**3GPP TSG-CT WG1 Meeting #141eC1-232307**

**Online 17– 21 April 2023**

Title: Reply LS on Research highlighting potential 5G and 4G Bidding Down Attacks

Response to: Research highlighting potential 5G and 4G Bidding Down Attacks (CVD-2022-0064)

Release: Rel-18

Work Item: SAES18

Source: CT1

To: GSMA CVD

Cc: SA3, RAN2

**Contact person:**

Name: Mikael Wass

Tel. Number:

E-mail Address: mikael.wass@ericsson.com

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

Attachments: None.

**1. Overall Description:**

CT1 would like to thank GSMA CVD for the LS on Research highlighting potential 5G and 4G Bidding Down Attacks. CT1 has discussed “Finding 2 - Security Capabilities handling in MME” which is in CT1 remit and would like to provide the following feedback.

CT1 agrees [RZ: do you mean: "agrees" or "confirms"?] that MME is not mandated to check/verify the UE indicated supported 5G security algorithms. These algorithms are not used in the EPS part of the network to which the UE requests connectivity. Using the HashMME mechanism ensures that the UE indicated 5G security information is correctly received by the MME. If the MME supports the receipt of UE indicated 5G security algorithms, the 5G security information is subsequently replayed EPS security protected to the UE, and transparently transported in the network and can be assessed where used (dual connectivity with NR in RAN or for N1 mode). By the specified functionality, 5G security algorithm support is not required in EPS, and the assessment and activation of specific 5G security algorithms are limited to the parts of the network where these algorithms are supported and used. [RZ: I don't think we should add the following to the LS, but this is how it works: "If the MME does not support the receipt of UE indicated 5G security algorithms, the parts of the network where these algorithms are used either derive the supported 5G security algorithms from the supported EPS security algorithms or they assume that the UE supports at least the mandatory set of 5G security algorithms defined in TS 33.501."]

The evaluation in MME of the UE indicated supported EPS security algorithms is based on the security required by the network to provide service to a UE. If the UE indicated EPS security capabilities do not match the capabilities required by the network for connectivity to EPS, then TS 24.301 clause 5.5.1.2.7 case j applies, and the UE connectivity request will be rejected.

**2. Actions:**

**To GSMA** **CVD group.**

**ACTION:** CT1 asks GSMA CVD group to take the above information into account.

**3. Date of Next CT1 Meetings:**

**3. Date of Next CT1 Meetings:**

CT1#142 22nd – 26th May 2023 Bratislava

CT1#143 21st – 25th August 2023 Goteborg

CT1#144 9th – 13th October 2023 China (TBC)

CT1#145 13th – 17th November 2023 Chicago