**3GPP TSG-SA3 6G Workshop**

**Conference Calls on 6G SID preparation, 6 - 7 August 2025**

**Source: SK telecom**

**Title: New Work Task on 6G security enhancement against False Base Station (FBS)**

**Document for: Discussion**

# 1 References

[1] TR 33.846 V17.0.0, ‘Study on authentication enhancements in the 5G System’, Release 17.

[2] TR 33.809 V18.1.0, ‘Study on 5G security enhancements against False Base Stations (FBS)’, Release 18.

[3] TR 22.870 V0.3.1, ‘Study on 6G Use Cases and Service Requirements’, Release 20.

# 2 Justification

In Rel-17, SA3 has carried out study on authentication enhancements in the 5G System [1]. Also, in Rel-18, SA3 has carried out study on 5G security enhancements against False Base Stations [2]. However, these potential attack points from FBS still remains in current 5G network, since there is no follow-up normative work of these topics until now. The biggest reason why normative work of security enhancement against FBS has not been done in 5G is most of candidate solutions require fundamental security protocol changes (e.g., public key infrastructure based base station certification) which cannot be easily applied to legacy 5G infrastructure, UE and USIM.

At the same time, there is also an increasing trend with cyber security threats and attacks over telecom systems, e.g., a recent malware attack over the subscription data management system led to massive subscriber data breach. If this leaked subscriber data is used by the potential attacker in combination with the existing attack points of FBS in current 5G specification, it makes more difficult to protect customer privacy information without any exception.

In contrast to 5G, 6G study in SA3 represents an opportunity to revisit the foundations of security protocol design, free from the constraints of backward compatibility. Also, SA1 already discussed on the potential new requirement for security enhancement against FBS for 6G and it is captured in [3]. Therefore, it is a right time to re-start the study of security enhancement against FBS targeting 6G in SA3.

# 3 Objectives

It is proposed that the SA3 6G security study shall include the following security work tasks by reusing existing 5G study results as much as possible:

* + - Rel-18 TR 33.809, ‘Study on 5G security enhancements against False Base Stations (FBS)’
    - Rel-17 TR 33.846, ‘Study on authentication enhancements in the 5G System’

The work tasks for this study are:

* **WT #1:** Study 6G security enhancement against False Base Station (FBS) including
  + - Study whether and how to support the protection on MIB/SIB, initial RRC, NAS REJECT message  
      (e.g., the verification of base station authenticity prior to starting the registration procedure)
    - Study whether and how to mitigate likability attack in Authenticated Key Agreement (AKA) procedure  
      (e.g., user identification with replayed SUCI based on AKA success/fail, error type: MAC/Synch fail)