**3GPP TSG-SA3 Meeting #100bis-e *S3-202393-r2***

**e-meeting, 12 – 16 October 2020** Revision of S3-202393-r1

**Source:** **Huawei, Hisilicon, CATT, Lenovo, Motorola Mobility**

**Title: New key issue on groupcast security**

**Document for: Approval**

**Agenda Item: 2.9**

# Decision/action requested

***This contribution proposes a new key issue on groupcast security and privacy***

2 References

[1] 3GPP TR 23.752: “Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)”, V0.4.0

3 Rationale

Based on the 3GPP TR 23.752, when the group identifier information is provided by the ProSe application layer, the lead UE converts the provided group identifier into a destination Layer-2 ID for groupcast communication. The group ID conversion procedure shall be protected from linking back to the group identifier.

4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## X.Y Key Issue #Y: Security and privacy of groupcast communication

### X.Y.1 Key issue details

In TR 23.752 [x1], Solution #22 "V2X-based group communication for commercial services" mentions the following note:

*“NOTE 2: The mechanism for converting the ProSe application layer provided group identifier to the destination Layer-2 ID depends on the conclusion of KI#8.”*

Solution #37 “Groupcast mode communication for commercial services and public safety” and solution#4 “PC5 group communication for commercial services”, also mentions the provisioning of Application layer group ID and the corresponding Destination L2-IDs in collaboration with the application server.

Thus far solution #7, #35 and #36 have been proposed for KI#8 “Support of PC5 Service Authorization and Policy/Parameter Provisioning” but do not address the conversion mechanism for application layer group ID to the destination L2 ID.

This conversion/mapping procedure should be secured in terms of privacy and traceability. Unless the conversion is carefully performed, the group membership of specific UEs could be disclosed. For example, attackers might be able to make an inquiry whether any member of certain group are exists in some location.

Also, for group communications, UEs are able to start communication without first discovering the receiving UE(s). This means that a UE can unilaterally start sending encrypted one-to-many data packets, which may be successfully decrypted by other group members without knowing in advance which group members can actually receive the data. Security for one-to-many direct communication in LTE Prose is specified in TS 33.303 [6]. However, it should be studied how to accommodate such procedures to 5G Prose.

In 5GS, ProSe services can be used for both public safety services and commercial services (e.g. interactive service). In TR 23.752 [2], group communications for commercial services has been studied. Therefore, the security of ProSe group communications for commercial services needs to be considered.

### X.Y.2 Security threats

If the group IDs are not securely converted by the application layer, the intruder can link them back to UE groupcast memberships, revealing which UEs have been associated with a specific group and hence causes privacy attacks.

Failures to protect groupcastcommunications, the following threats are identified:

- Passive attackers can eavesdrop on data packets exchanged between UEs.

- Active attackers can intercept, modify or replay data packets exchanged between UEs.

- An UE as a group member may be impersonated by an attacker.

### X.Y.3 Potential security requirements

5G system shall ensure that the group IDs and L2 IDs are protected from linkability and traceability attacks for ProSe groupcast communications.

One-to-many communications between ProSe-enabled UEs shall be protected by confidentiality and integrity.

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