**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231800-r3***

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

**Source: Qualcomm Incorporated**

**Title: Updates on the solution #23**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This contribution proposes to update the solution #23 in TR 33.740.***

# 2 References

[1] TS 23.304

[2] TR 33.740

# 3 Rationale

This contribution proposes to update the solution #23.

In particular, this contribution proposes two updates: (1) clarification on security protection of the direct discovery set(s) and the announcement message, and (2) addition of direct discovery set protection indication.

The direct discovery set protection indication informs the UE of whether to enable/disable the direct discovery set(s) protection, thus, enables a source UE/target UE to determine whether to do/undo the protection of direct discovery set(s) during the U2U relay discovery procedure.

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 restricted code and RSC) is FFS.

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.

How the target UE protects the direct discovery set is clarified and this is aligned with the discovery procedure defined by SA2. So, the following Editor’s Note is removed.

Editor’s Note: how the target UE provides the protected direct discovery set(s) to the U2U Relay needs to be aligned with the U2U relay Model A discovery procedure defined by SA2.

In addition, evaluation is updated based on the solution updates in this contribution.

# 4 Detailed proposal

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

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

## 6.23 Solution #23: Security mechanism for UE-to-UE Relay Model A discovery

### 6.23.1 Introduction

This solution addresses the Key Issue #1.

An Announcement 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 is constructed by the target UE and is only interpreted by the source UE. 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 Announcement messages that contain the direct discovery sets associated with different ProSe services. 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 Announcement message using two sets of security materials (i.e., the Announcement message and the direct discovery set(s) are protected using the respective set of security materials).

### 6.23.2 Solution details



**Figure 6.23.2-1: Model A discovery**

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

1. Direct discovery set(s) protection by the target UE:

The target UE is provisioned with the ProSe restricted code, RSC, and the respective discovery security materials as specified in clause 6.1.3.2.2 of TS 33.503 [6].

The target UE protects the direct discovery set(s) using the discovery security materials associated with the ProSe restricted code as specified in clause 6.1.3.2.3 of TS 33.503 [6].

The target UE protects the direct discovery set(s) using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of TS 33.503 [6].

The target UE provides the protected direct discovery set(s) to the U2U Relay.

NOTE 1: the protection mechanisms specified in clause 6.1.3.2.3 of TS 33.503 [6] are reused for the direct discovery set and U2U discovery set protection. 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.

2. Announcement message protection by U2U Relay:

The U2U Relay and source UE are provisioned with the RSC for a U2U relay service and the discovery security materials associated with the RSC as specified in clause 6.1.3.2.2 of TS 33.503 [6].

The U2U Relay constructs an Announcement message that contains RSC, user info ID of itself, and the direct discovery set(s) received from the target UE, as specified in TS 23.304 [8].

NOTE 3: The direct discovery set, if its protection is enabled, is protected by the Target UE. The Relay UE includes them in the Announcement message without modification.

The U2U Relay protects an Announcement message using the provisioned discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of TS 33.503 [6].

3. Announcement message processing by Source UE:

The source UE that is provisioned with the ProSe restricted code, RSC, and the respective discovery security materials as in the target UE, processes the Announce message as follows.

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

### 6.23.3 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.

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