**3GPP TSG-SA3 Meeting #107-e *S3-220911***

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

**Source:**  **Ericsson, Apple, AT&T, Cable Labs, China Southern Power Grid Co, Convida Wireless LLC, Intel, Interdigital, Johns Hopkins University APL, Lenovo, LGE, Mavenir, MITRE, NCSC, Oppo, Phillips, Samsung, Telefonica, US NIST, US NSA, Verizon Wireless, Xiaomi, ZTE, NTT DOCOMO**

**Title:** **New key issue on SUPI length disclosed by SUCI**

**Document for: Approval**

**Agenda Item:** **5.6**

# 1 Decision/action requested

***It is proposed to approve the key issue described in this document.***

# 2 References

[1] 3GPP TS 23.003: "Numbering, addressing and identification".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[3] Mihir Bellare, A. Desai, E. Jokipii, Phillip Rogaway: "A concrete security treatment of symmetric encryption ".

# 3 Rationale

According to TS 23.003 [1], subscribers’ permanent identifiers, called SUPIs, are allowed to be in Network Access Identifier (NAI) format -- username@realm. SUPIs can have significantly different lengths.

Using the Elliptic Curve Integrated Encryption Scheme (ECIES), a user device and the home network agree on a shared key by leveraging the public key of the home network. The user device uses the shared key in a symmetric encryption scheme (AES in counter mode) to encrypt SUPIs, into concealed identifiers, called SUCIs [2].

In the symmetric-key setup, security notions like real-or-random, left-or-right, or semantic security are defined in the context where plaintexts have the same lengths [3]. Though AES counter mode is secure according to these notions, direct use of it is not sufficient to serve an intended purpose of SUCIs -- indistinguishability of SUCIs. This is because SUPIs can have different lengths, and in counter mode, the length of the plaintext and the corresponding ciphertext is the same. Therefore, when two SUPIs have different lengths, their ciphertexts are distinguishable from each other. Also, SUCIs that have rare lengths are easily recognisable.

# 4 Detailed proposal

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

## 5.X Key issue: Privacy aspects of variable length user identifiers

### 5.X.1 Key issue details

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.

### 5.X.2 Security threats

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 confidentiality protected(e.g., relatively short or long SUPIs).

Note: NAIs can be used for any EAP method.

If such an unusual length of the username field is unique to a single subscriber, an adversary may be able to uniquely attribute to that subscriber.

If there is a group of subscribers with unusual lengths of username fields in their SUPIs, the attacker may be able to infer the membership of those subscribers in such group.

### 5.X.3 Potential security requirements

 The 5G system should protect against anonymity set reduction based on identifier length.

\*\*\* END OF CHANGES \*\*\*