**3GPP TSG-SA3 Meeting #116S3-242490**

**Jeju, South Korea, 20 May - 24 May, 2024**

**Source: Google**

**Title: Proposal to remove Editor’s Note and update solution in TR 33.701**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***Approve the pCR to TR 33.701***

# 2 References

[1] TR 33.701 Study on mitigations against bidding down attacks

# 3 Rationale

This contribution proposes to remove an Editor’s Note from a proposed a solution for key issue #1. The objective of KI#1 is to mitigate the risk of bidding down attacks from LTE/NR to decommissioned GERAN/UTRAN.

# 4 Detailed proposal

\*\*\*\*\*\*\*\* Start of Change #1 \*\*\*\*\*\*\*\*

### 5.3.1 Solution details



**Figure 6.3.1-1: Message flow showing steps to avoid UEs from connecting to decommissioned RATs**

In the above message flow, the message flow till NAS Security context establishment is as per legacy procedures. This message flow includes the possible scenario when, as soon as UE powers on, UE connects with a FBS which can perform bidding down attack to a decommissioned RAT.

* After NAS registration is complete, as part of NAS registration accept, the serving network informs the UE about the decommissioned RATs.
* UE updates the cell search criteria according to the list of decommissioned RATs to ensure that it does not select any cell belonging to those RATs.
* If UE has received a non-empty list of decommissioned RATs, it aborts that connection.

Editor's Note: the need for a UE to restart the connection after it gets the list of decommissioned RATs list is FFS.

Editor's Note: how a UE can abort the RRC connection is FFS.

* + Subsequently, UE performs fresh cell search where it ignores / de-prioritizes decommissioned RATs. Subsequently, the legacy procedure ensures that the UE does not connect to decommissioned RATs, and connects to a valid RAT.
* After UE moves to RRC Idle state, when it goes through the RRC connection procedure again and if it receives RRC redirection message it can ignore that message.

Editor’s Note: The UE will use this information to prevent downgrades to the decommissioned PLMNs. Implementation details are left to the UE specific implementation.

Editor's Note: whether an FBS can redirect the connected victim UE to 2/3G RATs is FFS.

\*\*\*\*\*\*\*\* End of Change #1 \*\*\*\*\*\*\*\*