**3GPP TSG-SA3 Meeting #101e *draft\_S3-203333-r1***

**e-meeting, 9 - 20 November 2020** Revision of S3-203333

**Source: Nokia, Nokia Shanghai Bell**

**Title: SQNms protection by concealment**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

# *Solution update for SQNms protection by concealment to address MCC editorial comments in TR 33.846.*

# 2 References

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.102: "Security architecture".

[4] Ravishankar Borgaonkar (published online: July 2019), “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”, <https://eprint.iacr.org/2018/1175.pdf>

[5] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[6] 3GPP TS 23.501 : System architecture for the 5G System (5GS)

# 3 Rationale

After SA3#100bis-e, a few editorial corrections were suggested by MCC:

* Clause 6.4.3.2: Figure and title have the wrong styles.
* Same clause: TS 23.003 [A] ??
* Clause 6.4.3.3: missing references to TS 33.501
* Step 1 in the same clause: TS 33.501 (missing reference) and “section 6.1.3.2.0”. We have no sections in 3GPP, we have “clauses”.
* Same clause: blue text in steps 8 and 11.
* Clause 6.4.3.5: missing reference to TS 23.003 and the word “section”.

This contribution addresses these editorials.

# 4 Detailed proposal

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

# References

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.102: "Security architecture".

[4] Ravishankar Borgaonkar (published online: July 2019), “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”, <https://eprint.iacr.org/2018/1175.pdf>

[5] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[6] 3GPP TS 23.501 : System architecture for the 5G System (5GS)

[X] 3GPP TS 23.003: Numbering, addressing and identification.

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

### 6.4.3 Solution #4.3: SQN protection by concealment with SUPI

#### 6.4.3.1 Introduction

This solution addresses the key issue #4.1 Protection of SQN during AKA re-synchronisations.

#### 6.4.3.2 Solution details

Current usage of ECIES for concealment of SUPI can be expanded to accommodate SQNMS and SUPI. Maximum allowed size of cipher text from concealment of protection scheme output is 3000 digits. SUPI utilizes only few bytes of those maximum allowed digits and still can adapt SQNMS.

A close up of a map

Description automatically generated

Figure 6.4.3.2-1 Encryption based on ECIES at UE

Figure 6.4.3.2**-**1 shows the encryption based on ECIES at UE side, where SUPI is concatenated with SQNMS and taken as one plain text block for symmetric encryption. In case of SUPI type as IMSI, then MSIN (9 to 10 digits) and SQNMS (48 bits: 6 bytes) is concatenated in UE.

A screenshot of a cell phone

Description automatically generated

Figure 6.4.3.2-2 Decryption based on ECIES at home network

Figure 6.4.3.2**-**2 shows the decryption based on ECIES at home network, where SUPI and SQNMS is dissociated after the symmetric decryption.



Figure 6.4.3.2-3: Structure of SUCI

Figure 6.4.3.2-3 shows the structure of SUCI with SUPI Type, which consists values in the range 0 to 7 as specified in clause 2.2B of TS 23.003 [X]. SUPI Type identifies the type of the SUPI concealed in the SUCI.

For this solution, the encoding of SUCI for ‘SUPI plus SQNMS' will be represented by a new SUPI Type value, e.g. value 4.

- 0: IMSI

- 1: Network Specific Identifier

- 2: Global Line Identifier (GLI)

- 3: Global Cable Identifier (GCI)

**- 4: SUPI plus SQNMS**

- 5 to 7: spare values for future use.

#### 6.4.3.3 Adaptation of authentication procedures

##### 6.4.3.3.0 General

The following sequence charts illustrates the text already specified in 3GPP TS 33.501[2], clause 6.1.2, for the case of initiation of authentication and selection of authentication method. Changes are marked in **bold**.

##### 6.4.3.3.1 Initiation of authentication and selection of authentication method

2. <N1 message>

(SUCI **containing SQNMS** )

UE

3. Nausf\_UEAuthentication\_ Authenticate Request

(SUCI **containing SQNMS** or SUPI, SN-Name)

4. Nudm\_UEAuthentication\_ Get Request (SUCI **containing SQNMS** or SUPI, SN-Name)

UDM/ARPF

AMF/

SEAF

AUSF

**1. Conceal SUPI and SQNMS**

5. [SUCI to SUPI, **SQNMS** de-concealment].

Authentication Method selection.

Figure 6.4.3.3.1-1: Illustration of UE and HE is sharing SQNMS along with SUCI

1. During the primary authentication procedure, USIM concatenates SUPI and SQNMS. The concatenated plain text block is encrypted using ECIES method. New value is introduced for “SUPI Type”, for e.g. Value 4 represents SUCI encoded with SUPI plus SQNMS.
2. UE uses SUCI containing SQNMS in Registration request message, which is sent to AMF/SEAF.
3. AMF/SEAF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the AMF/SEAF wishes to initiate an authentication.

The Nausf\_UEAuthentication\_Authenticate Request message contains either:

- SUCI containing SQNMS, as defined in the current specification, or

- SUPI, as defined in 3GPP TS 23.501 [6].

The AMF/SEAF includes the SUPI in the Nausf\_UEAuthentication\_Authenticate Request message in case the AMF/SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI containing SQNMS is included in Nausf\_UEAuthentication\_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf\_UEAuthentication\_Authenticate Request furthermore contains:

- the serving network name, as defined in sub-clause 6.1.1.4 of 3GPP TS 33.501 [2].

