**3GPP TSG-SA3 Meeting #102-e *S3-210164-r1***

**e-meeting, 18 - 29 January 2021** Revision of S3-21XXXX

**Source: ZTE Corporation**

**Title: Update solution#2.1 in TR 33.846**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***This contribution proposes to update solution#2.1 .***

# 2 References

*(Reference - in list form - should be made to previous related SA3/3GPP/etc. documents.)*

[1] 3GPP TR 33.846 V0.9.0“Study on authentication enhancements in 5G System”.

# 3 Rationale

This contribution proposes to update the solution#2.1 and mark the editor changes for TS 33.501 in bold.

# 4 Detailed proposal

***\*\*\*\* START OF CHANGES \*\*\*\****

### 6.2.1 Solution #2.1: Handling of Sync failure and MAC failure by AUTS/random number encryption and failure code

#### 6.2.1.1 Introduction

This solution addresses the key issue #2.1 Mitigation against the linkability attack and key issue #4.1 Protection of SQN during AKA re-synchronisations. The AUSF and UE stores the KAUSF during successful authentication. When MAC or sync failure occurred, the UE uses the KAUSF stored during previously successful authentication to encrypt the AUTS/random number and failure code, and the AUSF uses the KAUSF stored during previously successful authentication to decrypt the AUTS/random number and failure code.

Editor’s Note: The security risk of using a fixed key is FFS.

If no stored KAUSF, the KEY is a 256-bit binary string of all 0s.

#### 6.2.1.2 Solution details



Figure 6.2.1.2: Authentication procedure for 5G AKA

The authentication procedure of 5G AKA in 6.1.3.2.0 of TS 33.501 [2] is followed with the modifications:

Step 3: The AUSF shall store the XRES\* temporarily together with the received SUCI or SUPI. The AUSF shall store the KAUSF.

Step 8: The UE shall return RES\* to the SEAF in a NAS message Authentication Response. The UE shall store the KAUSF.

Step 11:When the AUSF receives as authentication confirmation the Nausf\_UEAuthentication\_Authenticate Request message including a RES\* it may verify whether the AV has expired. If the AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view, and in this case the AUSF shall remove the KAUSF stored in step 2. AUSF shall compare the received RES\* with the stored XRES\*. If the RES\* and XRES\* are equal, the AUSF shall consider the authentication as successful from the home network point of view, and in this case the AUSF shall remove the old KAUSF stored during previously successful authentication if exists. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for linking with the authentication confirmation).

The handling of Sync failure in 6.1.3.3 of TS 33.501 [2] is followed with the modifications in bold:

##### 6.2.1.2.1 Synchronization failure or MAC failure

###### 6.2.1.2.1.1 Synchronization failure or MAC failure in USIM

This clause describes synchronisation failure or MAC failure in USIM.

In step 7 in Figure 6.1.3.2-1 when 5G AKA is used; or in step 5 in Figure 6.1.3.1-1 when EAP-AKA’ is used, at the receipt of the RAND and AUTN, if the verification of the AUTN fails, then the USIM indicates to the UE the reason for failure and in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [9]) to the UE.

If 5G AKA is used: The ME shall respond with NAS message Authentication Failure with a CAUSE value indicating the reason for failure. In case of a synchronisation failure of AUTN (as described in TS 33.102 [9]), t**he UE should also include encrypted AUTS that the plaintext AUTS was provided by the USIM. In case of a MAC failure, the UE should generate and encrypt a random number as same length as the AUTS. Upon receipt of an authentication failure message from AUSF, the AMF/SEAF may initiate new authentication towards the UE.**

**The AUTS and failure code encryption is done by following: The UE generates a keystream by computing HMAC-SHA-256 with a KEY and RAND as input. If the UE has stored a KAUSF, the KEY is the KAUSF, otherwise the KEY is 256-bit string of all 0s. The UE uses a bit per bit binary addition of failure code, the AUTS and the keystream.**

If EAP-AKA’ is used: The UE shall proceed as described in RFC 4187 [21] and RFC 5448 [12] for EAP-AKA’.

###### 6.2.1.2.1.2 **Synchronization failure recovery and MAC failure in Home Network**

Upon receiving an authentication failure message *with***encrtyped AUTS/random number and failure code** from the UE, the SEAF sends a Nausf\_UEAuthentication\_Authenticate Request message with **the encrypted AUTS/random number and failure code** to the AUSF. **The AUSF generates a keystream by computing HMAC-SHA-256 with a KEY and RAND sent to the UE in the preceding Authentication Request as input. If the AUSF has stored a KAUSF that generated during previously successful authentication, the KEY is the KAUSF, otherwise the KEY is 256-bit string of all 0s. The AUSF uses a bit per bit binary addition of the encrypted AUTS/random number and failure code and the keystream to get the plaintext AUTS/random number and failure code.**

**Note: if the KEY is the KAUSF and the failure code is not synchronization failure or MAC failure, the KEY is changed into 256-bit string of all 0s for decrypting the encrypted AUTS/random number and failure code.**

**If the failure code is synchronization failure, the AUSF then sends a Nudm\_UEAuthentication\_Get Request message to the UDM/ARPF, together with the following parameters:**

***- RAND* sent to the UE in the preceding Authentication Request, and**

***- Plaintext AUTS*.**

**Else, the AUSF sends Nausf\_UEAuthentication\_Authenticate Response message with failure code to the SEAF, and the SEAF may send identity request to UE (see TS 24.501[35]).**

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf\_UEAuthentication\_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out).

When the UDM/ARPF receives an Nudm\_UEAuthentication\_Get Request message with a "*synchronisation failure indication*" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC. The UDM/ARPF sends an Nudm\_UEAuthentication\_Get Response message with a new authentication vector for either EAP-AKA’ or 5G-AKA depending on the authentication method applicable for the user to the AUSF. The AUSF runs a new authentication procedure with the UE according to clauses 6.1.3.1 or 6.1.3.2 depending on the authentication method applicable for the user.

#### 6.2.1.3 Evaluation

The protection of SQN will only work over 5G network.

The use of key of 256-bit string of all 0s may cause linkability attack.

The solution impacts the SEAF/AMF.

***\*\*\*\* END OF CHANGES \*\*\*\****