**3GPP TSG-SA3 Meeting #116S3-242513**

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

**Source: Google**

**Title: Propose to update a new solution text 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 a change in an approved new solution for TR 33.701.

# 4 Detailed proposals

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

#  5.9.2 Solution details

Steering of roaming (SoR) allows the HPLMN to update the "Operator Controlled PLMN Selector with Access Technology" list in the UE by providing the HPLMN protected list of preferred PLMN/access technology combinations via NAS signalling, which is described in Annex C (normative) in TS 23.122 [5].

After the operator has decommissioned the GERAN or UTRAN, they can reuse the existing SoR procedures to notify the UE to update the "Operator Controlled PLMN Selector with Access Technology," which indicates the PLMN list and whether the related access technology is valid or invalid. The SoR transparent container is described in 9.11.3.51 in TS 24.501 [6].

The UE will use this list for PLMN selection, as outlined in clause 4.4.3.1.1 in TS 23.122 [5]. The order of priority for PLMN selection is: 1) available HPLMN or EHPLMN; 2) user-controlled list; 3) operator-controlled list (updated by the SoR procedure); 4) other PLMN/RAT with high quality; 5) other PLMN/RAT in order of decreasing signal quality; 6) disaster condition (only if UE support MINT).

However, the UE can still select the PLMN/RAT not included in the operator-controlled list as for 4) and 5), which may lead to a bidding down attacks due to a potential decommissioned RAT and FBS. Thus, it is proposed that the user can configure the UE to support bidding down attack mitigation, and once it is activated, the UE shall not select the RATs that are invalid in the network according to the operator-controlled list, e.g. for the PLMN/RAT in case 4) and 5).

NOTE: It is left to UE implementation whether the user can configure the UE to support bidding down attack mitigation.

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