**3GPP TSG-SA3 Meeting #104e-Ad-hoc draft\_S3-213525-r1**

**e-meeting, 27 - 30 September 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated**

**Title: User-plane UE-to-network relay connection procedure**

**Document for: Approval**

**Agenda Item: 4.8**

# 1 Decision/action requested

***This contribution proposes a text on User-plane U2N relay for ProSe TS***

# 2 References

[1] TR 33.847 v.0.7.0 “Study on security aspects of enhancement for proximity based services in the 5G System (5GS)”

# 3 Rationale

This contribution proposes to add a content for User-plane UE-to-network relay based on the conclusion in TR 33.847 [1].

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the ProSe TS.

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

## X.Y UE-to-Network Relay Security

### X.Y.1 General

This clause describes a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. The mechanism includes how a Remote UE and UE-to-network relay get authorized by the ProSe Key Management Function (PKMF) and verify each other’s role.

Editor’s Note: Co-existence with CP based solution is FFS

### X.Y.2 Remote UE attaching to a ProSe UE-to-network relay



Figure X.Y.2-1: Authorization and secure PC5 link establishment procedure for UE-to-network relay

The remote UE is provisioned with the discovery security materials and Prose Remote User Key (PRUK) when it is in coverage. These security materials are associated with an expiration time, after which they become invalid. If the UE does not have valid discovery security materials, the Remote UE needs to connect to the PKMF and obtain fresh ones to use the UE-to-Network relay services.

NOTE: The procedure is described for a scenario that the PKMF of the remote UE is different from the PKMF of the UE-to-network relay. If both the remote UE and the UE-to-network relay are served by a single PKMF, the PKMF takes the role of the PKMF of the remote UE and the PKMF of the UE-to-network relay and the inter-PKMF message exchanges are not needed.

NOTE: Steps 0a, 0b, 1a, 1b are performed when the remote UE is in coverage.

0a. The Remote UE gets the ProSe Key management function (PKMF) address from the 5G DDNMF.

Editor’s Note: How the PKMF address is obtained by the Remote/Relay is to be aligned with SA2.

0b. The Remote UE is authorized to receive UE-to-network relay service and gets the discovery security material from the PKMF. The PKMF of the remote UE may request the discovery security materials to the PKMFs of the potential relay UEs from which the remote UE gets the relay services.

Editor’s Note: How the PKMF of the remote UE obtains the list of the PKMFs of the potential relay UEs and their addresses requires explanation.

0c. The UE-to-network relay gets the ProSe Key management function (PKMF) address from the 5G DDNMF.

0d. The UE-to-network relay is authorized to act as a relay and gets the discovery security material from the PKMF.

 The remote UE and relay UE shall communicate with the PKMF via PC3 reference point. Security for PC3 interface relies on Ua security if GBA [zz] is used.

1a. The Remote UE sends a PRUK Request message to its PKMF. The message indicates that the Remote UE is requesting a PRUK from the PKMF. If the Remote UE already has a PRUK from this PKMF, the message shall also contain the PRUK ID of the PRUK.

1b. The PKMF checks that the Remote UE is authorised to receive UE-to-network Relay service. This is done by using the Remote UE’s identity associated with the key used to establish the secure connection between the Remote UE and PKMF in step 0b. If the Remote UE is authorised to receive the service, the PKMF sends a PRUK and PRUK ID to the Remote UE. If a PRUK and PRUK ID are included, the Remote UE shall store these and delete any previously stored ones for this PKMF.

2. The discovery procedure is performed between the Remote UE and the UE-to-network Relay using the discovery parameters and discovery security material as described in X.Y.Z.

3. The Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID, Relay Service Code (RSC) of the UE-to-network relay service and KNRP freshness parameter 1 to the UE-to-network relay.

Editor’s Note: privacy of PRUK ID is FFS.

4a. The UE-to-network relay sends a Key Request message that contains PRUK ID, RSC and KNRP freshness parameter 1 to its PKMF.

4b. On receiving the Key Request message, the PKMF of the UE-to-network relay checks that the UE-to-network relay is authorized to act as a relay to the Remote UE. This is done by using the relay’s identity associated with the key used to establish the secure connection between the relay and PKMF. If the UE-to-network relay is authorized to provide the relay service, the PKMF of the UE-to-network relay sends the Key Request to the PKMF of the remote UE.

Editor’s Note: How the PKMF of the relay UE identifies the PKMF of the remote UE requires explanation. 4c The PKMF of the remote UE generates KNRP freshness parameter 2 and derives KNRP using PRUK identified by PRUK ID, KNRP freshness parameter 1 and KNRP freshness parameter 2. Then, the PKMF for the remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the PKMF of the UE-to-network relay.

4d The PKMF of the UE-to-network relay sends the Key Response message to the UE-to-network relay.5a. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE (see TS 33.536 [ww]). This message contains the KNRP Freshness Parameter 2 and protected based on the session key (KNRP-SESS) derived from KNRP. The Direct Security Mode Command message is integrity protected using the integrity protection key (KNRPIK) derived from the session key (KNRP-SESS).

5b. The Remote UE derives KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It then derives the session key (KNRP-SESS) in the same manner as the UE-to-network relay and processes the Direct Security Mode Command. The Remote UE further derives the integrity protection key (KNRPIK) and encryption key (KNRPEK) from the session key (KNRP-SESS). Then, the Remote UE checks the integrity of the Direct Security Mode Command message. If the integrity check is successful, the Remote UE is assured that the UE-to-network relay is authorized to provide the relay service.

5c. The Remote UE responds with a Direct Security Mode Complete message to the UE-to-network relay. The Direct Security Mode Complete message is ciphered and integrity protected.

5d. On receiving and processing the Direct Security Mode Complete message, the UE-to-network relay checks the integrity of the Direct Security Mode Complete message. If the integrity check is successful, the UE-to-network relay is assured that the Remote UE is authorized to get the relay service.

6. The remote UE and UE-to-network relay continues the rest of procedure for the relay service over the secure PC5 link.

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