**3GPP TSG-SA3 Meeting #106-e S3-220328**

**e-meeting, 14 - 25 February 2022** *revision of S3-22xxxx*

**Source: Qualcomm Incorporated**

**Title: CR to ProSe TS – Privacy protection of RSC and PRUK ID over U2N relay**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***This contribution proposes a text on privacy protection mechanism for U2N relay in TS 33.503.***

# 2 References

[1] TR 33.847 “Study on security aspects of enhancement for proximity based services in the 5G System (5GS)”

# 3 Rationale

This contribution proposes to add a content for privacy protection mechanism over UE-to-Network Relay Communication based on the conclusion in TR 33.847 [1].

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the ProSe TS.

**\*\*\*\*\* START OF 1st CHANGES \*\*\*\*\***

### 6.3.5 Security for Direct Communication Request in 5G ProSe UE-to-Network Relay Communication

#### 6.3.5.1 General

This clause describes the mechanism to protect the privacy of the PRUK ID and RSC in Direct Communication Request (DCR) message when restricted discovery is used for the U2N relay service.

Editor’s Note: the description of integrity protection needs to be added

#### 6.3.5.2 Security Protection of the DCR message

The Remote UE encrypts the PRUK ID and RSC using the code-receiving security parameters used for discovery. The U2N relay UE, on receiving the DCR message, decrypts the encrypted PRUK ID and RSC using the code-sending security parameters used for discovery and verifies if the RSC matches with the one that it sent in the discovery message. If the RSC does not match, the relay UE shall abort the PC5 direct link establishment procedure.

The Remote UE shall encrypt the RSC and PRUK ID as follows:

1. If the UE is configured with DUCK, the DCR ciphering key KDCR is set to DUCK. If the UE is configured with DUSK but not DUCK, KDCR is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and Step 2-3 is skipped.

2. Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in A.zz.

3. XOR the first L bits of the Keystream with the RSC where L is the length of the RSC, and XOR the remaining bits of the Keystream with the PRUK ID.

NOTE: If PRUK ID is in NAI format, encryption of the PRUK ID is performed on the username part of the PRUK ID.

The UE-to-network relay shall decrypt the encrypted PRUK ID and RSC as follows:

1. If the UE is configured with DUCK, the DCR ciphering key KDCR is set to DUCK. If the UE is configured with DUSK but not DUCK, KDCR is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and Step 2-3 is skipped.

2. Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in A.zz.

3. XOR the first L bits of Keystream with the encrypted RSC where L is the length of the encrypted RSC, and XOR the remaining bits of Keystream with the encrypted PRUK ID.

NOTE: If PRUK ID is in NAI format, decryption of the PRUK ID is performed on the username part of the PRUK ID.

Editor’s Note: integrity protection of DCR message or a part of DCR message needs to be added

**\*\*\*\*\* END OF 1st CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 2nd CHANGES \*\*\*\*\***

# A.zz Calculation of DCR 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 [8]:

- FC = 0xBB

- P0 = UTC-based counter

- L0 = length of UTC-based counter (i.e., 0x00 0x04).

- P1 = RSC

- L1 = length of RSC (i.e., 0x00 0x03).

The input key shall be the 256-bit selected key in Step 1 of clause 6.3.5.2.

The DCR confidentiality keystream is set to L least significant bits of the output of the KDF, where L = the length of the RSC + the length of the PRUK ID.

NOTE: If PRUK ID is in NAI format, the length of the PRUK ID is determined by the username part of the PRUK ID.

**\*\*\*\*\* END OF 2nd CHANGES \*\*\*\*\***