**3GPP TSG-SA3 Meeting #108-Bis-e *draft\_S3-222927-r1***

**e-meeting, 10 - 14 October 2022** *revision of S3-222570*

**Source: Interdigital, Apple, AT&T, CableLabs, Convida Wireless, Deutsche Telekom, Ericsson, Intel, JHU, Google, Lenovo, Nokia, NCSC, Oppo, Philips International B.V., US NIST, US NSA, Verizon, Xiaomi, ZTE**

**Title: PCR for KI #1: Privacy aspects of variable length user identifiers**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***This document proposes cleanup to key issue #1: Privacy aspects of variable length user identifiers. SA3 is kindly requested to approve this document.***

# 2 References

[1] 3GPP TR 33.870 v0.1.0

# 3 Rationale

This PCR addresses three editor’s notes in KI #1.

Main reasons:

Backward Compatibility: Since Rel-16, subscriptions (e.g., NPN subscriptions) have already been assigned NAI SUPIs of variable and unequal length that reflect the names that the end-users of those NPN subscriptions are using. If we assume that operators will now move to a scheme where usernames are all of equal length, then this would require users to be assigned new SUPIs when they upgrade devices. The 3GPP will study and ultimately propose a solution that will allow to preserve already-assigned meaningful username IEs of SUPI in the NAI format.

Flexibility and preserving operators’ choice: Variable length username allows MNOs to take advantage of the flexibility of the NAI SUPI format. In many cases, MNOs use SUPIs that are provided by the NPN owners and would prefer to have variable-length usernames that won’t leak private information, i.e., a 3GPP-developed solution instead of managing the "username" field.

Editor’s Notes in clauses 5.1.2 and 5.1.3 are redundant. 3GPP is contribution-driven and new threats and requirements can be added upon contributing with or without having such Editor’s Notes.

Additional reasoning and information to support this proposal are in the accompanying discussion paper in S3-222580.

# 4 Detailed proposal

\*\*\*\* START OF CHANGE 1 \*\*\*\*

## 5.1 Key issue #1: Privacy aspects of variable length user identifiers

### 5.1.1 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.

NPN networks are a deployment scenario where NAI based SUPI may be used while the use of IMSI based SUPI is also allowed.

In such deployments, SUPI privacy may be provided using one of the following methods

1. Standardized non-null schemes (i.e., profile A & B in TS 33.501) which require the presence of USIM
2. Method of SUPI protection using secondary messages (i.e., eap-based protection of SUPI) instead of e.g., NAS messages carrying protected SUPI. Anonymous SUCI use in TLS 1.2 and TLS 1.3 are examples of such protection method
3. Proprietary schemes as per TS 33.501

Operators may prefer to have a standardized solution for SUPI in NAI format privacy to achieve the following:

- preserving the privacy of SUPI in NAI format and remedying privacy leakage.

- ensuring backwards compatibility with e.g., SUPIs used for NPN subscriptions, that were deployed used before the username leakage vulnerability was discovered.

### 5.1.2 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 is 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 it 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 a group.

### 5.1.3 Potential security requirements

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

\*\*\*\* END OF CHANGE 1 \*\*\*\*