**3GPP TSG-SA3 Meeting #102-e S3-210483-r1**

**e-meeting, 18th - 29th January 2021 Revision of S3-20xxxx**

**Source: Qualcomm Incorporated**

**Title: Solution 18 EN resolution**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve ENs in solution #18***

# 2 References

[1]

# 3 Rationale

The contribution resolves the following ENs in solution 18.

- Editor’s Note: Out of coverage is FFS.

It is clarified that the remote UE is provisioned with discovery security materials and Remote User Key when it is in coverage. The relay UE should be in coverage for the UE-to-Network relay service. With such clarification, the EN is deleted.

- Editor’s Note: Security of communication with PKMF is FFS.

It is clarified that the remote UE and relay UE communicate with the PKMF via PC8 reference point (like in LTE Prose [6]); and security for PC8 interface relies on Ua security if GBA [12] is used or Ua\* when AKMA [7] is used.

With such clarification, the EN is deleted.

Minor editorial (i.e., text format change) for the remaining ENs.

# 4 Detailed proposal

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

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

### 6.18.1 Introduction

This solution addresses the KI #3. This solution provides a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. 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: 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.

0a-d. The Remote UE and the UE-to-network (U2N) relay get the discovery parameters and Prose Key management function (PKMF) address from the 5G Prose function and the discovery security material from the PKMF respectively.

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.

Editor’s Note: When GBA is used, how to provide identity privacy is FFS.

Editor’s Note: How the remote UE is configured to access the PKMF of the relay UE is FFS.

Editor’s Note: The location of PKMF is FFS.

Editor’s Note: It is FFS when Remote UE and Relay are served by different 5G DDNMF

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. 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 that contain the PRUK ID, Relay Service Code (RSC) of the UE-to-network relay service and KNRP freshness parameter 1.

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

4b. 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. 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.

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. Then, the Remote UE responds with a Direct Security Mode Complete message to the UE-to-network relay.

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).

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