**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220996-r1***

**e-meeting, 16 - 20 May 2022**

**Source: Qualcomm Incorporated, Huawei, HiSilicon**

**Title: CR to ProSe TS - Address the Editor’s Notes in clause 6.3.5**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes to update the text in clause 6.3.5 in TS 33.503.***

# 2 References

[1] TS 33.503: “Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)”

# 3 Rationale

This contribution proposes to address the following two Editor’s Notes in clause 6.3.5.

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

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

The above two Editor’s Notes were added in the previous meeting because an attacker can perform a denial of a U2N relay service on remote UEs by tampering a part of DCR message although the PRUK ID and RSC are privacy protected.

To address the above Editor’s Notes, we propose to add a mechanism to integrity protect the DCR message.

Particularly for the second Editor’s Note, if only a part of DCR message (e.g., PRUK ID and RSC) is integrity protected, an attacker could still manipulate the other parts of the message to induce additional signalling overheads in the network. Thus, we propose to integrity protect the entire DCR message.

# 4 Detailed proposal

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

### 6.3.5 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. This clause also describes a mechanism to integrity protect the DCR message when DUIK is provisioned for discovery.

#### 6.3.5.2 Privacy protection of PRUK ID and RSC in DCR

The 5G ProSe Remote UE encrypts the PRUK ID and RSC using the code-receiving security parameters used for discovery. The 5G ProSe UE-to-Network Relay, 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 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe 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 Steps 2-3 are skipped.

2. Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in A.5.

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 1: 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 Steps 2-3 are skipped.

2. Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in A.5.

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

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

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

#### 6.3.5.3 Integrity protection of DCR

The 5G ProSe Remote UE integrity protects the DCR message using the code-receiving security parameters used for discovery. The integrity protection of the DCR message is performed after the privacy protection of PRUK ID and RSC.

The 5G ProSe UE-to-Network Relay, on receiving the DCR message, verifies the integrity of the received DCR message using the code-sending security parameters used for discovery. If the integrity verification of the DCR fails, the 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe Remote UE shall integrity protect the DCR as follows:

1. If the UE is configured with DUIK, the DCR integrity key KINT is set to DUIK. Otherwise, the DCR message is not integrity protected, and Steps 2-3 are skipped.

2. Calculate Message Integrity Check (MIC) using KINT, UTC-based counter and the DCR message as described in A.XX.

3. Set the MIC IE to the calculated MIC.

The UE-to-network relay shall verify the integrity of the received DCR message as follows:

1. If the UE is configured with DUIK, the DCR integrity key KINT is set to DUIK. Otherwise, the DCR message is not integrity protected, and Step 2 is skipped.

2. Calculate a MIC using KINT, UTC-based counter and the received DCR message as described in A.XX and compare the calculated MIC with the MIC included in the DCR message. If they mismatch, the integrity check fails.

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

**\*\*\*\*\* START OF 3rd CHANGES \*\*\*\*\***

# A.XX Calculation of MIC value for Direct Communication Request

When calculating a MIC using the DUIK to integrity protect Direct Communication Request (DCR) message, 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 = 0xCC.

- P0 = UTC-based counter.

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

- P1 = DCR message with the MIC value field set to all zeros.

- L1 = length of above.

The MIC is set to the 32 least significant bits of the output of the KDF.

The DUIK, UTC-based counter and DCR message follow the encoding also specified in Annex B of TS 33.220 [8].

**\*\*\*\*\* END OF 3rd CHANGES \*\*\*\*\***