**3GPP TSG-SA3 Meeting #102bis-e *S3-211030r1***

**e-meeting, 1- 5 March 2021**

**Source: Apple**

**Title: Conclusion for key issue#2**

**Document for: Approval**

**Agenda Item: 2.1**

1 Decision/action requested

***It is proposed to add the conclusion for key issue#2 in 5GFBS TR 33.809.***

2 References

Null

3 Rationale

This pCR proposes to add the conclusion for key issue#2.

There are several solutions addressing key issue#2, including the following:

Solution#7: Verification of authenticity of the cell

Solution#9: Using symmetric algorithm with assistance of USIM and home network

Solution#11: Certificate based solution against false base station

Solution#12: ID based solution against false base station

Solution#14: Shared key based MIB/SIBs protection

Solution #19: AS security based MIB/SIBs integrity information provided by gNB

Solution #20: Digital Signing Network Function (DSnF)

Solution #21: Certificate based solution against false base station for Non-Public Networks

1)For Solution#7, #9, #11, #12, #20, #21, they propose to use signature-based solutions to protect the system information, even though with different technical details. The security attack committed by false base stations include tempering, replaying, etc., thus leading to the threats including DoS attack on both UE and network, rogue services and also privacy issues. In order to detect the tempering, when UE receives those MIB/SIBs, integrity protection is the only way to address this problem. During the discussion in previous SA3 meetings, the signature-based solutions have been discussed thoroughly on different parts of the complete solution, including the credentials provisioning, DS (Digital signing) signing entity, DS verification, etc. Both the advantages and the drawbacks of the solutions are analyzed. Therefore, it is proposed to move forward with the signature-based solutions.

Meanwhile some technical details have not be reached consensus yet. Since there are corresponding countermeasures in the current TR, it is proposed to address those details in normative phase.

2) For Solution#14 and #19, they propose to reuse the AS/NAS based solutions to solve the issue, i.e. UE reports the hash of MIB/SIBs it has received before to the visited network after the AS SMC in solution#14, or in solution#19, gNB sends the hash of MIB/SIBs to the UE after AS SMC. Even though those solutions help to provide some information to the network/UE on the genuine MIB/SIB, they cannot help to detect whether the MIB/SIB are genuine when UE receives them before the AS/NAS SMC. Therefore, they cannot protect UE in the IDLE mode, which means they cannot fully fulfil the security requirement in the key issue#2.

Given those solutions could still provide the security enhancement by making UE/network be aware of potential FBSs in the surrounding environment, it is beneficial to add those solutions as the enhanced feature on top of signature-based solutions based on consensus.

4 Detailed proposal

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

7 Conclusions

Editor's Note: This clause contains the agreed conclusions.

7.2 Conclusions on Key Issue #2

Following conclusions are made on Key Issue #2 "Security protection of system information":

- It is concluded that signature-based solution (a combined solution among solution#7, #11, #20) are taken as the basis of the normative work. The corresponding technical details are to be addressed in normative phase.

- It is concluded that AS/NAS based solution (a combined solution among solution#14, #19) are taken as enhanced features on top of the signature-based solutions. The corresponding technical details are to be addressed in normative phase.

EN: The actions taken following the detection of the FBS are FFS.

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