**3GPP TSG-SA3 Meeting #107e AdHoc *S3-221431-r2***

**e-meeting, 27 June - 1 July 2022**

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

**Title: SUPI padding 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: privacy aspects of variable length user identifiers. SA3 is kindly requested to approve this doc.***

# 2 References

[1] 3GPP TR 33.870 v0.2.0

# 3 Rationale

The problem of anonymity set reduction is addressed in key issue:Privacy aspects of variable length user identifiers [1]. 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 the key issue #1: padding SUPI in NAI format to conceal the username length .

### 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 before encryption with variable-length of 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.



Figure xx: authentication procedure when SUPI padding is used.

If UE and the network decide to use SUPI padding method to conceal the username length in NAT format. The original SUPI and plaintext are pre-configured in both USIM and UDM.

1. The UE sends the Registration Request message to the AMF/SEAF containing SUCI, and the SUCI includes SUPI Type, Home Network Identifier, Routing Indicator, Protection Scheme Identifier, Home Network Public Key Identifier and Scheme Output. The Cipher value text in Scheme Output of SUCI is the encryption of SUPI in NAI format and plaintext.

2. The SEAF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message containing the SUCI to the AUSF.

3. The Nudm\_UEAuthentication\_Get Request containing SUCI is sent from AUSF to UDM.

4. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF (Subscriber Identity De-concealing Function) to de-conceal the SUCI to obtain (e.g. determine) the SUPI with plaintext. If the SUPI is found in the database of the UDM, the UDM can compare the plaintext to get the username of SUPI without padding..

5. If SUPI with plaintext are found in the database of the UDM, the UDM selects the authentication method according to the SUPI. Then, the UDM generates the authentication data including authentication vector and sends it to AUSF in the Nudm\_UEAuthentication\_Get Response message with "200 OK". If SUPI is not found in the database, the UDM returns "404 Not Found" with "USER\_NOT\_FOUND" in the Nudm\_UEAuthentication\_Get Response message.

6. Upon reception of "200 OK", , the AUSF sends "201 Created" to AMF/SEAF with UEAuthentictionCtx containing authentication vector in the Nausf\_UEAuthentication\_Authenticate Response message. Upon reception of "404 Not Found", the AUSF sends "404 Not Found" to AMF/SEAF with "USER\_NOT\_FOUND".

7. The AMF/SEAF sends RAND and AUTN to the UE in the Authentication Request message in the case of "201 Created". Otherwise, the AMF/SEAF sends the Registration Reject message with Cause#3 to the UE in the case of "404 Not Found".

### 6.A.3 Evaluation

Edtor’s Note: evaluation is FFS.

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