**3GPP TSG SA WG3 Meeting #98e draft\_S3-200162-r1**

**e-meeting, 2-6 March 2020** revision S3-20abcd

**Source: Huawei, HiSilicon Lenovo, Motorola Mobility**

**Title: Adding privacy procedures for V2X groupcast communication.**

**Document for: Approval**

**Agenda Item: 3.15**

1 Decision/action requested

***This contribution proposes some text for groupcast security based on solution#20***

2 References

[1] 3GPP TR 33.836: “Study on Security Aspects of 3GPP support for Advanced V2X Services”, V0.5.0

[2] 3GPP TS 33.536: “Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services”

3 Rationale

Based on the 3GPP TS 23.287, when the group identifier information is provided by the V2X application layer, the V2X UE converts the provided group identifier into a destination Layer-2 ID. The group ID conversion procedure shall be protected from linking back to the group identifier. The destination Layer-2 ID shall be updated regularly as well to ensure privacy of the group members. Solution #20 covers both the requirements of KI#4 and in part of KI#3 in TR 33.836[1]. Hence we propose the following addition to TS 33.536 [2].

Document S3-200161 addresses all the editor’s comments and summarizes the advantages and shortcomings of solution #20.

4 Detailed proposal

It is proposed that SA3 agree the below pCR for inclusion in the TS [2].

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

5.4 Security for groupcast mode

5.4.3 Procedures

5.4.3.1 Security procedures

There are no security procedures defined for the PC5 bearer for groupcast mode.

5.4.3.2 Privacy procedures

The below privacy procedures follows the privacy mechanism defined in TS 33.185 [5] for V2X LTE which is intended to mitigate against the threat of tracking the UE by an attacker based on its used source identities.

The UE shall change and randomize its source Layer-2 ID and source IP address (if used) when V2X application indicates that the Application Layer ID has changed. The UE may change and randomize its source Layer-2 ID and source IP address (if used) at other times (e.g. see clause 5.6.1.1 in TS 23.287 [2]). The UE shall provide an indication to the V2X application layer whenever the source Layer-2 ID and/or source IP address are changed.

The UE shall convert the group identifier provided by the application layer to the destination Layer-2 ID and update it using a hash function and a random number from a set of random numbers. The set of random numbers and the time interval to trigger the update of the destination Layer-2 ID are provisioned to the group members by the application layer when the group is formed and every time group ID is updated.

NOTE: The size of the set of random numbers is allocated based on how frequently the group identifier is updated.

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*