**3GPP TSG-SA3 Meeting #102-e *S3-210206-r1***

**e-meeting, 18 - 29 January 2021** Revision of S3-21xxxx

**Source: Huawei, HiSilicon**

**Title: Propose to Resolve EN1 in Solution #17**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve EN in Solution#17 in TR 33.847***

# 2 References

[1] 3GPP TS 33.847 Study on security aspects of enhancement for proximity based services in the 5G System (5GS).

# 3 Rationale

The contribution proposes to delete the first EN of solution #17. The solution does not rely on the groupcast security. The very purpose of the solution is to ensure the group IDs and the L2 IDs are protected in tems of linkability, tracebility and privacy even when the groupcast security is not enabled. Only the authorised members are able to receive the group ID and corresponding information required to calculate the corresponding L2 IDs. The group creation and management, including the group announcement message is the scope of application layer.

# 4 Detailed proposal

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

6.17 Solution #17: Solution on securely creating destination Layer-2 ID in groupcast communication

6.17.1 Introduction

This solution addresses the KI #13 "Security and privacy of groupcast communication". This solution ensures that the group IDs and the L2 IDs are protected in tems of linkability, tracebility and privacy even when the groupcast security is not enabled. The group creation and management, including the group announcement message is the scope of application layer.

6.17.2 Solution details

The detailed solution is illustrated in Figure.

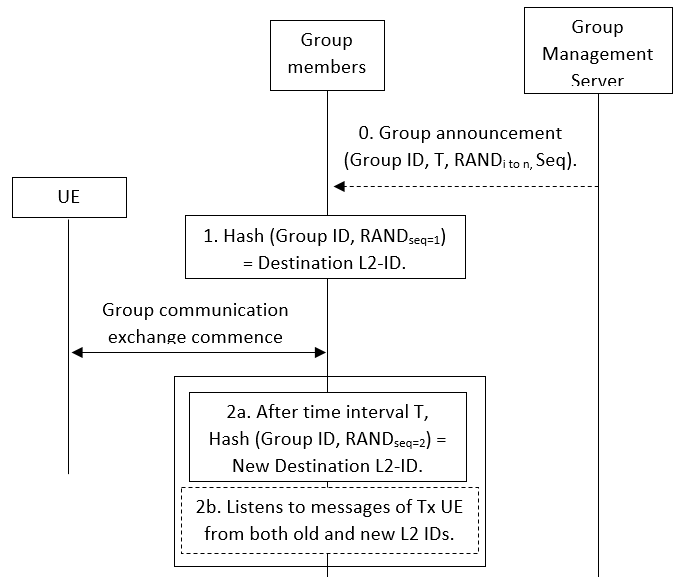
****

Figure 6.17.2-1: Procedure for secure conversion of application layer group ID to destination Layer-2 ID

0. Group Setup: Once the group is created, the group management server will send the application layer group ID to the associated UEs and a timer T. It will also send a set of random numbers and a specific sequence in which these random number are to be used. It is assumed that the application layer signalling is protected.

1. ID Conversion: All the UEs use the application layer group ID and the first random number according to the sequence as an input to a hash function to generate the destination Layer-2 ID.

2. ID Update: When the timer T expires, a new destination Layer-2 ID is calculated using the next random number according to the sequence. The UEs can listen to both old a new destination Layer-2 IDs, to avoid any time synchronization issues, for a certain period of time or until receives a message with the new ID.

The destination Layer-2 ID is updated until the ProSe application layer changes the group ID.

The group management server can also send the corresponding materials to generate random numbers rather than sending the random numbers itself.

Editor’s Note: time synchronization among group members is FFS

6.17.3 Evaluation

TBA.

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