**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202955-r1***

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

**Source: Huawei, HiSilicon**

**Title: Update to Sol#4 to resolve EN**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve an EN to solution#4 in TR 33.847***

# 2 References

N/A

# 3 Rationale

The contribution proposes to resolve the following EN in the Solution #4 to KI#1:

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.

# 4 Detailed proposal

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

## 6.4 Solution #4: Reuse LTE security mechanism for 5G ProSe restricted discovery

### 6.4.1 Introduction

This solution addresses Key Issue #1(Discovery message protection). It proposes to reuse the restricted discovery security mechanisms of Model A and Model B specified in TS 33.303 [6] for 5G ProSe restricted 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 restricted discovery.

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

Editor’s note: It’s FFS how this mechanism can be used in UE-to-Network and UE-to-UE relay discovery scenarios.

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.4.2 Solution details

#### 6.4.2.1 Model A restricted discovery

The security procedure for Model A restricted discovery is described as follows:

Steps 1-4 refer to an Announcing UE.

1. Announcing UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material. The announcing UE shall include its security policies for direct one-to-one communication of the service related to the RPAUID.
2. The DDNMF may check for the announce authorization with the ProSe Application Server. If the Discovery Request is authorized, the DDNMF stores the security policies received from step 1.
3. If the Announcing UE is roaming, the DDNMFs in the HPLMN and VPLMN of the Announcing UE exchange Announce Auth.
4. The DDNMF in the HPLMN of the Announcing UE returns the ProSe Code and the corresponding Code-Sending Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 5-10 refer to a Monitoring UE

1. The Monitoring UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application IDs. The monitoring UE shall include its security policies for direct one-to-one communication of the service related to RPAUID.
2. The DDNMF in the HPLMN of the Monitoring UE sends an authorization request to the ProSe Application Server. If, based on the permission settings, the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.
3. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the DDNMF in the HPLMN of the Monitoring UE contacts the indicated PLMN’s DDNMF i.e. the DDNMF in the HPLMN of the Announcing UE, by sending a Monitor Request message. The Monitor Request includes the security policies received in step 5.
4. The DDNMF in the HPLMN of the Monitoring UE may exchange authorization messages with the ProSe Application Server.
5. The DDNMF in the HPLMN of the Announcing UE shall first check if the security policies provided by the DDNMF of the monitoring UE match the security policies of the announcing UE, the DDNMF in the HPLMN of the Announcing UE responds to the DDNMF in the HPLMN of the Monitoring UE with a Monitor Response message including the ProSe Code, the corresponding Code-Receiving Security Parameters and an optional Discovery User Integrity Key (DUIK) if the Monitoring UE’s security policies match the Announcing UE’s security policies. The DDNMF in the HPLMN of the Announcing UE shall reject the monitor request if the security policies between the Announcing UE and the Monitoring UE do not match. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates the same PLMN, then the DDNMF does the match check locally.
6. The DDNMF in the HPLMN of the Monitoring UE returns the Discovery Filter and the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 11 and 12 occur over PC5.

1. The UE starts announcing.
2. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter. If the Monitoring UE was asked to send Match Reports for MIC checking, it proceeds to step 13.

Steps 13-16 refer to a Monitoring UE that has encountered a match.

1. The Monitoring UE sends a Match Report message to the DDNMF in the HPLMN of the monitoring UE.
2. The DDNMF in the HPLMN of the Monitoring UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Monitoring UE is authorised to discover the Announcing UE.
3. The DDNMF in the HPLMN of the monitoring UE returns to the Monitoring UE an acknowledgement that the integrity check passed.
4. The DDNMF in the HPLMN of the Monitoring UE may send a Match Report Info message to the DDNMF in the HPLMN of the Announcing UE.



Figure 6.4.2.1-1: Model A restricted discovery security procedure

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.4.2.2 Model B restricted discovery

The security procedure for Model B restricted discovery is described as follows:

Steps 1-4 refer to a Discoveree UE.

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to get the ProSe Code to announce and associated security material. The Discoveree UE shall include its security policies for direct one-to-one communication of the service related to the RPAUID.
2. The DDNMF may check for the announce authorization with the ProSe Application Server depending on DDNMF configuration. If the Discovery Request is authorized, the DDNMF stores the security policies received from step 1.
3. The DDNMFs in the HPLMN and VPLMN of the Discoveree UE exchange Announce Auth. messages. If the Discoveree UE is not roaming, these steps do not take place.
4. The DDNMF in the HPLMN of the Discoveree UE returns the ProSe Response Code and the Code-Sending Security Parameters, Discovery Query Filter(s) and their Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 5-10 refer to a Discoverer UE

1. The Discoverer UE sends a Discovery Request message containing the RPAUID to the DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application IDs. The Discoverer UE shall include its security policies for direct one-to-one communication of the service related to RPAUID.
2. The DDNMF in the HPLMN of the Discoverer UE sends an authorization request to the ProSe Application Server. If the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.
3. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the DDNMF in the HPLMN of the Discoverer UE contacts the indicated PLMN’s DDNMF i.e. the DDNMF in the HPLMN of the Discoveree UE, by sending a Discovery Request message. The Discovery Request includes the security policies received in step 5.
4. The DDNMF in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.
5. The DDNMF in the HPLMN of the Discoveree UE shall first check if the security policies provided by the DDNMF of the Discoverer UE match the security policies of the Discoveree UE, the DDNMF in the HPLMN of the Discoveree UE responds to the DDNMF in the HPLMN of the Discoverer UE with a Discovery Response message including the ProSe Query Code(s) and their associated Code-Sending Security Parameters, ProSe Response Code and its associated Code-Receiving Security Parameters, and an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code if the Discoverer UE’s security policies match the Discoveree UE’s security policies. The DDNMF in the HPLMN of the Discoveree UE shall reject the monitor request if the security policies between the Discoveree UE and Discoverer UE do not match. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates the same PLMN, then the DDNMF does the match check locally.

NOTE: The definition of security policy (i.e. REQUIRED/PREFERRED/NOT NEEDED) and whether security policies match to each other are aligned with the definition in TS 33.536.

1. The DDNMFs in the HPLMN and VPLMN of the Discoverer UE exchange Announce Auth. messages. If the Discoverer UE is not roaming, these steps do not take place.
2. The DDNMF in the HPLMN of the Discoverer UE returns the Discovery Response Filter and the Code-Receiving Security Parameters, the ProSe Query Code and the Code-Sending Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters.

Steps 12 to 15 occur over PC5.

1. The Discoverer UE sends the ProSe Query Code and also listens for a response message.
2. The Discoveree UE listens for a discovery message that satisfies its Discovery Filter.
3. The Discoveree sends the ProSe Response Code associated with the discovered ProSe Query Code.
4. The Discoverer UE listens for a discovery message that satisfies its Discovery Filter.

Steps 16-19 refer to a Discoverer UE that has encountered a match.

1. The Discoverer UE sends a Match Report message to the DDNMF in the HPLMN of the Discoverer UE.
2. The DDNMF in the HPLMN of the Discoverer UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Discoverer UE is authorised to discover the Discoveree UE.
3. The DDNMF in the HPLMN of the Discoverer UE returns to the Discoverer UE an acknowledgement that the integrity check passed.
4. The DDNMF in the HPLMN of the Discoverer UE may send a Match Report Info message to the DDNMF in the HPLMN of the Discoveree UE.



Figure 6.4.2.2-1: Model B restricted discovery security procedure

### 6.4.3 Evaluation

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*