**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231822\_r1***

**Electronic meeting, Online, 17 - 21 April 2023**

**Source: Philips International B.V.**

**Title: New solution: PC5 link establishment with secure integrated discovery**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***SA3 is kindly asked to approve the following solution addressing KI#1 and KI#2 in an Integrated Discovery scenario***

# 2 References

[1] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services"

# 3 Rationale

The proposed solution addresses KI#1 and KI#2 related to Security for UE-to-UE Relay discovery and Security of UE-to-UE Relay respectively.

The solution describes means to protect a Direct Communication Request with Integrated Discovery by Source-UE, and UE-to-UE relays that may use different keying materials or security mechanismus. The solution also describes the security establishment procedures that Target-UE performs based on the received DCR messages and path selection.

# 4 Detailed proposal

\*\*\* BEGIN CHANGES \*\*\*

6.X Solution #X: PC5 link establishment with secure integrated discovery

6.X.1 Introduction

This solution addresses KI#1 Security for UE-to-UE Relay discovery and KI#2 Security of UE-to-UE Relay.

The solution describes means to protect a Direct Communication Request message with Integrated Discovery, proposes a new field (i.e., “integrated\_discovery\_indication”), and describes the security establishment procedures that Target-UE could perform, to establish a secure link with a UE-to-UE relay and Source-UE, based on its evaluation of the DCR messages received and its path selection preferences.

6.X.2 Solution details



Figure 6.X.2-1 PC5 link establishment with secure integrated discovery

0. Source, Target, and UE-to-UE Relays are provisioned with security policies, discovery security materials and parameters to enable the establishment of secure PC5 links with a UE-to-UE relay and Source-UE.

NOTE1: The security parameters and the corresponding provisioning procedure will be decided in normative phase.

1. Source UE constructs the DCR message including a Direct Discovery set, a UE-to-UE Discovery set, and fields specific to the DCR message e.g., Security Information, relay indication, and an integrated\_discovery\_indication. Source-UE protects the Direct Discovery set and the integrated\_discovery\_indication using the Direct Code-sending security parameters, and the whole DCR message is protected with the UE-to-UE relay Code-sending security parameters, whereby the Direct Discovery set and integrated\_discovery\_indication are not confidentiality protected.

NOTE2: Whether E2E protection in integrated discovery is required to maintain consistency with UE-to-UE discovery procedures and/or 5G ProSe Direct communication is FFS in normative work.

NOTE3: The field integrated\_discovery\_indication indicates to Target-UE whether the discovery message is integrated into a DCR.

2.       When a UE-to-UE Relay receives the DCR message, it descrambles/decrypts, and integrity verifies it. If integrity verification succeeds, the UE-to-UE relay removes the relay indication, and constructs another DCR message (e.g., DCR1 or DCR2) as in step 1.

2.a If the relay e.g., UE-to-UE Relay1, identifies Target-UE and a secure link is already established with Target-UE, UE-to-UE Relay1 uses the security keys corresponding to the already established security context with Target-UE to protect DCR1.

Editor’s Note: How a UE-to-UE Relay identifies the Target-UE is FFS.

2.b If the relay, e.g., UE-to-UE Relay2, cannot identify Target-UE or does not have a security context established with it, UE-to-UE Relay2 uses the UE-2-UE Code-sending security parameters to protect DCR2.

NOTE 2: UE-to-UE Relay2 could protect DCR2 by re-using the same UE-2-UE Code-sending security parameters used to protect the DCR message.

3.a/b UE-to-UE Relay1 and UE-to-UE Relay2 transmit DCR1 and DCR2 to Target-UE.

4. As Target-UE may receive several DCR messages (e.g., from one or multiple UE-to-UE relays). When applicable, Target-UE unscrambles/decrypts, and verifies the integrity of the received DCR message with the corresponding keys (either corresponding to an existing security context or UE-2-UE Code-receiving security parameters). Then, the target-UE uses the Direct Code-receiving security parameters to decrypt, and integrity verify the Direct discovery set including integrated\_discovery\_indication.

Based on the received the DCR messages and Target-UE’s path selection preferences in step 4, a secure link is established with Source-UE in either one of the following ways:

Case 1: Target-UE selects a communication path going through UE-to-UE Relay1:

5.a Since a security context is already established, the Direct auth and Key Establishing, and Direct Security Mode Command procedures are skipped, instead, Target-UE sends a Direct Communication Accept to UE-to-UE Relay2.

6.a/7.a/8.a correspond to the establishment of a secure link between Source-UE and UE-to-UE Relay1.

 9.a Source-UE and Target-UE establish an end-to-end secure link through UE-to-UERelay1.

 Case 2: Target-UE selects a communication path going through UE-to-UE Relay2:

5.b/6.b/7.b correspond to the establishment of a secure link between UE-to-UE Relay2 and Target-UE.

8.b/9.b/10.b correspond to the establishment of a secure link between UE-to-UE Relay2 and Source-UE.

11.b. Source-UE and Target-UE establish an end-to-end secure link through UE-to-UERelay2.

NOTE4: E2E secure link establishment may be left to the application.

NOTE5: This solution is applicable to both L2 and L3 UE-to-UE relay scenarios.

NOTE6: Secure hop-by-hop or end-to-end links between UE-to-UE Relays and End-UEs, and between Ends UEs are established as described in clause 5.3 of TS 33.536 [1], based on Security Information in the DCR message.

6.X.3 Evaluation

TBD

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