**3GPP TSG-SA3 Meeting #103e *S3-211810-r1***

**e-meeting, 17 - 28 May 2021** Revision of S3-21xxxx

**Source: Qualcomm Incorporated**

**Title: Update of solution #18 to support privacy protection**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to update the existing solution in TR 33.847***

# 2 References

[1] TR 33.847 v0.5.0

# 3 Rationale

This contribution proposes to update to Solution #18 to support privacy protection during PC5 link setup for UE-to-Network relay service. In particular, a Remote UE’s PRUK ID and Relay Service Code (RSC) can be exploited for an attacker to perform linkability and trackability attack against targeted Remote UEs once these are exposed in plain during PC5 link setup. This solution proposes to mitigate these privacy risks by only sending scrambled RSC and PRUK ID based on the provisioned discovery security parameters during PC5 link setup procedure.

In addition, a NOTE is added to support privacy protection during path switch procedure.

Minor editorial changes are made.

# 4 Detailed proposal

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

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

## 6.18 Solution #18: Authorization and PC5 link setup for UE-to-Network relay

### 6.18.1 Introduction

This solution addresses the KI #3, KI #4, and KI #5. This solution provides a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. In addition, this solution describes how a Remote UE and UE-to-network relay get authorized by the ProSe Key Management Function and verify each other’s role. This solution also addresses privacy risks related to the use of a Remote UE’s identity (PRUK ID) and Relay Service Code (RSC) during the PC5 link setup. This solution assumes 5G Prose function and Prose Key Management Function as in LTE Prose. This solution only describes the PC5 link setup procedure that is common for both L2 and L3 UE-to-network relay.

### 6.18.2 Solution details



Figure 6.18.2-1: Authorization and secure PC5 link establishment procedure for UE-to-network relay

NOTE: In this solution, the remote UE needs to be provisioned with the discovery security materials and Remote User Key when it is 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 architecture of this solution needs to be aligned with SA2.

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

NOTE: The Remote UE may get multiple PKMF addresses for different PLMNs. If the Remote UE receives multiple PKMF addresses, it will contact each of PKMFs separately. The remote UE may contact those PKMFs directly or via the PKMF of its home PLMN.

0b. The Remote UE is authorized to receive UE-to-network relay service and gets the discovery security material from the PKMF

0c. The UE-to-network relay gets the discovery parameters and 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 communicate with the PKMF via PC8 reference point (like in LTE Prose [6]). Security for PC8 interface relies on Ua security if GBA [12] is used or Ua\* when AKMA [7] is used.

NOTE: 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.

1a. The Remote UE sends a Prose Remote User Key (PRUK) Request message to the PKMF of the UE-to-network relay.

1b. The ProSe Key Management Function checks that the Remote UE is authorised to receive UE-to-network Relay service. This is done by using the Remote UE’s identity that is bound to the keys that established 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.

2. The discovery procedure is performed between the Remote UE and the UE-to-network Relay using the discovery parameters and discovery security material.

Editor’s Note: The detail of discovery security material is FFS, and how it impacts on discovery procedure needs to be clarified

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. In DCR, the PRUK ID and RSC are scrambled using the code-receiving security parameters. The mechanism for scrambling protection is based on clause 6.1.3.4.3 of TS 33.303 [6].

Editor’s Note: The detailed protection mechanism and the security parameters to protect the PRUK ID and RSC are FFS

4a. On receiving the Direct Communication Request, the UE-to-network relay unscrambles the PRUK ID and RSC using the code-sending security parameters and checks if the RSC matches with the one that it sent in the discovery message. Then, the UE-to-network relay sends a Key Request message that contains PRUK ID, RSC and KNRP freshness parameter 1 to the PKMF.

4b. On receiving the Key Request message, the PKMF 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 that is bound to the keys that established the secure connection between the relay and PKMF in step 0d. If the UE-to-network relay is authorized to provide the relay service, the PKMF 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 sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the UE-to-network relay.

5a. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE (see 6.5.2.2). 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).

Editor’s Note: How to support flexibility between remote UE and relay UE is FFS.

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.

NOTE: The rest of procedure is determined depending on the UE-to-network relay types (i.e., L2 or L3 relay).

NOTE: The remote UE performs steps 2-6 during the path switch to another relay UE if the security materials obtained in steps 0-1 are still valid (i.e., have not expired).

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