**3GPP TSG-SA3 Meeting #102-e S3-210485-r1**

**e-meeting, 18th - 29th January 2021 Revision of S3-20xxxx**

**Source: Qualcomm Incorporated**

**Title: Solution 20 EN resolution**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve ENs in solution #20***

# 2 References

[1]

# 3 Rationale

The contribution resolves the following ENs in solution 20.

- Editor’s Note: Out of coverage is FFS.

It is clarified that the remote UEs and relay UE are assumed to be provisioned with the discovery security materials and Remote User Key when they are in coverage. Also, those security materials are associated with an expiration time, after which they become invalid. With such clarification, the EN is deleted.

- Editor’s Note: whether IPsec will be always used needs to be clarified.

The following NOTE is added to clarify that the need for the IPsec based end-to-end security is configured by the PKMF.

NOTE: whether the end-to-end IPsec is needed is configured at the remote UEs by the PKMF.

# 4 Detailed proposal

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

## 6.20 Solution #20: PC5 link setup for UE-to-UE relay

### 6.20.1 Introduction

This solution addresses the KI #6. This solution provides a mechanism to setup a connection between remote UEs via the UE-to-UE relay. This solution is a L3 relay solution and assumes 5G Direct Discovery Name Management Function (DDNMF) and Prose Key Management Function (PKMF) as in LTE Prose. This solution only describes the PC5 link setup procedure between the remote UE and the UE-to-UE relay and end-to-end security setup between remote UEs.

### 6.20.2 Solution details



Figure 6.20.2-1:. Secure PC5 link establishment procedure for UE-to-network relay

NOTE: In this solution, the remote UEs and relay UE 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 Remote UE needs to be in coverage to obtain fresh ones to be able to connect via relay.

Editor’s Note: the detail of discovery security materials is FFS.

NOTE: This solution assumes a peer UE discovery mechanism (e.g., DNS based).

0. The Remote UEs and the UE-to-UE (U2U) relay get the discovery parameters and Prose Key management function (PKMF) address from the 5G DDNMF and the discovery security material from the PKMF respectively. Furthermore, the Remote UEs can be provisioned with the security materials for end-to-end security setup by the PKMF. For example, the security materials for end-to-end security setup include the Prose Service Code (PSC) and associated key. The service code may be used as a key ID when IKEv2 PSK based authentication is used.

1. Remote UE 1 performs the discovery procedure and PC5 unicast link setup procedure with the UE-to-UE relay.

a. The Remote UE performs discovery of a U2U relay.

b. The Remote UE sends a Direct Communication Request that includes Relay Service Code (RSC) and Nonce1.

c. Authentication and key agreement may be performed between the remote UE and U2U relay. As a result of successful authentication, KNRP is derived.

d. The U2U relay generates Nonce2 and derives KNRP-SESS using KNRP, Nonce1 and Nonce2. The U2U relay sends a Direct Security Mode Command that contains Nonce 2 to the Remote UE. The Direct Security Mode Command is integrity protected based on KNRP-SESS.

e. The Remote UE derives KNRP-SESS using KNRP, Nonce1 and Nonce2 and checks the integrity of the Direct Security Mode Command. If the verification is successful, the Remote UE sends a Direct Security Mode Complete to the U2U relay. From this point, all PC5 unicast traffic between the Remote UE and the U2U relay can be protected based on the KNRP-SESS.

Editor’s Note: How to support flexibility between remote UE1 and relay UE, and between Relay and Remote UE 2 are FFS.

Editor’s Note: The location of PKMF and how the remote UEs and relay UE use the PKMF is FFS.

2. Remote UE 2 performs the discovery procedure and PC5 unicast link setup procedure with the UE-to-UE relay in the same manner as Remote UE 1.

3. Remote UE 1 and Remote UE 2 can establish an end-to-end IPsec connection via U2U relay. To establish an end-to-end IPsec connection, Remote UE1 and Remote UE2 may perform IKEv2 authentication using the keying materials provisioned in step 0.

NOTE: Whether the end-to-end IPsec is needed is configured at the remote UEs by the PKMF.

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