**3GPP TSG-SA3 Meeting #101-e *draft\_S3-210249-r2***

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

**Source: Huawei, HiSilicon**

**Title: Propose to mitigate the conflict between policies using restricted discovery**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to provide new solution to address KI#1 and #12 in TR 33.847***

# 2 References

N/A.

# 3 Rationale

This solution addresses Key Issue #1 and Key Issue #12. 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 confliction 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 conflict between policies in advance with the help of the discovery request procedures.

# 4 Detailed proposal

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

## 6.x Solution #x: Mitigating the conflict between security policies using restricted discovery procedures on network side.

### 6.x.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 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 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. 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 conflict between policies in advance with the help of the discovery request procedures specified in TS 33.303 [6] for 5G ProSe restricted discovery.

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

### 6.x.2 Solution details

The security procedure for restricted discovery is described as follows:

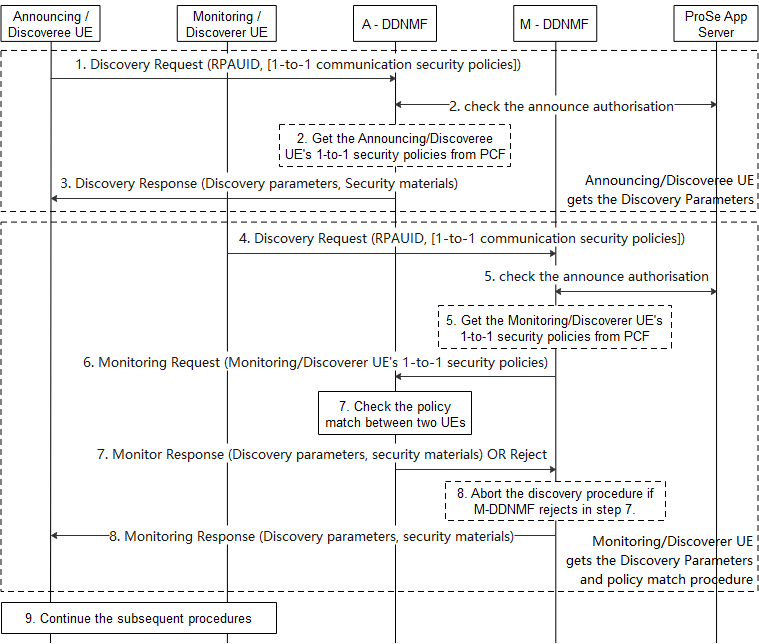


Figure 6.x.2.1-1: Check the conflict between policies using restricted discovery procedure

The Step 1-3 show the discovery request procedures of Announcing/Discoveree UE:

1. The Announcing/Discoveree UE sends a Discovery Request message including its PRAUID to the DDNMF in its HPLMN (A-DDNMF) to get the discovery parameters and the associated security material for announcing. The Announcing/Doscoveree UE may include its ProSe one-to-one communication security policies of the service related to the RPAUID. The one-to-one communication security policies are used to establish security during one-to-one communication establishment.
2. The DDNMF may check for the announce authorization with the ProSe Application Server. The A-DDNMF further exchanges the announce authorisation with the DDNMF of VPLMN if the Announcing/Doscoveree UE is roaming. The A-DDNMF get the Announcing/Doscoveree UE’s ProSe one-to-one communication security policies of the service related to the RPAUID from PCF if not received in step 1.
3. The A-DDNMF returns the discovery parameters and the associated security materials.

The Step 4-8 shows the discovery request procedures of Monitoring/Discoverer UE:

1. The Monitoring/Discoverer UE sends a Discovery Request message including its RPAUID to the DDNMF in its HPLMN (M-DDNMF) to get the discovery parameters and security materials for monitoring. The Monitoring/Discoverer UE may include its ProSe one-to-one communication security policies of the service related to its RPAUID.
2. The M-DDNMF sends an authorisation request to the ProSe Application Server and gets an authorisation response if the RPAUID is allowed to discovery at least one of the Target RPAUID(s). The authorisation response includes the above Target RPAUID(s). The M-DDNMF get the Monitoring/Doscoverer UE’s ProSe one-to-one communication security policies of the service related to the RPAUID from PCF if not received in step 4.
3. If the Discovery Request is authorised, and the PLMN ID in the Target RPAUID indicates a different PLMN, the M-DDNMF sends a Monitor Request to the indicated PLMN’s DDNMF i.e. the A-DDNMF. The Monitor Request includes the security policies got from either step 4 or 5. The A-DDNMF may exchange authorisation messages with the ProSe Application Server.
4. The A-DDNMF shall first check if the security policies provided by the DDNMF of the Monitoring/Discoverer UE and the security policies of the Announcing/Doscoveree UE are not conflict, the A-DDNMF responds to the M-DDNMF with a Monitor Response message including the discovery parameters and the associated security materials if the Monitoring/Discoverer UE’s security policies and the Announcing/Doscoveree UE’s security policies are not conflict to each other. The A-DDNMF shall reject the monitor request if the security policies between the Announcing/Doscoveree UE conflict the security policies of the Monitoring/Discoverer UE. If the Discovery Request is authorised, and the PLMN ID in the Target RPAUID indicates the same PLMN, then the M-DDNMF does the confliction check locally.

For Model B scenario, the DDNMFs in the HPLMN and VPLMN of the Discoverer UE exchange Announce Authorisation messages if the Discoverer UE is roaming.

1. The M-DDNMF returns the discovery parameters and the associated security materials to the Monitoring/Discoverer UE. If the A-DDNMF rejects the Monitor Request, the M-DDNMF shall abort the discovery procedure and inform the Monitoring/Discoverer UE.
2. The Monitoring/Discoverer UE and the Announcing/Discoveree UE continue the subsequent procedures if M-DDNMF informs to continue the discovery procedures, i.e. Model A or Model B discovery, the match report procedures (if applicable) and establishment of ProSe one-to-one communication.

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

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

### 6.x.3 Evaluation

TBD

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