**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211505-r1***

**e-meeting, 17 – 28 May 2021** Revision of S3-211505

**Source:** **Nokia, Nokia Shanghai Bell**

**Title: Editor note removal on solution #2.9 MAC, SYNCH failure cause concealment**

**Document for: Approval**

**Agenda Item: 2.5**

# 1 Decision/action requested

***Editor note removal of solution #2.9 MAC, SYNCH failure cause concealment.***

# 2 References

[1]

# 3 Rationale

The following editor’ note has been captured in SA3#102bis-e meeting in solution #2.9 details to consider if the solution could be vulnerable.

Editor's Note: It is FFS, if failure cause sent in AUTSCAUSE is vulnerable (similar to SQN recovery attack).

**Observations**:

As described in clause 6.2.9.2 NOTE 2, in order to handle the attack scenario, where the attacker repeats the same RAND and AUTN in 5G AKA challenge and retrieves the "cause value", which is concealed (similar to SQN leakage key issue), USIM generated 128 bits of RAND (RANDMS / RANDSQN as described in solution #4.5 or #4.7) is used in initial registration request message to conceal the SQNMS at UE / UDM.

When registration request is sent with RANDMS / RANDSQN, USIM stores only LSB of 128 bits for future verification purposes and UDM uses received RAND (RANDMS / RANDSQN) to concatenate with newly generated random value at UDM (Note, only LSB of 128 bits RANDMS / RANDSQN is concatenated). AKA challenge is sent with concatenated RAND, so USIM can verify the received RAND by checking the LSB from stored RANDMS/RANDSQN. After verification, USIM deletes previously stored RANDMS / RANDSQN. An attacker cannot repeat the same RAND and AUTN, as LSB of random number does not exist in USIM and verification of RAND fails.

**Resolution:**

It is proposed to delete this editor's note in solution.

# 4 Detailed proposal

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

### 6.2.9 Solution #2.9: MAC, SYNCH failure cause concealment

#### 6.2.9.1 Introduction

This solution addresses Key Issue #2.1: Mitigation against the linkability attack.

In this document, there are many solutions available like solution#4.3, solution #4.5, solution #4.7, solution#3.1 for study to prevent SQN leakage (Key Issue#4.1) by sharing the SQNMS value in various forms in Registration request message to UDM. This removes the necessity of sending SQNMS value in AUTS during synch failure or MAC failure cause in Authentication failure message.

This solution proposes to conceal the failure cause to avoid the linkability attack.

#### 6.2.9.2 Solution details

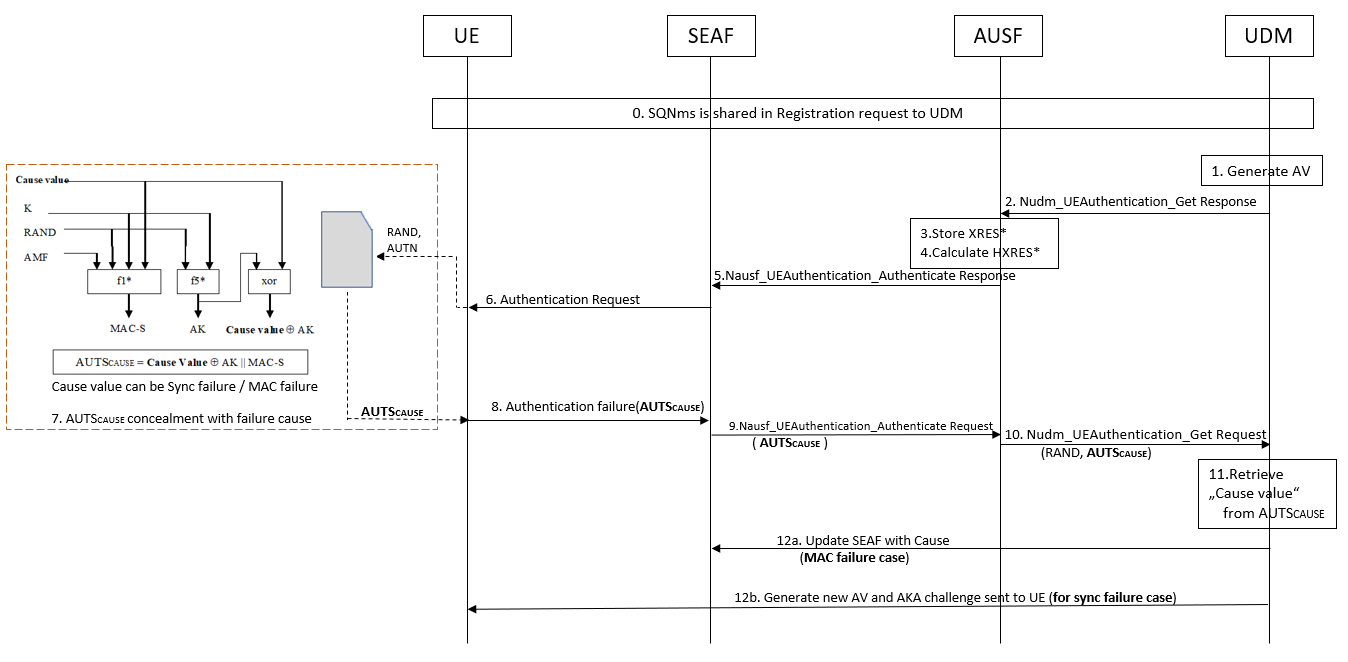


Figure 6.2.9.2-1: Cause concealment (5GS) in case of authentication failure

The initial Registration procedure is triggered from UE and the procedure is the same as described in clause 6.1.2 of 3GPP TS 33.501 [2]. Only step 7 varies by creating a new 5GMM cause value.

