**3GPP TSG-SA3 Meeting #100Bis-e *S3-202662-r4***

**e-meeting, 12 – 16 October 2020** merge of S3-202532 and S3-202662

**Source: Nokia, Nokia Shanghai Bell, Philips International, CableLabs**

**Title: pCR to 33.809 – Enhanced Description of Key Issue #7**

**Document for: Approval**

**Agenda Item: 2.1**

# 1 Decision/action requested

***Enhancement of the description of key issue #7 (protection against m-i-t-m false gNB attacks).***

# 2 References

# 3 Rationale

As mentioned in TR 33.809, Key Issue #7, a “sophisticated attacker may launch various types of attacks in a stealth manner using false base stations” operating as Man-in-the-Middle between the network and victim UEs. This pCR further details the description of Key Issue #7.

# 4 Detailed proposal

*\*\*\*\*\* BEGINN OF CHANGES*

## 5.7 Key Issue #7: Protection against Man-in-the-Middle false gNB attacks

### 5.7.1 Key issue details

Typical false base station attacks result in denial of service to UE. Consequently, UE or user may infer such attacks based on the service unavailability and take an action accordingly. However, a more sophisticated attacker may launch various types of attacks in a stealth manner using false base stations. A MitM false gNB transports messages between the UE and the network. For example, it may transport security protected messages without any modification while dropping, altering and/or injecting unprotected messages, such as

– the pre-authentication traffic

– MAC/RLC layer message headers

– lower layer control messages such as buffer status reports

In some situations, a MitM attack mainly works by replaying messages i.e., the MitM sits between the actual base station and a UE and the MitM forwards the messages of the base station towards the UE and the messages of the UE towards the base station. In this position, the MitM might do nothing for a very long time making it very difficult to detect. However, in certain occasions the MitM might inject/alter/drop messages. The basic requirement to defeat MitM attacks is often related to replay protection.

The exact behaviour of a FBS (False Base Station) operating as a MitM false gNB may vary depending on the goals of the attacker. In particular, the degree to which the FBS mimics the impersonated gNB with respect to its radio configuration is unknown. In known attacks that have been done in real networks as a proof of concept rather than with malicious intentions (e.g. [19], [20]), the FBS did not comprise the feature to mimic closely the behaviour of the impersonated gNB. However, this may be different in a true attack, when the attacker takes into account that UE and/or network may implement measures to detect the FBS.

Without addressing the MitM threats, detection of false base stations and countermeasures against them have limited effectiveness.

Note that the authentication relay attack (Key Issue #5) is a special case of a Man-in-the-Middle false gNB attack, using what can be called a “distributed Man-in-the-Middle false gNB”, consisting of a FBS at one location connected to a malicious UE at another location.

A repeater simply forwarding all traffic unchanged is not considered a MitM false base station for the purposes of this key issue. There may be legitimate use for such devices, such as range extension.

### 5.7.2 Security Threats

A MitM false base station may force a UE to camp on to it by passing all the message on between the UE and real base station. It may then deny the UE service, e.g. reject or drop service request, not pass on paging messages etc.

A MitM false base station may perform a linkage attack by SUCI replay, i.e. replace a SUCI in a registration request or in an identity response by a previously captured SUCI and observe whether the UE will be authenticated and receive service.

### When UP integrity protection is not used, a MitM false base station may further perform attacks like aLTEr [20] or IMP4GT [19], i.e. trick the UE into accessing malicious websites or even impersonating the UE on the IP layer, which includes decryption of downlink traffic and performing encryption of faked uplink traffic.5.7.3 Potential Requirements

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