**3GPP TSG-SA3 Meeting #104-e ad-hoc *S3-213528-r1***

**e-meeting, 27 - 30 September 2021** Revision of S3-21xxxx

**Source: Qualcomm Incorporated**

**Title: A new solution for privacy enhancements during PC5 link setup for UE-to-Network relay**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution proposes a new solution for privacy enhancements during PC5 link setup for UE-to-Network relay.***

# 2 References

[1] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects"

[2] TR 33.847 v0.6.0

# 3 Rationale

This contribution proposes a new solution that provides a mechanism for protecting Relay Service Code (RSC) (and PRUK ID) during PC5 link setup for UE-to-Network (U2N) relay when RSC is protected in restricted discovery. In restricted discovery, RSC is protected (i.e., scrambled and/or ciphered) in both discovery model A and B based on the provisioned discovery security parameters (i.e., DUSKs and/or DUCKs). However, the RSC is not protected in subsequent link setup procedure even when it can be protected in a similar way as in the discovery. To ensure this privacy protection in the subsequent link setup procedures, this solution can be optionally enabled by applying the same protection mechanisms to the Remote UE’s RSC (and PRUK ID) if they are transmitted between the Remote UE and the U2N relay. The protection mechanisms for the restricted discovery are based on TS 33.303 6.1.3.4.3 [1]. Note that this protection mechanism only applies when the RSC is privacy protected during restricted discovery procedure.

# 4 Detailed proposal

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

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

## 6.Y Solution #Y: Privacy enhancements during PC5 link setup for UE-to-Network relay

### 6.Y.1 Introduction

This solution addresses KI #5. This solution provides a mechanism for protecting RSC (and PRUK ID) during PC5 link setup for UE-to-Network (U2N) relay when RSC is protected in restricted discovery. In restricted discovery, RSC is protected (i.e., scrambled and/or ciphered) in both discovery model A and B based on the provisioned discovery security parameters (i.e., DUSKs and/or DUCKs). However, the RSC is not protected in subsequent link setup procedure even when it can be protected in a similar way as in the discovery. To ensure this privacy protection in the subsequent link setup procedures, this solution can be optionally enabled by applying the same protection mechanisms to the Remote UE’s RSC (and PRUK ID) if they are transmitted between the Remote UE and the U2N relay. Note that this protection mechanism only applies when the RSC is privacy protected during restricted discovery procedure.

### 6.Y.2 Solution details

#### 6.Y.2.1 General

This solution provides a mechanism to optionally privacy protect the RSC and PRUK ID in Direct Communication Request (DCR) message based on the provisioned discovery security materials in case a restricted discovery is used to protect the discovery message during a PC5 link setup procedure for U2N relay service. In particular, the RSC and PRUK ID in DCR message are protected using the code-receiving security parameters as described in clause 6.Y.2.2. The U2N relay, on receiving the DCR message, retrieves the RSC and PRUK ID from DCR message using the code-sending security parameters as described in clause 6.Y.2.2 and checks if the RSC matches with the one that it sent in the discovery message. The reason that the code-receiving security parameters are used for privacy protection is to have consistency between discovery Model A and Model B, and reuse the already provisioned security parameters. The rest of the PC5 setup procedure remains the same as described in the U2N relay solution selected for the normative work.

#### 6.Y.2.2 Protection of PRUK ID and RSC over the PC5 interface

The Remote UE does the following:

- If the Remote UE is provisioned with DUCK:

 1. Form Message = RSC || PRUK ID

2. Calculate *Keystream* = KDF (DUCK, UTC-based counter) – see subclause 6.Y.2.3.

3. Ciphertext = Message XOR *Keystream*

- If the Remote UE is provisioned with DUSK:

1. Set the 4 LSBs of the UTC-based counter equal zero, for the purpose of this scrambling calculation only.

2. Compute the time-hash-bitsequence from Discovery User Scrambling Key (DUSK) and the UTC-based counter (modified as in step 1), passed through a keyed hash function as described in 6.Y.2.4.

3. XOR the time-hash-bitsequence with the RSC and PRUK ID being processed.

The UE-to-network relay does the following to retrieve the RSC and PRUK ID from the received DCR:

 - If the U2N relay UE is provisioned with DUCK:

1. Form Ciphertext = a part of protected (RSC || PRUK ID) in the received DCR message.

2. Calculate *Keystream* = KDF (DUCK, UTC-based counter) – see subclause 6.Y.2.3.

3. Message = Ciphertext XOR *Keystream*

 - If the U2N relay is provisioned with DUSK:

1. Set the 4 LSBs of the UTC-based counter equal zero, for the purpose of this scrambling calculation only.

2. Compute the time-hash-bitsequence from Discovery User Scrambling Key (DUSK) and the UTC-based counter (modified as in step 1), passed through a keyed hash function as described in 6.Y.2.4.

3. XOR the time-hash-bitsequence with the scrambled part of RSC and PRUK ID in the received DCR.

To provide an integrity and correctness check, the U2N relay UE has to verify that the RSC in the decrypted message is as expected, i.e., that it equals the RSC linked to the DUIK (or DUSK) used to decrypt the incoming encrypted message.

Editor’s Note: the FC values used in the confidentiality/scrambling routines for the DCR message protection must be different than the FC values used for the discovery message protection.

#### 6.Y.2.3 Calculation of message-specific confidentiality keystream

When calculating the message-specific confidentiality keystream, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0xXX

- P0 = UTC-based counter

- L0 = length of above (i.e., 0x00 0x04).

The input key shall be the 256-bit DUCK.

The message-specific confidentiality keystream is set to the L least significant bits of the output of the KDF, where L is the length of the RSC and PRUK ID.

#### 6.Y.2.4 Calculation of time-hash-bitsequence

When calculating the time-hash-bitsequence, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [12]:

- FC = 0xZZ

- P0 = UTC-based counter (modified as in subclause 6.Y.2.2)

- L0 = length of above (i.e., 0x00 0x04).

The input key shall be the 256-bit DUSK.

The time-hash-bitsequence keystream is set to the L least significant bits of the output of the KDF, where L is the length of the RSC and PRUK ID.

## 6.Y.3 Solution Evaluation

The solution fulfils the requirements of KI#5 by protecting Remote UE’s RSC and PRUK ID in case 1) a restricted discovery is performed as a relay discovery and 2) RSC is protected based on either a DUCK or DUSK during restricted discovery.

This solution does not introduce additional network impacts.

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