**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212722-r1***

**e-meeting, 16 – 27 August 2021**

**Source: Huawei, HiSilicon**

**Title: Update to clause 7.02**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***This pCR proposes to update to clause 7.02 and add conclusion to key issue 3.2 in TR 33.846.***

# 2 Rationale

Database of SUPI is essential and significant for operators. It’s proposed to use solution#3.3 as baseline for normative work. The solution only has impact to the visiting network.

# 3 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.846.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.0.2 Impact of solutions

Table: Comparison table of UE and network impacts per solution

|  |  |  |  |
| --- | --- | --- | --- |
|   | **UE impacts** | **Network impacts** | **comments** |
| **Solutions** |  | AMF/SEAF | UDM/ARPF |  |
| **Solutions for resilience against identifier linkability** |  |  |  |  |
| #2.1: Handling of Sync failure by AUTS encryption | ME | X | X | Risk of linkability attack. |
| #2.2: Encryption of authentication failure message types by UE with new keys derived from K\_AUSF | Probably ME | X | X | Authentication failure message for the first UE registration is left unencrypted |
| #2.3: Unified authentication response message by UE | USIM  | X | X |  |
| #2.4: MAC-S based solution | USIM | X | X |  |
| #2.5: Encryption of authentication failure message with SUCI method | USIM or ME | X | X | This solution relies on the availability of SUCI mechanism. |
| #2.6: Certificate based encryption of unicast NAS message | USIM and ME | X | X | This solution relies on the availability of PKI architecture, and there is companion list of open questions. |
| #2.7: Mitigation against the SUCI replay attack | USIM and ME |  | X |  |
| #2.8 Assuring SUCI generation by legitimate SUPI owner using KSUCI | USIM and ME |  | X | The security risk to derive new key from long term key for any new purposes (example: during KSUCI derivation) different from the ones already specified for AKA procedure needs to be evaluated by ETSI SAGE |
| #2.9: MAC, SYNCH failure cause concealment | USIM | X | X |  |
| #2.10: Solution to key Issue #2.2: SUCI replay |  |  | X |  |
| #2.11: Mitigate the SUCI replay based on UE’s public key |  |  | X |  |
| **Solutions for availability aspects of SUCI usage** |  |  |  | Usage of the long term key K for other uses. |
| #3.1: Mitigation of SUPI guessing and SUCI replay attack using long term key | USIM and ME | X | X | Security issue due to the use of the long term key K for other purpose than AKA. |
| #3.2: Adding Check Value behind SUPI to mitigate the SUPI guessing attacks | USIM |  | X |  |
| #3.3: Mitigation of SUPI guessing attack |  | X |  |  |
| **Solutions on re-synchronisation in AKA** |  |  |  |  |
| #4.1: Using MACS as freshness in the calculation of AK | USIM |  | X |  |
| #4.2: Using symmetric encryption function to protect SQN during a re-synchronisation procedure in AKA | USIM |  | X | This solution requires the definition of a new function f6\* for AKA procedure |
| #4.3: SQN protection by concealment with SUPI in USIM | USIM | X | X | Solution works if SUCI computation is performed in the USIM. |
| #4.4: SQN protection during re-synchronisation procedure in AKA | USIM and ME |  | X | Limitation of SQNMS leakage depends on RAND storage in the USIM. |
| #4.5: AUTS SQNMS solution for 5GS | USIM and ME | X | X | TBD |
| #4.6: Using time-based or partly time-based SQN generation |  |  |  | Solution requires time based SQN generation |
| #4.7: SQN protection by concealment with SUPI with f5\* | USIM and ME | X | X | TBD |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*