**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231801-r3***

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

**Source: Qualcomm Incorporated**

**Title: Updates on the solution #24**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This contribution proposes to update the solution #24 in TR 33.740.***

# 2 References

[1] TS 23.304

[2] TR 33.740

# 3 Rationale

This contribution proposes to update the solution #24.

In particular, this contribution proposes to add a NOTE for clarification on security protection of the direct discovery set(s). In addition, it is proposed to remove the Editor’s Notes with the following reasons.

First, the need for the two sets of security parameters is explained in the companion contribution (S3-231798). Therefore, we remove the following Editor’s Notes.

Editor’s Note: The need of two sets of security parameters is FFS.

Editor’s Note: The need of two different discovery codes (ProSe code and RSC) is FFS.

Second, SA2 (according to TS 23.304 [1]) does not restrict RSC to be used for a single ProSe service. This means a single U2U Relay service (identified by RSC) can provide relay service to multiple ProSe services. If additional clarification on whether the same RSC can be shared by multiple Prose services, it should be clarified by SA2. Therefore, the following Editor’s Note is removed.

Editor’s Note: It's FFS whether ProSe services requiring different security materials share the same RSC.

Evaluation is also updated to clarify the required procedures.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [2].

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

## 6.24 Solution #24: Security mechanism for UE-to-UE Relay Model B discovery

### 6.24.1 Introduction

This solution addresses the Key Issue #1.

A (relayed) Solicitation message and (relayed) Response message by the U2U relay includes two sets of elements, i.e., direct discovery set(s) (e.g., the User Info ID of source UE and target UE) and a U2U discovery set (e.g., Type of Discovery Message, RSC, User Info ID of the relay). The 5G ProSe U2U Relay only modifies the elements of the U2U discovery set. The direct discovery set that is constructed by the source UE can only be interpreted by the target UE, and vice versa. The U2U Relay can use a single RSC (and the associated security materials) to relay direct discovery sets associated with the multiple ProSe services. This means that the 5G ProSe U2U Relay uses the same security materials to protect the discovery messages that contain the direct discovery sets associated with different ProSe service. Unless each direct discovery set is protected using the security materials of the corresponding ProSe service, a source UE (or a target UE) that is authorized to use the RSC for U2U discovery can decrypt (and manipulate) any direct discovery sets that are delivered using the same RSC. This poses security threats.

To prevent such security threats, this solution proposes a U2U discovery security mechanism that protects the discovery messages using two sets of security materials (i.e., the discovery messages and the direct discovery set(s) are protected using the respective set of security materials).

### 6.24.2 Solution details



Figure 6.24.2-1: Model B discovery

This solution consists of two protection mechanisms using two sets of security materials: one for the Solicitation and Response message protection and the other one for the direct discovery set(s) protection.

The security procedure is described as follows:

NOTE 1: the procedures for discovery security materials provisioning and protection mechanisms specified in clause 6.1.3.2 of TS 33.503 [6] are reused for the U2U Relay Model B discovery. The details of how the protection mechanisms in clause 6.1.3.2.3 of TS 33.503 [6] is applied to the U2U discovery message protection will be specified during the normative work.

NOTE 2: The direct discovery set contains all information (e.g., UTC-based time counter and MIC) needed to process (decrypt/integrity check) it.

Editor’s Note: How to retrieve the corresponding direct security material associated with Prose Code to verify the direct discovery set(s) is ffs.

0. The source UE, target UE, and U2U Relay are provisioned with the following discovery security materials based on the procedure specified in clause 6.1.3.2.2 of TS 33.503 [6].

0a. The source UE and target UE are provisioned with the discovery security materials associated with the ProSe code (i.e., query and response code) for a ProSe service.

0b. The source UE, target UE, and U2U Relay are provisioned with discovery security materials associated with an RSC.

1. The source UE protects a direct discovery set(s) (e.g., user info ID of target UE) using the discovery security materials associated with the ProSe code. Then, the source UE provides the protected direct discovery set(s) to the U2U Relay via a Solicitation message. The Solicitation message is protected as specified in clause 6.1.3.2.3 of TS 33.503 [6].

2. On receiving the Solicitation message from the source UE, the U2U Relay decrypts and/or verifies the received Solicitation message using the discovery security materials associated with the RSC. If the verification is successful, the U2U Relay constructs a (relayed) Solicitation message that contains U2U discovery set and the direct discovery set(s). Then, the U2U Relay protects the (relayed) Solicitation message using the same security materials and forwards (relays) the message to the target UE.

3. The target UE decrypts and/or verifies the received Solicitation message using the discovery security materials associated with the RSC.The target UE further extracts the protected direct discovery set(s) from the message and decrypts and/or verifies the direct discovery set(s) using the discovery security materials associated with the ProSe code.

4. The target UE protects direct discovery set(s) (e.g., user info ID of source UE) using the discovery security materials associated with the ProSe code and includes it in a Response message. Then, the target UE protects the Response message using the discovery security materials associated with the RSC and sends the message to the U2U Relay.

5. The U2U Relay decrypts and/or verifies the received Response message using the discovery security materials associated with the RSC. If the verification is successful, the U2U Relay constructs a (relayed) Response message that contains (modified) U2U discovery set and the direct discovery set(s) and protects the message using the same security materials. Then, the U2U Relay forwards (relays) the message to the source UE.

6. The source UE decrypts and/or verifies the received Response message using the discovery security materials associated with the RSC. If the verification is successful, the source UE further extracts the protected direct discovery set(s) from the message and decrypts and/or verifies the direct discovery set(s) using the discovery security materials associated with the ProSe code as specified in clause 6.1.3.2.3 of TS 33.503 [6].

### 6.24.3 Evaluation

This solution addresses the Key Issue #1.

This solution fulfils all security requirements of the Key Issue #1.

This solution requires to support provisioning of:

* Two sets of discovery security materials at source UE and target UE

This solution reuses the security material provisioning mechanism for Restricted 5G ProSe Direct Discovery as specified in TS 33.503 for the provisioning of discovery security materials for the direct discovery set.

This solution reuses the security material provisioning mechanism for 5G ProSe UE-to-Network Relay discovery as specified in TS 33.503 for the provisioning of discovery security materials for the U2U relay discovery message.

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