**3GPP TSG-SA3 Meeting #102bis-e *draft\_S3-210892-r1***

**e-meeting, 1 – 5 March 2021** Revision of S3-21xxxx

**Source: Huawei, HiSilicon**

**Title: Address Editor’s Notes in Solution #27**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***Approve this contribution to solve ENs in Sol#27 of TR 33.847***

# 2 References

N/A.

# 3 Rationale

This contribution proposes to address the following ENs:

Editor’s Note: How this solution work with out-of-coverage UEs is FFS.

This one is addressed by adding NOTEs in both 6.27.2.1 and 6.27.2.2 to clarify the specific steps within coverage or out of coverage, respectively.

Editor’s Note: How this solution work with DCR broadcast discovery mechanism is FFS.

This EN is addressed by adding a NOTE to restrict the scenario: only work with the standalone discovery over PC5 for commercial services and public safety (both Model A and B are supported), not work with the V2X based direct discovery.

# 4 Detailed proposal

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

## 6.27 Solution #27: Mitigating the conflict between security policies using match report procedures.

### 6.27.1 Introduction

This solution addresses Key Issue #1 and Key Issue #12, including how to get the security materials to protect discovery and avoids one-to-one communication failure in advance. Two UEs should finish the discovery procedure 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 one-to-one communication policies. The security policies for ProSe UEs may be provisioned by different PCFs and they might issue different values. The referenced technology, eV2X unicast in 33.536 [8], still has mechanism to abort the PC5 unicast establishment upon policy mismatch (e.g. NOT NEED and REQUIRED) if the peer UE replies to the announciation of the same v2x service from the initiating UE. This shows the security policies on each UE may not the same for the same service/ProSe Code. Moreover, UEs still need to negotiate final security activation status according to the real-time conditions and the network has no such real-time information. For the above reasons, the conflict between security policies may cause one-to-one communication establishment failure and make the previous discovery request procedures in vain. To avoid resource waste caused by the conflict between policies, this contribution proposes to check the policy match in advance with the help of the match report procedures specified in TS 33.303 [6] for 5G ProSe open discovery and restricted discovery.

NOTE: This solution does not work with the V2X based direct discovery (e.g. clause 6.2 in TR 23.752 [2]).

### 6.27.2 Solution details

Editor’s Note: How security policy is configured at A-DDNMF and M-DDNMF for a ProSe Service is FFS.

NOTE: This solution requires network coverage to work.

#### 6.27.2.1 Open discovery scenario

Mitigating security conflict between policies using open discovery match report procedures is described as follows:



Figure 6.27.2.1-1: Check the conflict between policies using open discovery match report

1. The Announcing UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN (A-DDNMF) to get the permission to announce on its serving PLMN. The A-DDNMF returns the ProSe App Code, Discovery Key and other discovery parameters in Discovery Response message. This step reuses the procedures as specified in TS 33.303 [6].
2. The Announcing UE starts announcing with a Message Integrity Check (MIC) calculated by using the Discovery Key as described in TS 33.303 [6].
3. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the DDNMF in its HPLMN (M-DDNMF) to get the parameters for monitoring. The DDNMF returns the Discovery Filter containing the ProSe App Code(s) and/or the ProSe App Mask(s) with other discovery parameters in Discovery Response message. The M-DDNMF and A-DDNMF exchanges Monitor Req/Resp messages if the ProSe Application ID indicates a different PLMN. This step reuses the procedures as specified in TS 33.303 [6].
4. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter. On hearing the 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 M-DDNMF. The Match Report includes the ProSe App Code and MIC.
5. The M-DDNMF gets the Monitoring UE’s ProSe one-to-one communication security policies of the service related to the ProSe App Code from PCF and passes the policies to the A-DDNMF in the Match Report message. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
6. The A-DDNMF shall check the MIC is valid. The A-DDNMF 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 policies of the Monitoring UE and the policies of the Announcing UE are not conflict. If the MIC check passes and the security policies are not conflict to each other, the A-DDNMF shall acknowledge a successful check of the MIC to the M-DDNMF in the Match Report Ack message, otherwise it shall acknowledge check failure.
7. The M-DDNMF acknowledges the Monitoring UE to continue the subsequent procedures if passing the checks in step 6. Otherwise the M-DDNMF indicates the Monitoring UE to stop the procedure.

#### 6.27.2.2 Restricted discovery scenario

Mitigating security conflict between policies using restricted discovery match report procedures is described as follows:



Figure 6.27.2.2-1: Check the conflict between policies using open discovery match report

1. The Announcing/Discoveree UE sends a Discovery Request message to the DDNMF in its HPLMN (A-DDNMF) to get the ProSe Code, the discovery parameters and the associated security material for announcing. The DDNMF may check for the announce authorization with the ProSe Application Server. The A-DDNMF returns the ProSe Code, the discovery parameters and the associated security materials to the Announcing/Discoveree UE.
2. The Monitoring/Discoverer UE sends a Discovery Request message to the DDNMF in its HPLMN (M-DDNMF) to get the ProSe Code, the discovery parameters and security materials for monitoring. The M-DDNMF sends an authorisation request to the ProSe Application Server and gets an authorisation response. If the Discovery Request is authorised, the M-DDNMF sends a Monitor Request to the A-DDNMF to get the discovery parameters and the associated security materials if they are not in the same PLMN. The M-DDNMF returns the discovery parameters and the associated security materials to the Monitoring/Discoverer UE.
3. The Monitoring/Discoverer UE and the Announcing/Doscoveree UE continue the discovery procedure over PC5 including the MIC, i.e. Model A or Model B discovery. The Monitoring/Discoverer UE sends a Match Report to M-DDNMF including the MIC and ProSe Code if required.
4. The M-DDNMF checks the MIC is valid. The M-DDNMF gets the Monitoring/Discoverer UE’s ProSe one-to-one communication security policies of the service related to the ProSe Code from PCF and passes the policies to the A-DDNMF. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
5. The A-DDNMF gets the security policies of the Announcing UE for direct one-to-one communication service related to the ProSe Code from PCF, and checks if the security policies of the Monitoring/Discoverer UE and the policies of the Announcing/Discoveree UE are not conflict to each other. The A-DDNMF returns the check result to the M-DDNMF.
6. The M-DDNMF shall only indicate the acknowledge Monitoring/Discoverer UE to continue subsequent procedures if both MIC and the policies are not conflict to each other.

### 6.27.3 Evaluation

TBD

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