**3GPP TSG-SA3 Meeting #102-e *S3-210207-r1***

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

**Source: Huawei, HiSilicon**

**Title: Propose to resolve ENs 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).”

[2] 3GPP TS 23.434 “Service Enabler Architecture Layer for Verticals (SEAL) Functional architecture and information flows.”

[3] 3GPP TS 29.343 “Proximity-services (ProSe) function to ProSe application server aspects”.

# 3 Rationale

The contribution proposes to delete the second EN in solution#17. Our solution allows the UEs to listen to the messages from both the L2 IDs after conversion for a set timer that ensures that no meesages are lost and there is no interference to the application layer communication. Thus ensuring synchronization among group members.

The group creation and group management are conducted by the application layer TS 23.434 [2] and TS 29.343 [3]. The message 0 as presented in the figure is from the application layer specification. Hence the time synchronization for the members of the group while calculating the destination L2 IDs is not the scope of this solution. The synchronization of the members while calculating multiple L2 IDs introduced by our solution has been addressed by listening to both the older and new L2 IDs as mentioned in step 2.

# 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".

6.17.2 Solution details

The detailed solution is illustrated in Figure.

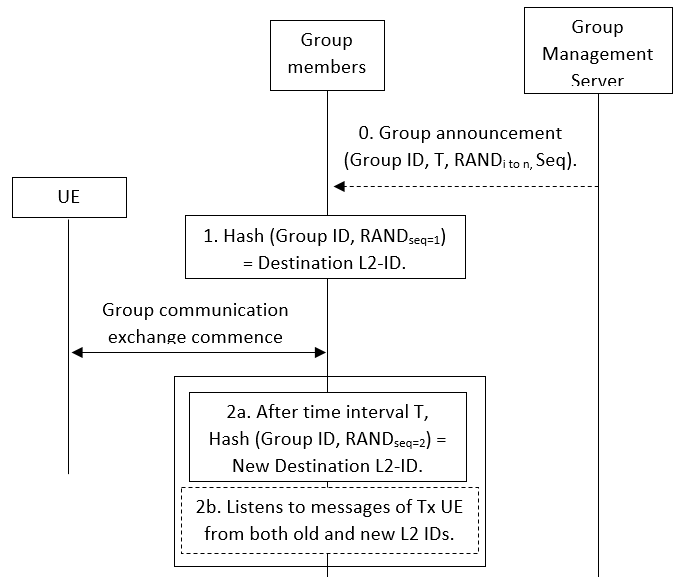
****

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 message 0 as presented in the figure is from the application layer specification. Hence the time synchronization for the members of the group while calculating the destination L2 IDs during the first conversion is not in the scope of this solution.

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: security for group management (including message 0 in the figure) is FFS

6.17.3 Evaluation

TBA.

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