**3GPP TSG SA WG3 (Security) Meeting #94Ad-Hoc S3-190793**

**Stockholm (Sweden), 11-15 March 2019** *revision of S3-190381*

**Source: Qualcomm Incorporated**

**Title: Protection against Man-in-the-Middle false base station attacks**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the key issue***

# 2 References

[1] TR 33.809 Study on 5G security enhancements against false base stations

# 3 Rationale

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. MitM false gNB transports security protected messages between the UE and the network without any modification while altering unprotected messages.

We note that the MitM attack does not need to use a false base station and a malicious UE that connect with each other via a private channel to transport the traffic between the victim UE and the real network as described in KI #5: mitigation against the authentication relay attack. Instead, the MitM base station impersonates the legitimate base station that the UE is supposed to connect to at the current location, in order to avoid any potential detection (e.g., based on the location) by the UE.

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

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [1].

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

## 5.x Key issue #x: Protection against Man-in-the-Middle false gNB attacks

### 5.x.1 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. MitM false gNB transports security protected messages between the UE and the network without any modification while altering and/or injecting unprotected messages.

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

### 5.x.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.

### 5.x.3 Potential security requirements

Proposed solutions in the present document, when applicable, shall be evaluated against the MitM attack.

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