**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222800-r1***

**e-meeting, 10 - 14 October 2022**

**Source: Ericsson**

**Title: Resolve EN for same credentials used for both in-coverage and out-of-coverage mode in Solution 3**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This document proposes to resolve EN for PC5 link setup between U2U and Target UE in Solution3.***

# 2 References

[1] 3GPP TR 23.700-33

[2] 3GPP TR 33.740

# 3 Rationale

This contribution proposes to resolve the following EN in Solution #3: PC5 security establishment when L3 UE-to-UE relay is in coverage.

Editor’s Note: how to verify the service authorization information if relay UE uses the same security materials for both in-coverage and out-of-coverage mode.

The peer UEs support UP and/or CP based security procedure via the relay UE as specified in TS 33.503, in case the Relay UE is in-coverage case. It is expected such security method is not used when the Relay UE is out-of-coverage.

The peers UEs may also be provisioned with other credentials (e.g. as described in Solution #4) to support PC5 security procedure for case the Relay UE is out-of-coverage. It could be also possible that the peer UEs may utilize such security method even when the Relay UE is in-coverage.

It is our view that security procedure described in this solution should be preferred when the Relay UE is in-coverage. Nevertheless, the Relay UE can indicate in the discovery announcement whether both security methods are supported and preference of using them or only one method is used when the Relay UE is in-coverage.

It is proposed to clarify that the Relay UE can indicate more security methods are supported and their preference.

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 6.3 Solution #3: PC5 security establishment when L3 UE-to-UE relay is in coverage

### 6.3.1 Introduction

This solution addresses Key issue #2: Security of UE-to-UE Relay and Key issue #3: Authorization in the UE-to-UE Relay Scenario. This solution addresses a L3 UE-to-UE relay.

For L3 UE-to-UE relay use cases, the L3 UE-to-UE relay may be in or out of 3GPP coverage. This solution provides a mechanism for PC5 security setup procedure between a source UE or target UE and a L3 UE-to-UE relay when the L3 UE-to-UE relay is in 3GPP coverage.

This solution assumes 5GC NFs e.g., 5GDDNMF and PKMF are deployed in the network.

### 6.3.2 Solution details

Figure 6.3.2-1 illustrates the high-level procedure of the proposed solution.



Figure 6.3.2-1: High-level procedure of PC5 security between Source/Target UE and UE-to-UE relay

0. The 5G ProSe Source/Target UE and UE-to-UE relay are provisioned with the discovery security materials and/or PRUK when they are in coverage.

Editor’s Note: Further provisioned parameters e.g., PC5 security policies of UE-to-UE relay are FFS.

1. The discovery procedure for UE-to-UE Relay is performed by the 5G ProSe Source UE using the discovery parameters and discovery security material, based on the Relay Service Code for UE-to-UE Relay. If the UE-to-UE Relay is in 3GPP coverage, it also indicates whether network-based Relay service authentication and authorization is supported for UE-to-UE relay in the discovery announcement message.

NOTE: In case the Relay UE is capable to support more security methods (e.g., as described in Solution #4) when the Relay UE is in 3GPP coverage,it is preferrable to use the security method described in this solution.

2. If the discovered UE-to-UE Relay supports network-based Relay service authentication and authorization, the 5G ProSe Source UE sends a Direct Communication Request (DCR) that contains PRUK ID or SUCI, Relay Service Code (RSC) of the 5G ProSe UE-to-UE Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-UE Relay.

Editor’s Note: Its FFS whether the included parameters in Direct Communication Request message in step 2 can be protected by the discovery keys similar as to the Direct Communication Request message when establishing a secure PC5 link in between Remote UE and UE-to-network relay as described in TS 33.503 [6].

3. The 5G ProSe UE-to-UE Relay sends a Key Request message that contains PRUK ID or SUCI, RSC and KNRP freshness parameter 1 to the 5GC.

NOTE: 5GC NFs and internal signalling are not described in detail.here for brevity. The similar security procedure as Security for 5G ProSe Communication via 5G ProSe Layer-3 UE to-Network Relay as defined in TS33.503 [6] can be reused.

4. The 5GC sends the Key Response message to the 5G ProSe UE-to-UE Relay, which includes KNRP, KNRP freshness parameter 2.

Editor’s Note: Further input parameters in the Key Response message are FFS.

5a. The 5G ProSe UE-to-UE Relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.536 [9]. The 5G ProSe UE-to-UE Relay sends a Direct Security Mode Command message to the 5G ProSe Source UE and include KNRP Freshness Parameter 2 in the message.

5b. The 5G ProSe Source UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2 and then derive the session key (KNRP-SESS) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the 5G ProSe UE-to-UE Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the 5G ProSe Source UE that the 5G ProSe UE-to-UE Relay is authorized to provide the UE-to-UE relay service.

5c. The 5G ProSe Source UE responds with a Direct Security Mode Complete message to the 5G ProSe UE‑to-UE Relay.

5d. On receiving the Direct Security Mode Complete message, the 5G ProSe UE-to-UE Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-UE Relay that the 5G ProSe Source UE is authorized to get the UE-to-UE relay service.

6. The 5G ProSe Source UE and 5G ProSe UE-to-UE Relay continues the rest of procedure for the UE-to-UE relay service over the secure PC5 link.

Editor’s Note: Further and remaining messages needs to be updated and clarified in step 6.

7. Step 1-6 are repeated for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay.

Editor’s Note: Its FFS how target UE determines whether this PC5 link is used for direct communication with U2U relay or for U2U communication with Source UE.

Editor’s Note: PC5 security set up procedure between target UE and Relay UE (step7) can be performed in parallel to the PC5 security set up procedure between source UE and Relay UE (step 1-6).

8. The 5G ProSe Source UE and the 5G ProSe Target UE may establish an end-to-end Security via 5G ProSe UE-to-UE relay. The detail is not described in this solution.

Editor’s Note: The method for providing End to End IP security is FFS.

### 6.3.3 Evaluation

**\*\*\*\*** END OF CHANGE **\*\*\*\***