**3GPP TSG-SA3 Meeting #108adhoc-e *S3-222655***

**e-meeting, 10 – 14 Oct 2022**

**Source: Apple**

**Title: Editorial - Mapping between key issues and solutions**

**Document for: Approval**

**Agenda Item: 5.1**

1 Decision/action requested

***It is proposed to add the update in 5GFBS TR 33.809.***

2 References

Null

3 Rationale

Null

4 Detailed proposal

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

6 Candidate Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

6.0 Mapping between key issues and solutions

|  |  |
| --- | --- |
| Solutions | Key Issues |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Solution #1: Protection for the UE Capability Transfer | x |  |  |  |  |  |  |
| Solution #2: Protection of RRCReject message in RRC\_INACTIVE state  | x |  |  |  |  |  |  |
| Solution #3: Protection of uplink UECapabilityInformation RRC message  | x |  |  |  |  |  |  |
| Solution #4: Enriched measurement reports  |  |  | x |  |  |  |  |
| Solution #5: Mitigation against the authentication relay attack  |  |  |  |  | x |  |  |
| Solution #6: Avoiding UE connecting to false base station during HO  |  |  | x |  |  |  |  |
| Solution #7: Verification of authenticity of the cell  |  | x |  |  |  |  |  |
| Solution #8: Network detection of nearby false base stations from call statistics and measurements  |  |  | x |  |  |  |  |
| Solution #9: Using symmetric algorithm with assistance of USIM and home network  | x | x |  |  |  |  |  |
| Solution #10: Protection on the unicast message based on ECDH  | x |  |  |  |  |  |  |
| Solution #11: Certificate based solution against false base station  | x | x |  |  |  |  |  |
| Solution #12: ID based solution against false base station  | x | x |  |  |  |  |  |
| Solution #13: Protecting RRCResumeRequest against MiTM  | x |  |  |  |  |  |  |
| Solution #14: Shared key based MIB/SIBs protection  |  | x |  |  |  |  |  |
| Solution #15: Mitigation against the authentication relay attack with different PLMNs  |  |  |  |  | x |  |  |
| Solution #16: Protection of RRC Reject Message  | x |  |  |  |  |  |  |
| Solution 17: Integrity protection of the whole RRCResumeRequest message  | x |  |  |  |  |  |  |
| Solution #18: Avoiding UE connecting to False Base Station during Conditional Handover  |  |  | x |  |  |  |  |
| Solution #19: AS security based MIB/SIBs integrity information provided by gNB  |  | x |  |  |  |  |  |
| Solution #20: Digital Signing Network Function (DSnF)  |  | x |  |  |  |  |  |
| Solution #21: Certificate based solution against false base station for Non-Public Networks  | x | x |  |  |  |  |  |
| Solution #22: Detecting false base stations based on UE positioning measurements  |  |  | x |  |  |  |  |
| Solution #23: Cryptographic CRC to avoid MitM relay nodes  |  |  | x |  | x |  | x |
| Solution #24: UE&Network-assisted UE avoidance and Network detection of FBS  |  |  | x |  |  |  |  |
| Solution #25: Detection of Man-in-the-Middle false base stations  |  |  | x |  |  |  |  |
| Solution #26: KI#2 with PKC-based and without tight time synchronization  |  | x |  |  |  |  |  |
| Solution #27: Short-lived asymmetric key-based solution for protecting system information  |  | x |  |  |  |  |  |

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