**3GPP TSG-SA3 Meeting #99e *S3-201140***

**e-meeting, 11 -15 May 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Clarification to the Usage of KAUSF for Solution #2.2 in TR 33.846**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This pCR clarifies the usage of KAUSF for the solution #2.2 in TR 33.846, and is kindly asked to be approved by SA3.***

# 2 Reference

[1] 3GPP TR 33.846 V0.4.0, Study on authentication enhancements in 5G System

[2] 3GPP TS 33.501 V15.5.0, Security architecture and procedures for 5G system

# 3 Rationale

There is Editor’s note for the solution #2.2 in TR 33.846, i.e. “The use of previous KAUSF needs to be further clarified.” This pCR makes a clarification for this.

The so called previous KAUSF is the KAUSF stored in the UE and AUSF after the mutual authentication between UE and AUSF is successful. The stored KAUSF has already been used in Steering of Roaming and UE Parameter Update procedures to provide AUSF to UE integrity protection, as well as in AKMA to derive the intermediary key KAKMA.

Similar to the usage of KAUSF mentioned above, to prevent the linkability attack, the KAUSF stored in UE and AUSF is used to protect the authentication failure message. This usage is not special compared to other ones. The only difference is how to use KAUSF when a UE registers to the network at the first time, as UE and AUSF has no stored (previous) KAUSF. To address this issue, authentication failure message for the first UE registration is left unencypted, i.e. the initial value of KAUSF is set to zero. This does not raise the security threats, as the attacker does not have a valid RAND and AUTN associated with the successful authentication at this time, which is a prerequisite to luanch the linkability attack. In other words, authentication failure message for the first UE registration can not be invoked by the attacker.

Based on the above disscussion, the Editor’s note could be removed.

# 4 Detailed proposal

\*\*\*\* Beginning of Change \*\*\*\*

### 6.2.2 Solution #2.2: <Mitigation against the linkability attack and the SQN leakage attack>

#### 6.2.2.1 Introduction

This solution addresses the key issue#2.1 and key issue #4.1.

#### 6.2.2.2 Solution details

The basic idea of the solution is that the UE sends only one encrypted message to the network to indicate the error message type (MAC\_FAIL, SYNC\_FAIL) if the UE authentication network fails. This message is protected by using the encryption key KE and the integrity key KM, which are derived from the session anchor key KAUSF that is known to the UE and the network. Since this message is encrypted, the attacker cannot get the content of this message, and can not initiate a linkability attack. Moreover, the SQN is not disclosed even if the key stream to encrypt the SQN is resued, since the AUTS which is the XORes value between SQN and the key stream is encrypted with the key KE. The procedure of the proposal is illustrated in the following figure.



The steps of the proposal are as follows.

1. The network authenticates the UE using the selected authentication protocol.

2. The UE verifies the network. If the verification fails, an *Authentication Response* message is generated, which includes FAIL\_CAUSE, Nonce, SUPI, and RES\_DATA. The value of FAIL\_CAUSE can be MAC\_FAIL, SYNC\_FAIL. Nonce is a one-time random number that makes the ciphertext of the Authentication Response message different each time to prevent the attacker from guessing the actual value of FAIL\_CAUSE. The SUPI of the UE may be optionally sent to the network in this message to prevent the SEAF from initiating an *Identity Request* message to the UE. In this way, SEAF could only send an *Authentication Request* message to the UE regardless of whether it is MAC\_FAIL or SYNC\_FAIL, thereby avoiding the linkability attack raised by that the SEAF acknowledeges the UE with different actions after receiving the different *Authentication Response* message specified in reference [3]. If the value of FAIL\_CAUSE is SYNC\_FAIL and RES\_DATA is AUTS, it is generated according to reference [2] for restoring SQN synchronization between UE and network. If the value of FAIL\_CAUSE is MAC\_FAIL, RES\_DATA is a random number whose length is the same as that of AUTS. This *Authentication Response* message is encrypted by using the ncryption key KE, and its MAC is generated by using the integrity key KM. The generation of the keys KE and KM is carried out in accordance with the key derivation function KDF of TS 33.220 Appendix B, which is calculated as follows:

KE=KDF (KAUSF, RAND || length of RAND‖"Encryption Key"‖ Length of " Encryption Key")

KM=KDF (KAUSF, RAND || length of RAND‖"MAC Key"‖Length of "MAC Key" )

 Here " ‖" represents the string concatenation.

 The authentication failure message for the first UE registration is left unencrypted, i.e. the initial value of KAUSF is set to zero.

3. The UE sends an *Authentication Response* message to the SEAF.

4. The SEAF forwards the *Authentication Response* message to the AUSF in the message Nausf\_UE Authentication\_Authenticate request.

5. Like UE, the AUSF derives the encryption key KE and the integrity key KM from the session achnor key KAUSF. Further the AUSF verifies the MAC using the integrity key KM, and if the verification is successful, decrypts the message using the encryption key KE.

6. If FAIL\_CAUSE is SYNC\_FAIL, the AUSF sends a Nudm\_UEAuthentication\_Get request message to the UDM with the following parameters: RAND and AUTS. The UDM synchronizes the SQN of the network with the SQN of the UE according to AUTS and RAND.

7. The AUSF sends FAIL\_CAUSE and the SUPI of the UE to the SEAF.

#### 6.2.2.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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

#