**3GPP TSG-SA3 Meeting #102bis-e draft\_S3-211066-r3**

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

**Source: Qualcomm Incorporated**

**Title: EN resolution and evaluation for solution #20**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***Approve this contribution to resolve ENs and add evaluation of solutions #18 in TR 33.847***

# 2 References

[1] TR 33.847 v0.4.0

# 3 Rationale

This contribution proposes to resolve the following EN for solution #20.

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

To resolve the EN, the following NOTE is added.

NOTE x: For commercial services, the PKMF is located in the operator’s network. For Public Safety use cases, the PKMF can be managed by the Public Safety service provider.

Also, the contribution adds an evaluation of the solution.

# 4 Detailed proposal

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

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

### 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.

NOTE x: For commercial services, the PKMF is located in the operator’s network. For Public Safety use cases, the PKMF can be managed by the Public Safety service provider.

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.

### 6.20.3 Evaluation

This solution provides end-to-end confidentialty and integrity protection of commincation between the peer UEs over the UE-to-UE Relay at the IP layer.

This solution provides confidentiality and integrity protection of user-plane data and control-plane signaling between the remote UE and the UE-to-UE relay based on PC5 unicast security.

Editor’s Note: Further evaluation is FFS.

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