**3GPP TSG-SA3 Meeting #102Bis-e *S3-211132-r1***

**e-meeting, 1 - 5 March 2021** Revision of S3-20xxxx

**Source: Samsung**

**Title: [5GFBS] Identifying MitM attack**

**Document for: Approval**

**Agenda Item: 2.1**

# 1 Decision/action requested

***It is requested to approve this contribution to address MitM by a FBS.***

# 2 References

[xx] 3GPP TS 33.501 Security architecture and procedures for 5G System

# 3 Rationale

This proposal addresses loop registration problem as described in S3-211131, Key Issue#3 and Key Issue #7: Protection against Man-in-the-Middle false gNB attacks.

# 4 Detailed proposal

***\*\*\*\*\*Start of Change\*\*\*\*\****

## 6.x Solution #x: Identifying MitM attack (on CAG IDs and TAIs) by a FBS

### 6.x.1 Introduction

The proposed solution is performed as part of Protection of Initial NAS message as specified in TS 33.501 [xx] (Clause 6.4.6).

The initial NAS message is the first NAS message that is sent after the UE transitions from the idle state. The UE sends a limited set of IEs (called the cleartext IEs) including those needed to establish security in the initial message when it has no NAS security context. When the UE has a NAS security context, the UE sends a message that has the complete initial NAS message ciphered in a NAS Container along with the cleartext IEs with whole message integrity protected. The ciphered NAS container includes the TAI and the CAG ID (if UE is accessing a CAG cell), which the UE selected from the broadcasted element in the SIB. The complete initial message is included in the NAS Security Mode Complete message in a NAS Container when needed (e.g. AMF cannot find the used security context) in the latter case and always in the former case as described below.

In case, the UE selects a PLMN other than Registered PLMN/EPLMN in the 5GMM-IDLE state and the UE has a NAS security context containing the NEA0, then the UE discards the NAS security context and follows the procedure specified in this clause for protection of initial NAS message.

### 6.x.2 Solution details

The protection of the initial NAS message proceeds as shown in Figure 6.x.2-1.



Figure 6.X.2-1: Protecting the initial NAS message

Step 1: The UE sends the initial NAS message to the AMF. If the UE has no NAS security context, the initial NAS message only contains the cleartext IEs, i.e. subscription identifiers (e.g. SUCI or GUTIs), UE security capabilities, ngKSI, indication that the UE is moving from EPC, Additional GUTI, and IE containing the TAU Request in the case idle mobility from LTE.

If the UE has a NAS security context, the message sent contains the information given above in cleartext and the complete initial NAS message ciphered in a NAS container, which is ciphered. The ciphered NAS container includes the TAI and the CAG ID (if UE is accessing a CAG cell), which the UE selected from the broadcasted element in the SIB. Additionally, the AMF also receives the TAI(s) and CAG ID(s) broadcasted by the gNB. With a NAS security context, the sent message also be integrity protected. In the case that the initial NAS message was protected and the AMF has the same security context, then steps 2 to 4 may be omitted. In this case, the AMF uses the complete initial NAS message that is in the NAS container as the message to respond to.

Step 2: If the AMF is not able to find the security context locally or from last visited AMF, or if the integrity check fails, then the AMF initiates an authentication procedure with the UE. If the AMF fetches old security context from the last visited AMF, the AMF may decipher the NAS container with the same security context, and get the initial NAS message, then the step 2b to 4 may be omitted. If the AMF fetches new K AMF from the last visited AMF (receiving keyAmfChangeInd), the step 2b may be omitted.

Step 3: If the authentication of the UE is successful, the AMF sends the NAS Security Mode Command message. If the initial NAS message was protected but did not pass the integrity check (due either to a MAC failure or the AMF not being able to find the used security context) or the AMF could not decrypt the complete initial NAS message in the NAS container (due to receiving "keyAmfChangeInd" from the last visited AMF), then the AMF includes in the Security Mode Command message a flag requesting the UE to send the complete initial NAS message in the NAS Security Mode Complete message.

Step 4: The UE sends the NAS Security Mode Complete message to the network in response to a NAS Security Mode Command message. The NAS Security Mode Complete message is ciphered and integrity protected. Furthermore, the NAS Security Mode Complete message includes the complete initial NAS message in a NAS Container if either requested by the AMF or the UE sent the initial NAS message unprotected. The AMF uses the complete initial NAS message that is in the NAS container as the message to respond to.

Step 5: The AMF determines, whether the TAI and CAG ID selected by UE is in the gNB broadcasted list. If the UE selected TAI and CAG ID are not listed in the gNB broadcasted list, then the AMF sends a NAS reject response message with an indication to search for a new suitable cell other than the current camped cell. If the UE selected TAI and CAG ID are listed, then the AMF sends its response to the Initial NAS message. Response message is ciphered and integrity protected.

### 6.x.3 Evaluation

This solution addresses the requirements in key issue#3, key issue#7 and the MitM attack identified as a result of agreed CR in SA2 (S2-2004454). The proposal has minimal impact at the Access node and core network.

***\*\*\*\*\*End of Change\*\*\*\*\****