**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 -26 May 2023** (revision of S3-yyxxxx)

**Source: Ericsson**

**Title: Update to solution #3**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This paper proposes an update to solution #3.***

# 2 References

[1] 3GPP TR 23.700-33

[2] 3GPP TR 33.740

# 3 Rationale

There is an EN in solutions #3 requiring SA2 coordination regarding the new messages introduced in solutions #3, which have impacts on Direct Communication Request/Accept procedure defined in SA2.

Editor’s Note: The need for the new Direct Communication Invite message is FFS in coordination with SA2.

It is our view that the new messages introduced in the flow are for purpose of security establishment, thus it makes sense that such messages should be defined and under remit of SA3. To avoid impact on SA2 specifications, it is proposed to define new messages which are security specific, i.e., new messages Direct Communication Security Request and Direct Communication Security Accept are proposed. These new messages would then have no impacts on the existing Direct Communication Request/Accept procedure in SA2 specification. It means no need to send further LS to SA2.

This paper proposes to update the solution#3 and remove the EN.

# 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

#### 6.3.2.1 Procedure for PC5 security establishment between the 5G ProSe Source UE and 5G ProSe UE-to-UE Relay

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



Figure 6.3.2.1-1: 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, PC5 security policies and/or PRUK when they are in coverage.

NOTE 1: 5GC NF(s) that provision PC5 security policies are to be determined during normative work.

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.

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.

NOTE 2: 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. Protection of PRUK ID and RSC in DCR can be done same as described in TS33.503 [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 3: 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. The message may also contain GPI, EAP message exchange depending on the selected security methods (UP or CP) as defined in TS33.503 [6]

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. After successful verification, PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay is performed according to the procedure described in clause 6.3.2.2.

7. After receiving the Direct Communication Accept message from the 5G ProSe target UE, the 5G ProSe UE-to-UE Relay sends a Direct Communication Accept message to the 5G ProSe source UE.

#### 6.3.2.2 Procedure for PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay



Figure 6.3.2.2-1 PC5 security establishment between the 5G ProSe Target UE and 5G ProSe UE-to-UE Relay

1. If the target UE is not discovered by the 5G ProSe UE-to-UE Relay yet, the discovery procedure is performed.

2. The 5G ProSe UE-to-UE Relay sends a Direct Communication Request that contains Relay Service Code and an indicator for the second hop PC5 link security establishment to the 5G ProSe Target UE to trigger the second hop PC5 link security establishment procedure. It is assumed the PRUK of Target UE is used as root for the PC5 security.

3. The 5G ProSe target UE sends a Direct Communication Security Request that contains UP-PRUK ID or SUCI of the 5G ProSe target UE, Relay Service Code of the 5G ProSe UE-to-UE Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-UE Relay.

4-6. Step 4-6 are same as step 3-5 of clause 6.3.2.1, where the 5G ProSe Target UE acts the role of the 5G ProSe Source UE.

7. After successful Direct Security Mode Command procedure for the second hop PC5 link, the 5G ProSe UE-to-UE Relay sends a Direct Communication Security Accept to the 5G ProSe target UE.

8. The 5G ProSe target UE sends a Direct Communication Accept to the 5G ProSe UE-to-UE Relay.

### 6.3.3 Evaluation

This solution resolves Key issue #2: Security of UE-to-UE Relay and Key issue #3: Authorization in the UE-to-UE Relay Scenario when L3 UE-to-UE relay is within 3GPP coverage.

This solution is for commercial services and public safety and supports the PC5 communication with a UE-to-UE Relay capable with network-based Relay service authentication and authorization similar to the UE-to-network relay as described in clauses 6.3.3.2.2 and 6.3.3.3.2 in TS 33.503 for the PC5 security establishment when in 3GPP coverage.

This solution only works when the UE-to-UE relay is located within network’s coverage area. The 5G ProSe Source/Target and UE-to-UE relay need to store security materials dedicated to the In-Coverage scenario. Apart from the PC5 signalling, additional user plane/signalling interactions with the network are required in this mechanism.

In the case the UEs (Source/Target/Relay) support multiple security methods (i.e. for In-Coverage and Out-of-Coverage), the 5G ProSe Source/Target and UE-to-UE relay are required to have the logic to choose between the In-Coverage dedicated mechanism and the Out-of-Coverage dedicated mechanism before starting the direct communication establishment.

This solution supports per-hop links setup. The Source UE initiates the PC5 security link setup with UE-to-UE Relay (first hop) similar to the UE-to-network relay as defined in TS 33.503. And the UE-to-UE Relay initiates the PC5 security link setup with the target UE (second hop) after the Security Establishment procedure is completed at the first hop. In order to trigger the Target UE to initiate the second hop PC5 link security establishment procedure, the UE-to-UE Relay could send a Direct Communication Request message that contains Relay Service Code to the 5G ProSe Target UE and an indication to trigger the 5G ProSe target UE to set up PC5 link security establishment for the 2nd hop. The 5G ProSe target UE then sends a new Direct Communication Security Request to the 5G ProSe Target UE to trigger the second hop PC5 link security establishment procedure. The need for this new message can be decided during normative work.

Editor’s Note: Further evaluation is FFS.

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