ME supports both 128-bit security algorithms and 256-bit security algorithms
* 128-bit long-term key K in UICC, the ME only supports 128-bit security algorithms
* 256-bit long-term key K in UICC, the ME supports both 128-bit security algorithms and 256-bit security algorithms
* 256-bit long-term key K in UICC, the ME only supports 128-bit security algorithms

It is not clear how the UE indicates its support on the security algorithms during the algorithm negotiation procedure when UICC and the ME are different in terms of security level (e.g., 256-bit long-term key K in UICC, the ME only supports 128-bit security algorithms).

**256-bit CK/IK issue**

If MILENAGE-256-R or Tuak algorithm set is selected, the USIM/UDM/ARPF will generate 256-bit CK and 256-bit IK. However, how to enable the ME/UDM/ARPF to support 256-bit CK/IK is not clear.

### 5.X.2 Security threats

The security algorithm negotiation between UE and the network to select either 128 bits or 256 bits security algorithm without considering the permanent key length (K) will result in insufficient entropy in case when 128 bits K is used and 256 bit algorithm is selected. To achieve 256 bits entropy or the strength of the 256 bits algorithm, the root key needs to be 256 bits length. If the 128 bits key is used, then use of 256 bits algorithm is of no use from security perspective and results in additional computation and latency.

Algorithm for NAS/AS security negotiated between the UE and network may not correctly reflect the security level of the UE when UICC and the ME are different in terms of security level.

If the mechanism to derive KAUSF/CK'/IK' with 256-bit CK/IK rather than 128-bit CK/IK is not clear, the AKA procedures cannot be completed.

### 5.X.3 Potential security requirements

The 5G system shall support the negotiation of security algorithm (either 128 bits or 256 bits) based on the permanent secret key length (K).

Based on operator policy, 256-bit cryptographic algorithms should be used only when the long-term keys are of 256-bit length or higher.

5GS shall be able to support the negotiation of applicable security algorithm for NAS/AS security when UICC and the ME are different in terms of security level.

5GS shall be able to support deriving KAUSF/CK'/IK' based on 256-bit CK and the 256-bit IK.

\*\*\* End of Changes \*\*\*