**3GPP TSG-SA3 Meeting #119 *draft\_S3-245263-r3***

**Orlando, US, 11th - 15th November 2024**

**Source: Qualcomm Incorporated, Huawei, HiSilicon, Interdigital, Ericsson, Beijing Xiaomi Mobile Software, and CATT**

**Title: Conclusion of multi-hop U2N relay discovery security in KI#1**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***This contribution proposes a conclusion of multi-hop U2N relay discovery security in KI #1.***

# 2 References

[1] TR 33.743

# 3 Rationale

This contribution proposes to add a conclusion of multi-hop U2N relay discovery security in Key Issue #1.

Particularly, it is proposed to reuse the existing security procedure for 5G ProSe UE-to-Network Relay discovery.

# 4 Detailed proposal

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

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

## 7.x Key issue #1: Security for multi-hop UE-to-Network Relay

The following statements are agreed as a basis for normative work:

For 5G ProSe Multi-hop UE-to-Network Relay discovery:

* 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 from the 5G PKMF/5G DDNMF of 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay’s HPLMN respectively, based on the procedure specified in clause 6.1.3.2 of TS 33.503 [5].
* The discovery security materials contain a Discovery User Integrity Key (DUIK) for the integrity protection of discovery messages.
* The Intermediate UE-to-Network Relay processes the received discovery message using the provisioned discovery security materials associated with the RSC as specified in clause 6.1.3.2 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 same security materials associated with the RSC as specified in clause 6.1.3.2 of TS 33.503 [5].

NOTE 1: Since the Intermediate UE-to-Network Relay and 5G ProSe UE-to-Network Relay are provisioned with a single set of discovery security materials from the 5G PKMF/5G DDNMF in their own HPLMN, it is assumed Intermediate UE-to-Network Relays and 5G ProSe UE-to-Network Relay belong to the same HPLMN during 5G ProSe multi-hop UE-to-Network Relay discovery.

* Both discovery with Model A and discovery with Model B are supported.
* For discovery with Model A, the Intermediate UE-to-Network Relay may (as specified in step 6 in clause 6.3.2.5.2 of TS 23.304 [4]) protect and send the Announcement message after a secure PC5 link establishment with the upstream Intermediate UE-to-Network Relay or the 5G ProSe UE-to-Network Relay.

Editor’s Note: How the PC5 link establishment is performed based on the optional procedure (step 6 in clause 6.3.2.5.2 of TS 23.304 [4]) is FFS.

* For discovery with Model B, the 5G ProSe Remote UE protects the discovery message (i.e., Relay Discovery Solicitation) reusing the procedures as specified in clause 6.1.3.2.3 of TS 33.503[5], i.e., using the discovery security materials associated with the RSC and HPLMN ID of the potential 5G ProSe UE-to-Network Relay.

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