Step 0: SQNms is shared from UE to UDM in registration request message. Concealed format of SQNms (could be encrypted separately or sent as AUTN or embedded in SUCI).

Step 1: UDM generates authentication vector, derives KAUSF and calculates XRES\*. UDM/ARPF will create 5G HE AV from RAND, AUTN, XRES\* and KAUSF.

Step 2: UDM will return 5G HE authentication vector to AUSF to be used for 5G AKA in Nudm\_UEAuthentication\_Get Response. UDM will include SUPI in the SUPI in the Nudm\_UEAuthentication\_Get Response after deconcealment of SUCI by SIDF.

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

Step 4: AUSF will then generate 5G authentication vector from the 5G HE authentication vector received from the UDM/ARPF by computing the HXRES\* from XRES\* and KSEAF from KAUSF, and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G.

Step 5: AUSF will remove the KSEAF and return the 5G SE authentication vector (RAND, AUTN, HXRES\*) to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response.

Step 6: SEAF will send RAND, AUTN to the UE in a NAS message Authentication Request. This message will also include ngKSI that will be used by UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message will also include the ABBA parameter. ME will forward the RAND and AUTN received in NAS message Authentication Request to the USIM.

Step 7: These three steps are followed at USIM after reception of RAND and AUTN.

7.1. USIM computes XMAC and compares this with received MAC from AUTN. If they are different, then it results in **MAC failure**. If it is same, then it continues to step 7.2.

7.2. USIM verifies if the received sequence number SQN is in correct range or not. If it is not in correct range, then it results in **Synchronisation failure**. If it is in correct range, then it continues to step 7.3.

7.3. As MAC verification and sequence number range is verified, USIM computes RES to be included in authentication response.

For MAC failure or Synchronisation failure, the cause value is taken as input for concealment in AUTSCAUSE.

The generation of MAC-S, AK and Cause concealment is shown below.

MAC-S = f1\*K(Cause value || RAND || AMF)

AK = f5\*K(RAND)

Conc(Cause value) = Cause value ⊕ AK

AUTSCAUSE = Conc(Cause value ) || MAC‑S

NOTE 1: AUTSCAUSE containing cause value will be sent for both MAC and Synch failure. USIM conceals the cause values in AUTSCAUSE and forwards it to ME.

Step 8: Authentication failure message is sent from UE to SEAF with new 5GMM cause value as generic "authentication failure cause" along with AUTSCAUSE.

Step 9: Upon receiving an authentication failure message with AUTSCAUSE from the UE, the SEAF sends a Nausf\_UEAuthentication\_Authenticate Request message with a "synchronisation failure indication" to the AUSF.

Step 10: AUSF 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

- AUTSCAUSE received by the SEAF in the response from the UE to that request.

Step 11: UDM retrieves cause value from AUTSCAUSE using RAND value.

Step 12: In case of MAC failure cause value, UDM updates SEAF with MAC failure for the Authentication procedure. Rest of the procedures of how MAC failure is treated remains the same (as described in TS 33.501[V] & TS 24.501[W] 5.4.1.3.6 & 5.4.1.3.7 item c.).

In case of Synch failure, a new Authentication vector is generated in UDM and the AKA challenge is sent to UE. Below figure 6.2 shows the concealed cause value in AUTSCAUSE generation at step 7 in USIM and related 5GS procedures.

NOTE 2: In order to handle the attack scenario, where the attacker repeats the same RAND and AUTN in 5G AKA challenge and retrieves the "cause value", which is concealed (similar to SQN leakage key issue), USIM generated 128 bits of RAND (RANDMS / RANDSQN as described in solution #4.5 or #4.7) is used in initial registration request message to conceal the SQNMS at UE / UDM.

When registration request is sent with RANDMS / RANDSQN, USIM stores only LSB of 128 bits for future verification purposes and UDM uses received RAND (RANDMS / RANDSQN) to concatenate with newly generated random value at UDM (Note, only LSB of 128 bits RANDMS / RANDSQN is concatenated). AKA challenge is sent with concatenated RAND, so USIM can verify the received RAND by checking the LSB from stored RANDMS/RANDSQN. After verification, USIM deletes previously stored RANDMS / RANDSQN. An attacker cannot repeat the same RAND and AUTN, as LSB of random number does not exist in USIM and verification of RAND fails.

#### 6.2.9.3 Evaluation

The USIM needs to conceal a MAC or Sync cause value.

Solution works only when SQNms is already shared in Registration request message.

Solution has an impact of serving network (AMF) as home network decrypts cause value and updates serving network, in case of MAC failure.The solution also has an impact on USIM and UDM.

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