**3GPP TSG-SA3 Meeting #102e *draft\_S3-210336-r5***

**e-meeting, 18 – 29 January 2021** Revision of S3-203330

**Source: Nokia, Nokia Shanghai Bell**

**Title: SQNms protection by concealment in ME**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***Solution proposal for SQNms protection by concealment in ME to address key issue #4.1 in TR 33.846.***

# 2 References

# 3 Rationale

As described in key issue #4.1 of TR 33.846:

The freshness parameter for the calculation of AK (the keystream that protects the SQN returned to the network) during a re-synchronisation in AKA is the random number RAND from the challenge. An attacker can force the re-use of RAND and hence the keystream AK may be used multiple times to protect different SQNs [4]. The attacker could leverage the feedback from the network side and conduct an activity monitoring attack to break subscribers' privacy. It is preferable to avoid such keystream re-use.

The presented solution proposal prevents the attacker from retrieving any SQNMS information from UE in a way that both UE and HE side need to do a proactive / prior step before AKA challenge begins during primary authentication. SUCI concealment is done in the ME in this solution.

# 4 Detailed proposal

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

6.0 Mapping of solutions to key issues

**Table 6.0-1: Mapping of solutions to key issues**

|  |  |
| --- | --- |
|  | **Key Issues** |
| **Solutions** | #1.X | #2.1 | #2.2 | #3.1 | #3.2 | #4.1 |  |  |
| **Solutions for anchor keys security** |  |  |  |  |  |  |  |  |
| No solution so far |  |  |  |  |  |  |  |  |
| **Solutions for resilience against identifier linkability** |  |  |  |  |  |  |  |  |
| #2.1: Handling of Sync failure by AUTS encryption |  | x |  |  |  | x |  |  |
| #2.2: Encryption of authentication failure message types by UE with new keys derived from K\_AUSF |  | x |  |  |  | x |  |  |
| #2.3: Unified authentication response message by UE |  | x |  |  |  |  |  |  |
| #2.4: MAC-S based solution |  | x |  |  |  | x |  |  |
| #2.5: Encryption of authentication failure message with SUCI method |  |  | x |  |  |  |  |  |
| #2.6: Certificate based encryption of unicast NAS message |  | x |  |  |  | x |  |  |
| **Solutions for availability aspects of SUCI usage** |  |  |  |  |  |  |  |  |
| No solution so far |  |  |  |  |  |  |  |  |
| **Solutions on re-synchronisation in AKA** |  |  |  |  |  |  |  |  |
| #4.1: Using MACS as freshness in the calculation of AK |  |  |  |  |  | x |  |  |
| #4.2: Using symmetric encryption function to protect SQN during a re-synchronisation procedure in AKA |  |  |  |  |  | x |  |  |
| #4.3: SQN protection by concealment with SUPI in USIM |  | x | x |  |  | x |  |  |
| #4.4: SQN protection during re-synchronisation procedure in AKA |  |  |  |  |  | x |  |  |
| #4.X: SQN protection by concealment with SUPI with f5\* |  | x | x |  |  | x |  |  |
|  |  |  |  |  |  |  |  |  |

*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE*

### 6.4.X Solution #4.X: SQN protection by concealment with SUPI with f5\*

#### 6.4.X.1 Introduction

This solution addresses the key issue #4.1 Protection of SQN during AKA re-synchronisations, the linkability attack in key issue #2.2, and key issue #3.2 to mitigate the SUPI guessing attacks.

#### 6.4.X.2 Solution details

This solution is based on solution #4.3 (from TR 33.846), which proposes that the USIM is concealing SQNMS and SUPI together, to protect SQN during AKA re-synchronisation. The solution described in the following works for SUCI concealment in ME also for other schemes than null scheme.

ME shall calculate the SUCI, according to 3GPP TS 33.501 [X] clause 6.12.2, if the operator's decision is to do so. In this case, the ME shall read the SUCI calculation information from the USIM, including the SUPI, the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the list of protection scheme identifiers.

To allow the ME doing SQN protection by concealment with SUPI according to solution #4.3, ME also needs to include SQNMS in the SUCI calculation. However, it has to be assured that the SQNMS does not leave USIM in the clear. It is therefore proposed that USIM calculates SQNMS. For this, a new RANDSQN value is calculated in the USIM and the following steps are followed:

1. At USIM, using a newly generated RANDSQN value and counter value SQNMS, the concealed value Conc(SQNMS) is generated with the existing key generating function f5\*, i.e. Conc(SQNMS) = SQNMS Å f5\*K(RANDSQN). Both Conc(SQNMS) and RANDSQN value are shared, together with SUPI, to ME for SUCI calculation.

2. At ME, SUCI is then generated from SUPI, Conc(SQNMS) and RANDSQN. The SUPI type is marked as SUPI plus SQNMS (e.g. value 4).

3. At the home network UDM/ARPF/SIDF, after SUCI de-concealment, SUPI, Conc(SQNMS) and RANDSQN are retrieved. Further, SQNMS is retrieved from Conc(SQNMS) (similar to step 1 of 3GPP TS 33.102 clause 6.3.5). The Home Environment temporarly stores SQNMS. UDM/ARPF retrieves with SUPI the existing SQNHE and generates an authentication vector AV.

4. At UE, for a success case, if there is neither a MAC failure nor a synchronization failure, the Authentication response message is sent back to AMF/SEAF. At UDM, since the SQNMS and SQNHE are already aligned, the temporarily stored SQNMS in UDM is deleted.

5. At UE, for a failure case, if there is synchronization failure, then no AUTS calculation is performed. Only a cause for failure is shared from UE to the network with Authentication failure message. Since UDM already holds the SQNMS temporarily till 5G AKA is finalized, no AUTS need to be added in the failure message, i.e. SQNMS is not needed to be sent in the failure message. When Authentication failure message is received by UDM, a new AV is generated from the already available SQNMS (received in Registration request as part of SUCI). In this case, UDM also synchronizes SQNHE with SQNMS. AUSF provides (RAND, AUTN) to AMF/SEAF, which will send another challenge to UE. This fresh challenge cannot have SQN synchronisation failure anymore, because UDM has synchronized SQNHE and SQNMS already.

#### 6.4.X.3 Evaluation

TBD

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