**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202954-r1***

**e-meeting, 9 - 20 November 2020** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: Update Sol#3 to resolve EN**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve EN to solution#3 in TR 33.847***

# 2 References

N/A

# 3 Rationale

The contribution proposes to resolve the following EN in the Solution #3:

Editor’s note: It’s FFS how to support the security flexibility.

Two UEs should finish the discovery authorisation and the direct one-to-one communication establishment before actually starting direct one-to-one communication (i.e. the discovery request procedures are prerequisite steps of direct one-to-one communication). Security flexibility is provided by introducing on-demand PC5 unicast policies. However the security policies mismatch may cause one-to-one communication establishment failure and make the previous discovery request procedures in vain. To avoid resource waste caused by policy mismatch, this contribution proposes to check the policy match in advance with the help of the discovery request procedures.

The contribution captures some editorial changes in step 15 as well.

# 4 Detailed proposal

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

## 6.3 Solution #3: Reuse LTE security mechanism for 5G ProSe open discovery

### 6.3.1 Introduction

This solution addresses Key Issue #1(Discovery message protection). It proposes to reuse the open discovery security mechanism specified in TS 33.303 [6] for 5G ProSe open discovery. This solution does not address UE-to-Network and UE-to-UE relay discovery.

In LTE ProSe, the ProSe function is used to provide the UE with the necessary security material in order to protect discovery messages transmitted over the air. In 5G ProSe, the 5G Direct Discovery Name Management Function (DDNMF) is used to replace the ProSe function in the open discovery.

Editor’s note: It is FFS how this solution will perform out of coverage.

Editor’s note: How to derive the discovery key is FFS.

Editor’s note: Whether this solution based on CP or UP is FFS.

Editor’s note: It’s FFS about new security parameters for 5G that is different from LTE ProSe.

Editor’s note: The detailed security-related parameters in the announcing message are FFS.

The on-demand PC5 unicast policy gives security flexibility but may lead policy mismatch during during one-to-one communication establishment. To mitigate the policies mismatch, the policy match is checked in advance during discovery procedures.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.3.2 Solution details

The open discovery security procedure is described as follows:

1. The announcing UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN in order to be allowed to announce a code on its serving PLMN (either VPLMN or HPLMN).
2. If the announcing UE wants to send announcements in the VPLMN, the DDNMF in the HPLMN requests authorization from the VPLMN DDNMF by sending Announce Auth.() message.
3. VPLMN DDNMF responds with an Announce Auth. Ack () message.
4. The DDNMF in HPLMN of the announcing UE returns the ProSe App Code that the announcing UE can announce and a Discovery Key associated with it. The DDNMF stores the Discovery Key with the ProSe App Code. In addition, the DDNMF provides the UE with a CURRENT\_TIME parameter, which contains the current UTC-based time at the DDNMF, a MAX\_OFFSET parameter, and a Validity Timer. The UE sets a clock which is used for ProSe authentication (i.e. ProSe clock) to the value of CURRENT\_TIME and the UE stores the MAX\_OFFSET parameter, overwriting any previous values. The announcing UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB16, NITZ, NTP, GPS, via Ub interface (in GBA) (depending on which is available).
5. The UE starts announcing, if the difference between UTC-based counter provided by the system associated with the discovery slot and the UE’s ProSe clock is not greater than the MAX\_OFFSET and if the Validity Timer has not expired. For each discovery slot it uses to announce, the announcing UE calculates a 32-bit Message Integrity Check (MIC) to include with the ProSe App Code in the discovery message. Four least significant bits of UTC-based counter are transmitted along with the discovery message. The MIC is calculated as described in clause A.2 of TS 33.303 [6] using the Discovery Key and the UTC-based counter associated with the discovery slot.
6. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN in order to get the Discovery Filters that it wants to listen for.
7. The DDNMF in the HPLMN of the monitoring UE sends Monitor Req. message to the DDNMF in the HPLMN of the announcing.
8. The DDNMF in the HPLMN of the announcing UE sends Monitor Resp. message to the DDNMF in the HPLMN of the monitoring.
9. The DDNMF returns the Discovery Filter containing either the ProSe App Code(s), the ProSe App Mask(s) or both along with the CURRENT\_TIME and the MAX\_OFFSET parameters. The UE sets its ProSe clock to CURRENT\_TIME and stores the MAX\_OFFSET parameter, overwriting any previous values. The monitoring UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB16, NITZ, NTP, GPS (depending on which is available).
10. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the difference between UTC-based counter associated with that discovery slot and UE’s ProSe clock is not greater than the MAX\_OFFSET of the monitoring UE's ProSe clock.
11. On hearing such a discovery message, and if the UE needs to check the MIC for the discovered ProSe App Code, the Monitoring UE sends a Match Report message to the DDNMF in the HPLMN of the monitoring UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the monitoring UE’s UTC-based counter associated with the discovery slot where it heard the announcement, other discovery message parameters including the ProSe App Code and MIC, and the security policies of the monitoring UE for direct one-to-one communication service related to the ProSe App Code.
12. The DDNMF in the HPLMN of the monitoring UE passes the discovery message parameters including the ProSe App Code, MIC, associated counter parameter and the security policies of the monitoring UE in step 11 to the DDNMF in the HPLMN of the announcing UE in the Match Report message.
13. The DDNMF in the HPLMN of the announcing UE shall check the MIC is valid. The DDNMF in the HPLMN also gets the security policies of the announcing UE for direct one-to-one communication service related to the ProSe App Code from PCF, and checks if the security policy of the monitoring UE match the policy of the announcing UE.
14. If the MIC check and the security policy match check passes, the DDNMF in the HPLMN of the announcing UE shall acknowledge a successful check of the MIC to the DDNMF in the HPLMN of the monitoring UE in the Match Report Ack message, otherwise it shall acknowledge check failure.
15. The DDNMF in the HPLMN of the monitoring UE acknowledges the check result to the monitoring UE.



Figure 6.3.2-1: Open discovery security procedure

### 6.3.3 Evaluation

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*