**3GPP TSG-SA3 Meeting #124 S3-253838-r2**

**Wuhan, China, 13 – 17 October 2025**

**Source: Huawei, HiSilicon**

**Title: New solution for SUCI Calculation - SUPI pseudonym**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

It is proposed to approve the following solution for SUCI calculation in the TR 33.703.

\* \* \* First Change \* \* \* \*

#### 7.2.1.Y Solution #Y to Protocol #1: SUPI Pseudonym

##### 7.2.1.Y.1 Introduction

This contribution proposes SUPI concealment using pseudonym instead of asymmetric encryption for SUPI.

##### 7.2.1.Y.2 Solution details

The Figure 7.2.1.Y.2-1 illustrates the procedure:

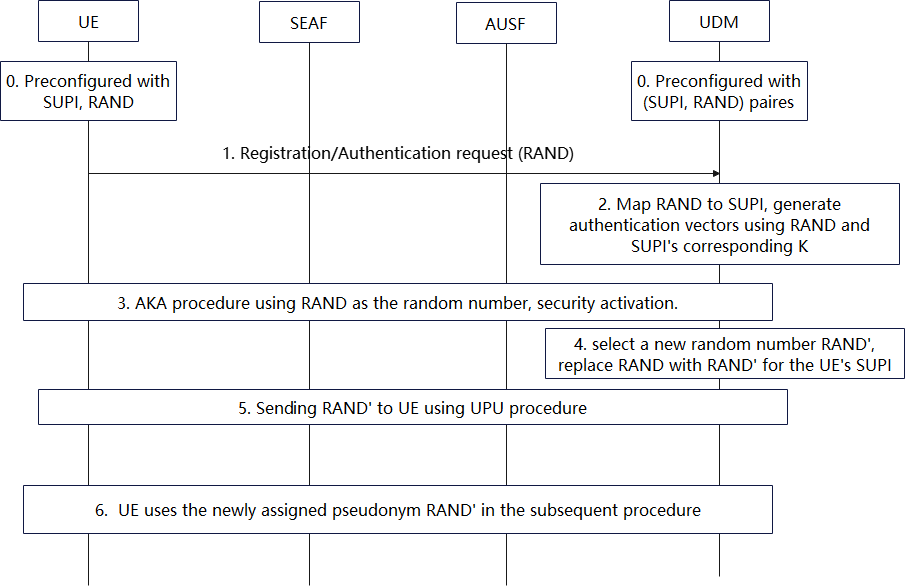


Figure 7.2.1.Y.2-1 procedure of using random number to do SUPI concealment

0. The UE and the UDM are pre-configured with the UE’s SUPI and a pseudonym, i.e., a random value RAND.

1. During registration, the UE uses the preconfigured pseudonym RAND as the UE's SUCI sent over the air interface.

2-3. The UDM/AUSF maps the pseudonym RAND to SUPI and complete the authentication using the SUPI. The RAND can also be reused as the RAND in the primary authentication.

4-5. After authentication, the UDM assigns a new pseudonym RAND' for the SUPI and sends it to the UE.

6. The UE uses the newly assigned pseudonym RAND' in the subsequent procedure.

Editor’s Note: it is ffs that RAND without binding to any UE specific key or encryption or MAC value will result in the attacker is just sending and RAND number blocking the genuine UE.

Editor’s Note: it is ffs that just the RAND can’t be used for routing of the information.

Editor’s Note: How does pre-configured pseudonym prevent traceability is FFS.

##### 7.2.1.Y.3 Evaluation

TBD

\* \* \* End of Changes \* \* \* \*