**3GPP TSG-SA3 Meeting #115 *Adhoc-e S3-241115***

**15 April - 16 April 2024**

**Source: IIT Delhi, IIT Bhilai**

**Title: New solution on SUPI privacy issue in PLMN hosting NPN Scenario**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***Approve the pCR to TR 33.757***

# 2 References

1. 3GPP TS 33.501, “Security architecture and procedures for 5G system.”

# 3 Rationale

This contribution proposes a new solution for TR 33.757.

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

## 6.Y Solution #Y: SUPI privacy in PLMN hosting NPN scenario

### 6.Y.1 Introduction

This solution addresses the security requirement in key issue#3 on the SUPI privacy issue in PLMN hosting NPN scenario.

### 6.Y.2 Solution details

After obtaining the SUPI from SUCI, UDM in the operator side generates a Virtual SUPI corresponding to the original SUPI and keeps this mapping table. Once the SUPI is obtained by the UDM, Virtual SUPIs are derived from it using cryptographic techniques. These techniques are designed to create temporary and pseudonymous identifiers that can be used in place of the actual SUPI during communication sessions. Virtual SUPIs are temporary in nature and are often used for specific communication sessions or transactions. They are not meant to be permanent identifiers and are regenerated or changed periodically to enhance security. Virtual SUPIs are typically randomized and encrypted to ensure that they cannot be easily reverse-engineered or linked back to the original SUPI. This randomization adds an extra layer of security and privacy, making it difficult for unauthorized parties to track or identify subscribers based on their Virtual SUPIs alone. During communication sessions, the Virtual SUPI is used instead of the actual SUPI to protect the subscriber's identity and prevent potential attacks or unauthorized access.

After the successful primary authentication procedure as mentioned in clause 6.1.3.2 [1], here in this solution, the Home Network (HN) sends the anchor key K\_SEAF along with Virtual SUPI instead of the original SUPI. AMF in the customer premises generates GUTI corresponding to this Virtual SUPI and keeps this Virtual SUPI to GUTI mapping.



**Fig 1: Solution-Virtual SUPI**

### 6.Y.3 Evaluation

Virtual SUPI is an extension of SUPI designed to enhance privacy and security in 5G networks. Virtual SUPI works by creating temporary identifiers that can be used instead of the actual SUPI during communication sessions. This helps in preventing the exposure of the real SUPI to unauthorized parties. By using Virtual SUPIs, operators can add an extra layer of security and privacy to their networks, reducing the risk of identity theft or unauthorized tracking of subscribers.

Virtual SUPIs are temporary and can change periodically. UE must be capable of handling these changes and updating their identifiers as needed to maintain secure and reliable communication with the network.

Editor's Note: "This solution has UE impact, how to avoid UE impact is FFS.

 Need for this solution: Virtual-SUPI ensures confidentiality, compliance, trust, data minimization, and subscriber’s right, hence this solution ensures SUPI privacy in PLMN hosting NPN Scenario.”

\*\*\* End of 1st Change \*\*\*