**3GPP TSG-SA3 Meeting #108Adhoc-e S3-222696**

**e-meeting, 10th – 14th October, 2022**

**Source: China Telecom**

**Title: New solution on Key issue #1**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***This document proposes to add a new solution on key issue #1.***

# 2 References

[1] 3GPP TS 33.870: "Study of privacy of identifiers over radio access".

[2] 3GPP TS 23.003: "Numbering, addressing and identification".

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

# 3 Rationale

The Key Issue#1 in 33.870[1] has already proposed that some networks may decide to allow user identifiers with variable length, e.g. in case SUPI of type NAI. If an attacker can learn something about the length, this will reduce the size of the anonymity set.The length can become visible to an attacker in case a length preserving encryption scheme is being used for identifier concealment. An attacker on the air interface can identify and track subscribers with unusual lengths of the username field of variable-length SUPI in NAI format even if it is confidentiality protected (e.g., relatively short or long SUPIs).

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

## 6.X Solution #X: Concealing length of SUPIs in SUCIs by truncating the SUPIs

### 6.X.1 Introduction

Editor’s Note: This solution may need to be updated to align with the KI once the ENs in the KI is resolved.

This is a solution to KI #1, using truancation of SUPIs.

### 6.X.2 Solution details

Edtor’s Note: The exact way that this solution addresses requirements in KI#1 needs to be elaborated in detail.

#### 6.X.2.1 UE Side

UE shall truancate the username portion before encrypting it using ECIES.

Truancation of SUPIs in NAI format shall be performed by the same component, either USIM or ME that performs the calculation of SUCI in the following manner:

* Encrypt username portion using byte-encode, e.g. ASCII.
* Choose one kind of the bytes (e.g. 0-F in [hexadecimal](javascript:;)) by the random number generator.
* Delete the corresponding byte chosen before on the corresponding positions and record.
* Encrypt the truancated SUPI using ECIES.

NOTE 1: SUPI in IMSI format is not truncated because it is fixed length.

NOTE 2: The UE shall not truancate the SUPI in NAI format when using the null scheme.

#### 6.X.2.2 Home Network Side

The UDM invokes the SIDF to de-conceal the SUCI to the truancated SUPI. The UDM restores the original SUPI according to the record.

### 6.X.3 Evaluation

TBD

Edtor’s Note: It is FFS whether the SUPI truncation leads to the loss of meaningful NAI username information.

\*\*\* END OF CHANGE \*\*\*