**3GPP TSG-SA3 Meeting #109e-AdHoc *draft\_S3-230298-r1***

**e-meeting, 16 - 20 January 2023**

**Source: Qualcomm Incorporated**

**Title: Updates to the solution #25**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This contribution proposes to update the solution #25 in TR 33.740.***

# 2 References

[1] TR 33.740 v0.4.1

# 3 Rationale

This contribution proposes to update the solution #25.

First, it is proposed to remove the last sentence of step 0 as the details of discovery security materials is out of scope of this solution as already described in NOTE 2.

Second, we removed the following Editor’s Note:

Editor’s Note: the needs of E2E security in L3 solution is FFS.

This solution describes that an end-to-end security is established only when it is configured by the ProSe service. This means that the need for end-to-end security between the source UE and target UE is determined by the ProSe service and configured by 5G PKMF as described in the step 0. Therefore, the Editor’s Note is removed.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [1].

**\*\*\*\*\* START OF CHANGES \*\*\*\*\***

## 6.25 Solution #25: PC5 link setup for Layer-3 UE-to-UE Relay

### 6.25.1 Introduction

This solution addresses the KI #2. This solution provides a mechanism to setup a connection between source and target UEs via the UE-to-UE (U2U) Relay. This solution is a Layer-3 (L3) U2U Relay solution when the U2U Relay is in coverage and is based on the L3 user-plane UE-to-Network Relay architecture specified in TS 33.503 [6]. This solution only describes the PC5 link setup procedure between the source/target UE and the U2U Relay and end-to-end security setup between source and target UEs. The end-to-end security is an optional feature and is only established when configured by the service (i.e., 5G ProSe Key Management Function).

### 6.25.2 Solution details



Figure 6.25.2-1:. Secure PC5 link establishment procedure for UE-to-UE Relay

NOTE 1: In this solution, the source and target UEs, and U2U Relay are assumed to be provisioned with the discovery security materials when they are in coverage. Also, those security materials are associated with an expiration time, after which they become invalid. When the security materials become invalid the source/target UE needs to be in coverage to obtain fresh ones to be able to connect via U2U Relay.

Note 2: The details of discovery security materials are addressed in other solutions addressing KI#1 in the present document.

0. The source UE, target UE and the U2U Relay get the discovery parameters and 5G Prose Key management function (PKMF) address from the 5G DDNMF and the discovery security materials from the 5G PKMF respectively. Furthermore, the source and target UEs are provisioned with the security materials for end-to-end security setup by the PKMF if the U2U Relay service requires end-to-end security.

1a. The source UE performs the discovery procedure.

NOTE 3: The discovery procedure is based on the solution of Key Issue #1.

1b. The source UE performs a PC5 unicast link setup procedure with the U2U Relay. The PC5 unicast link setup procedure is based on the procedure specified in clause 6.3.3.2.2 of TS 33.503 [6].

2. The target UE performs the discovery procedure and PC5 unicast link setup procedure with the U2U Relay in the same manner as source UE.

3. The source UE and target UE establish an end-to-end IPsec connection via U2U Relay if security materials for end-to-end security are provisioned by the 5G PKMF. To establish an end-to-end IPsec connection, the source UE and target UE may perform IKEv2 authentication using the keying materials provisioned in step 0.

NOTE 4: Whether the end-to-end IPsec is needed is configured at the source UE and target UE by the 5G PKMF.

Editor’s Note: the needs of E2E security in L3 solution is FFS.

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