**3GPP TSG-SA3 Meeting #116 *S3-242153***

Jeju, Korea, 20th – 24th May 2024

**Source: Qualcomm Incorporated**

**Title: A new solution for multihop U2N relay discovery security**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***This contribution proposes a new solution to address the key issue #1.***

# 2 References

[1] Draft TR 33.743 v0.1.0

# 3 Rationale

This contribution proposes a new solution for multi-hop UE-to-Network Relay discovery security.

# 4 Detailed proposal

It is proposed that SA3 approved the below changes for inclusion in the draft TR [1].

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

## 6.Y Solution #Y: Multi-hop UE-to-Network Relay discovery security

### 6.Y.1 Introduction

This solution addresses the first, second and fourth security requirements in the key issue #1 regarding the multi-hop UE-to-Network (U2N) Relay discovery. This solution proposes to reuse the security procedure for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.3 of TS 33.503 [5]. In addition, it is proposed to mandate the integrity protection of discovery messages as the messages contain information related to path selection (e.g., hop count indicating the number of hops to reach the 5G ProSe UE-to-Network Relay). The proposed security procedure is based on the multi-hop UE-to-Network Relay discovery procedures in several solutions (e.g., solution #1, #2, and #7) of TR 23.700-03 [1].

### 6.Y.2 Solution details

#### 6.Y.2.1 Discovery with Model A

The security procedure for multi-hop UE-to-Network Relay discovery with Model A is shown in Figure 6.Y.2.1-1.



Figure 6.Y.2.1-1: Model A Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3 of TS 33.503 [5]. The discovery security materials contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Announcement.

Editor’s Note: Which HPLMN provision the discovery security materials associated with RSC to the Remote UE, Intermediate Relay and UE-to-Network Relay is FFS.

1. The 5G ProSe UE-to-Network Relay protects a Relay Discovery Announcement using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the 5G ProSe UE-to-Network Relay broadcasts the Relay Discovery Announcement.

2. The Intermediate UE-to-Network Relay processes the received Relay Discovery Announcement message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count, Relay Info.) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay broadcasts the message.

Editor’s Note: How the solution protects the path information during the discovery of multi-hop U2N relay is FFS.

3. Upon receiving the Relay Discovery Announcement message from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

#### 6.Y.2.2 Discovery with Model B

The security procedure for multi-hop UE-to-Network Relay discovery with Model B is shown in Figure 6.Y.2.2-1.



Figure 6.Y.2.2-1: Model B Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3 of TS 33.503 [5]. The discovery security materials contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Solicitation and Relay Discovery Response.

1. The 5G ProSe Remote UE protects a Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the 5G ProSe Remote UE broadcasts the Relay Discovery Solicitation.

2. The Intermediate UE-to-Network Relay processes the received Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay broadcasts the message.

3. Upon receiving the Relay Discovery Solicitation from the Intermediate UE-to-Network Relay, the 5G ProSe UE-to-Network Relay processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the 5G ProSe UE-to-Network Relay constructs a Relay Discovery Response and protects it using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

The 5G ProSe UE-to-Network Relay replies to the Intermediate UE-to-Network Relay with the Relay Discovery Response.

4. Upon receiving the Relay Discovery Response from the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. If the processing is successful, the Intermediate UE-to-Network Relay updates the path information (e.g., hop count) and protects the updated message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5]. Then, the Intermediate UE-to-Network Relay replies to the 5G ProSe Remote UE with the message.

5. Upon receiving the Relay Discovery Response from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE processes the received message using the discovery security materials associated with the RSC as specified in clause 6.3 of TS 33.503 [5].

### 6.Y.3 Evaluation

TBD

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