1. Upon receiving the Nausf\_UEAuthentication\_Authenticate Request message, the AUSF checks that the requesting AMF/SEAF in the serving network is entitled to use the serving network name in the Nausf\_UEAuthentication\_Authenticate Request by comparing the serving network name with the expected serving network name. The AUSF stores the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF responds with "serving network not authorized" in the Nausf\_UEAuthentication\_Authenticate Response.

The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes the following information:

- SUCI containing SQNMS or SUPI;

- the serving network name;

1. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF if a SUPI type is SUPI plus SQNMS, then SIDF de-conceals SUCI to gain SUPI and SQNMS before UDM can process the request.

Based on SUPI, the UDM/ARPF chooses the authentication method. SQNMS is stored in UDM for future use. At UDM, Authentication vector is generated with existing SQNHE. The solution is restricted to 5G.

NOTE 1: The Nudm\_UEAuthentication\_Get Response in reply to the Nudm\_UEAuthentication\_Get Request and the Nausf\_UEAuthentication\_Authenticate Response message in reply to the Nausf\_UEAuthentication\_Authenticate Request message are described as part of the authentication procedures in 3GPP TS.33.501 [2], clause 6.1.3.

NOTE 2: SQNMS is not considered for Authentication vector generation on purpose.

##### 6.4.3.3.2 Successful Authentication case

In success case the Authentication procedure (considering example of 5G AKA) is the same as 3GPP TS.33.501[2], clause 6.1.3.2.0. The solution does not impact the existing call flow.

##### 6.4.3.3.3 Authentication failure case



Figure6.4.3.3.3-1: Authentication procedure for 5G AKA (Failure case)

Figure 6.4.3.3.3-1 shows the failure case of Authentication procedure (considering example of 5G AKA). Changes are shown in blue.

1. For each Nudm\_Authenticate\_Get Request, the UDM/ARPF creates a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [3]. The UDM/ARPF then derives KAUSF (as per Annex A.2) and calculate XRES\* (as per Annex A.4). Finally, the UDM/ARPF creates a 5G HE AV from RAND, AUTN, XRES\*, and KAUSF.

2. The UDM then returns the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G-AKA in a Nudm\_UEAuthentication\_Get Response. In case SUCI was included in the Nudm\_UEAuthentication\_Get Request, UDM will include the SUPI in the Nudm\_UEAuthentication\_Get Response.

3. The AUSF stores the XRES\* temporarily together with the received SUCI or SUPI.

4. The AUSF then generates the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES\* from XRES\* (according to 3GPP TS 33.501 [2] Annex A.5) and KSEAF from KAUSF (according to 3GPP TS 33.501 [2] Annex A.6), and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G HE AV.

5. The AUSF then removes the KSEAF return the 5G SE AV (RAND, AUTN, HXRES\*) to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response.

6. The SEAF sends RAND, AUTN to the UE in a NAS message Authentication -Request. This message also includes the ngKSI that will be used by the UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message also includes the ABBA parameter. The SEAF sets the ABBA paremeter as defined in Annex A.7.1. The ME forwards the RAND and AUTN received in NAS message Authentication Request to the USIM.

7. At receipt of the RAND and AUTN, the USIM verifies the freshness of the 5G AV by checking whether AUTN can be accepted as described in 3GPP TS 33.102 [3]. If the verification of the AUTN fails, then the USIM indicates to the ME the reason for failure.

8. The ME responds with NAS message Authentication Failure **only with a CAUSE value indicating the reason for failure (as SQN failure/mismatch). AUTS is not calculated by the UE and not shared to network.**

9. Upon receiving an authentication failure messagefrom the UE, the SEAF sends an Nausf\_UEAuthentication\_Authenticate Request message to the AUSF.

10. AUSF sends an Nudm\_UEAuthentication\_Get Request message to the UDM/ARPF.

11. When the UDM/ARPF receives an Nudm\_UEAuthentication\_Get Request message it acts as described in 3GPP TS 33.102 [3], 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 **by considering the SQNMS from database (i.e. SQNMS received in Nudm\_UEAuthentication\_ Get Request).** The AUSF runs a new authentication procedure with the UE according to clauses 6.1.3.1 or 6.1.3.2 of 3GPP TS 33.501 [2] depending on the authentication method applicable for the user.

#### 6.4.3.4 Solution summary

The solution adds a new SUPI type in 3GPP TS 23.003 [X], clause 2.2B.

Encryption and decryption on ECIES consider plain text block as “SUPI and SQNms” at UE and UDM / ARPF in 3GPP TS 33.501 [2].

Registration request is sent with SUPI plus SQNMS.

Sync failure during AKA challenge sends only failure cause and no AUTS is sent to the network.

Editor’s Note: It is ffs if this solution works for synchronization failure when AMF receives 5G-GUTI and decides to initiate authentication.

Editor’s Note: Backward compatibility analysis is FFS.

#### 6.4.3.5 Evaluation

The solution only protects the sequence number in 5GS.

The solution requires changes on the USIM and the UDM.

At USIM, during ECIES procedure of primary authentication, New SUPI type is added, SQNMS is concatenated with SUPI (plain text block).

At UDM, when the SUPI indicates ‘SUPI plus SQNMS' the de-concealment needs to disassociate SUPI and SQNMS. UDM stores SQNMS temporarily until the success or failure of the authentication is known.

There is no change to any entities if the authentication succeeds.

If there is authentication failure at the UE, UE sends only Authentication failure message to the HE with SQN failure cause code (new value), without AUTS.

At the UDM, if an authentication failure message with cause code (SQN failure) is received, the stored value of SQNMS received at the very first step is processed. UDM synchronizes its value of SQN, i.e SQNHE = SQNMS. Sequence number management profiles detailed in Annex C in 3GPP TS 33.102 [3] is kept intact.

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