**3GPP TSG-SA3 Meeting #107-e *S3-220759-r1***

**e-meeting, 16 - 20 May 2022**

**Source: China Southern Power Grid Co., Ltd, ZTE**

**Title: new solution on Key issue: SUPI length disclosed by SUCI**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***This document proposes to add a new solution on key issue: SUPI length disclosed by SUCI. SA3 is kindly requested to approve this doc.***

# 2 References

[1] 3GPP TR 33.870 v0.1.0

# 3 Rationale

The problem of poor anonymity SUCI is addressed in key issue:SUPI length disclosed by SUCI. This new solution proposes to provide a padding mechanism to protect the privacy of variable length SUPIs in NAI format.

# 4 Detailed proposal

\*\*\*\* START OF CHANGE \*\*\*\*

## 6.A Solution #A: Padding SUPI in NAI format to conceal the username length

### 6.A.1 Introduction

This solution addresses key issue #1.

### 6.A.2 Solution details

To conceal the username length leaked by SUCI and make it harder for an attacker to distinguish SUCIs based on their lengths, it is proposed to pad the plaintext identifier before encryption with a fixed or variable-length padding octets behind or before the username.

There are a variety of padding schemes such as block-length, random length padding, etc. Details of the SUPI padding mechanism may depend on the network operator and other deployment preferences..

Edtor’s Note: The details of this solution, e.g., call flow details, are FFS.

### 6.A.3 Evaluation

Edtor’s Note: The evaluation is FFS.

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