**3GPP TSG SA WG3 (Security) Meeting SA3#102-e S3-210321-r1**

**e-meeting, 18– 29 January 2021** *revision of S3-210321*

**Source: China Mobile**

**Title: Solution to address the Key issue #2.2 in TR 33.846**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***The pCR proposes a solution to address the key issue#2.2 regarding SUCI Replay, and is kindly asked to be approved by SA3.***

# 2 Reference

[1] TR 33.846 v 0.8.0, Study on authentication enhancements in 5G System.

# 3 Rationale

The SUCI replay attack shall be mitgated as it has various potential threats. In this contribution, we propose a method based on the public key of UE to address the SUCI replay attack.

Usually there are two ways to mitgate the replay attack: counter-based and nonce-based scheme. For the counter-based scheme, the receiver determines whether the message is a replay attack based on the value of counter. The complexity of the this scheme is that sender and receiver have to maintain the counter and deal with the asynchronization of the counter. The nonce-based scheme is relatively simple, the senders generate a random number that is never used (nonce) and sends it algong with the message, the receiver checks the nonce and determins whether it is a replay attack. There is no need to maintain the state between the sender and receiver.

A UE converts its SUPI into the SUCI by using ECIES scheme. For this, the UE generates a random number as the private key, and derives the public key from the private key. The UE’s public key is included in the SUCI and transimitted to the UDM. To identitfy whether the SUCI message is a replay message or not, the UDM checks whether the UE’s public key has been presented in the database of the UDM. If the UE’s public key can not be found by the UDM, the UDM can determin that the received SUCI message is not a replay message, and store this public key in the database; otherwise, the UDM is confronted with a replay attack, and acknowleges UE with an error message.

UE's public key is a random number that varies within the range of [0, 2n], where n is the length of the UE's public key. The probability that the UE generates the same public key is 1/2n. The length of the UE's public key is usually greater than or equal to 256 bits, so it is plausible to apply UE's public key to address the SUCI replay attack. The proposed scheme is actually a nonce-based scheme as it used the public key in the SUCI as the nonce.

The proposed method does not impact on current standardized SUPI protection scheme. It also does not need any change on the UE and the network. The only change required is that the UDM has to store the received UE's public key after determining that the SUCI is not a replay message.

The proposed method prevents the linkablity attack as it can identify the replay attack without returning the RAND and AUTN to the attacker. The possible DoS attack is also mitgated as it does not invoke the computation heavy ECIES algorithm before determining whether the SUCI is a replay message or not.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.2.X Solution #2.X: Mitigate the SUCI replay based on UE's public key

#### 6.2.X.1 Introduction

This solution addresses key issue #2.2: SUCI replay attack.

#### 6.2.X.2 Solution details

The proposed solution has the following steps.

1. UE applies the ECIES scheme to conceal SUPI according to TS 33.501 to generate SUCI which contains the UE's public key, and delivers the SUCI to the UDM.
2. The UDM exploits the received UE's public key to query on the database of the UDM. If it is found, the SUCI is judged as a replay message. If it is not found, the UDM stores it on the database, de-conceals the SUCI o get SUPI and acknowledges the UE with the generated authentication vector.

Note: The SUCI will be stored in the UE for 60s after it is generated.

Editor’s Note: In case a SUCI is sent when the timer is not expired, the solution will consider a genuine SUCI as an attack. It is FFS how to deal with the incoming SUCI within 60s in the UDM

#### 6.2.X.3 Evaluation

The proposed method does not have an impact on current standardized SUPI protection scheme. It also does not need any change on the UE and the network. The only change required is that the UDM has to store the received UE's public key after determining that the SUCI is not a replay message.

The proposed method prevents the linkablity attack as it can identify the replay attack without returning the RAND and AUTN to the attacker. The possible DoS attack is also mitgated as it does not invoke the computation heavy ECIES algorithm before determining whether the SUCI is a replay message or not.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 