**3GPP TSG-SA3 Meeting #102Bis-e *draft\_S3-210841-r1***

**e-meeting, 01 – 05 March 2021** Revision of [S3-210841](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/SGS3_102Bis-e/Docs/S3-210841.zip) and [S3-210851](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/SGS3_102Bis-e/Docs/S3-210851.zip)

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

**Title: Editor note removal on SQNms protection by concealment with SUPI with f5\***

**Document for: Approval**

**Agenda Item: 2.5**

# 1 Decision/action requested

***Editor note removal of SQNms protection by concealment with SUPI with f5\*.***

# 2 References

[1]

# 3 Rationale

The following editor’ note has been captured in SA3#102-e meeting in solution details to consider if the solution can

work for both ME and USIM.

Editor's Note: It is FFS whether this solution could be extended to SUCI computation in the USIM.

**Observations**:

For SUCI calculation in USIM: Conc(SQNMS) can be concealed in USIM using generated RANDSQN. SUCI is generated with SUPI, Conc(SQNMS) and RANDSQN in USIM.

For SUCI calculation in ME: Conc(SQNMS) can be concealed in USIM using generated RANDSQN. Conc(SQNMS) and RANDSQN are shared in existing SUCI related EF files from USIM to ME. When SUCI is generated in ME, the input parameters like SUPI, Conc(SQNMS) and RANDSQN is considered.

**Resolution:**

It is proposed to delete this editor's note and solution is adapted to replace ME with UE (covering both ME and USIM).

# 4 Detailed proposal

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

### 6.4.7 Solution #4.7: SQN protection by concealment with SUPI with f5\*

#### 6.4.7.1 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.

#### 6.4.7.2 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 or in the USIM. The solution also applies for other schemes than null scheme.

UE 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 case of SUCI concealment in ME, 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 UE doing SQN protection by concealment with SUPI according to solution #4.3, UE 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 conceals SQNMS. For this, a new RANDSQN value is generated in the USIM. For SUCI concealment in the ME or in the USIM the following steps are performed:

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, for SUCI calculation.

2. At UE, 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 temporarily stores SQNMS; and RANDSQN is deleted. 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.

#### 6.4.7.3 Evaluation

TBD

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