**3GPP TSG-SA3 Meeting #107-e *draft\_S3-221001-r1***

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

**Source: Qualcomm Incorporated, Ericsson**

**Title: CR to ProSe TS - Clarification on Knrp derivation for U2N relay over user plane**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes to update texts in clause 6.3.3.2.2 and add an annex 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 update the procedure of UE-to-Network (U2N) relay over user plane.

Particularly, in the security procedure for U2N relay over user plane, KNRP is defined as the equivalent key specified in TS 33.536. However, KNRP derivation for U2N relay over user plane is different from the KNRP derivation specified in TS 33.536 based on the description in step 4d in clause 6.3.3.2.2:

* The 5G PKMF of the 5G ProSe Remote UE shall generate KNRP freshness parameter 2 and derive KNRP using the PRUK identified by PRUK ID, RSC, KNRP freshness parameter 1 and KNRP freshness parameter 2.

Thus, this contribution proposes to add an annex for calculation of KNRP based on the description in step 4d.

# 4 Detailed proposal

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

##### 6.3.3.2.2 5G ProSe Remote UE attaching to a 5G ProSe UE-to-Network Relay



Figure 6.3.3.2.2-1: Authorization and secure PC5 link establishment procedure for 5G ProSe UE-to-Network Relay

The 5G ProSe Remote UE is provisioned with the discovery security materials (see clause 6.1.3.2) and Prose Remote User Key (PRUK) when it is in coverage. These security materials are associated with an expiration time, after which they become invalid. If the UE does not have valid discovery security materials, the 5G ProSe Remote UE needs to connect to the 5G PKMF and obtain fresh ones to use the 5G ProSe UE-to-Network Relay services.

NOTE 1: The procedure is described for the scenario that the 5G PKMF of the 5G ProSe Remote UE is different from the 5G PKMF of the 5G ProSe UE-to-Network Relay. If both the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay are served by a single 5G PKMF, the 5G PKMF takes the role of the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the 5G ProSe UE-to-Network Relay and the inter-5G PKMF message exchanges are not needed.

NOTE 2: Steps 0a, 0b, 1a, 1b are performed when the 5G ProSe Remote UE is in coverage.

0a. The 5G ProSe Remote UE gets the 5G PKMF address from the 5G DDNMF of its HPLMN. Alternatively, the 5G ProSe Remote UE may be provisioned with the 5G PKMF address by PCF. If the 5G ProSe Remote UE is provisioned with the 5G PKMF address, the 5G ProSe Remote UE may access the 5G PKMF directly without requesting it to the 5G DDNMF. In case that the 5G ProSe Remote UE cannot access the 5G PKMF using the provisioned 5G PKMF address, the 5G ProSe Remote UE may request the 5G PMKF address to the 5G DDNMF.

0b. The 5G ProSe Remote UE shall establish a secure connection with the 5G PKMF via PC8 reference point. Security for PC8 interface relies on Ua security if GBA specified in TS 33.220 [8] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [5] is used (see clause 5.2.5.4). The 5G PKMF of the 5G ProSe Remote UE shall check whether the 5G ProSe Remote UE is authorized to receive UE-to-Network relay service and if the UE is authorized, the 5G PKMF of the 5G ProSe Remote UE provides the discovery security materials to the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe Remote UE shall request the discovery security materials to the 5G PKMFs of the potential 5G ProSe UE-to-Network Relay UEs from which the 5G ProSe Remote UE gets the relay services, if the 5G ProSe Remote UE provided the list of the visited networks. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to be provided to the 5G ProSe Remote UE.

NOTE 3: The 5G PKMF may be locally configured with the UE’s authorization information. Otherwise, the 5G PKMF interacts with the UDM to retrieve the UE’s authorization information.

NOTE 4: The 5G ProSe Remote UE is provisioned by PCF with the list of the potential visited networks for the 5G ProSe UE-to-Network Relay service (which is identified by RSC).

0c. The 5G ProSe UE-to-Network Relay gets the 5G PKMF address from its HPLMN in the same way as described in step 0a.

0d. The 5G ProSe UE-to-Network Relay shall establish a secure connection with the 5G PKMF via PC8 reference point as in step 0b. The 5G PKMF of the 5G ProSe UE-to-Network Relay shall check whether the 5G ProSe UE-to-Network Relay is authorized to provide 5G ProSe UE-to-Network relay service and if authorized, the 5G PKMF of the 5G ProSe UE-to-Network Relay provides the discovery security materials to the 5G ProSe UE-to-Network Relay. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to the 5G ProSe UE-to-Network Relay.

1a. The 5G ProSe Remote UE sends a PRUK Request message to its 5G PKMF. The message indicates that the 5G ProSe Remote UE is requesting a PRUK from the 5G PKMF. If the 5G ProSe Remote UE already has a PRUK from this 5G PKMF, the message shall also contain the PRUK ID of the PRUK.

 PRUK ID shall take the form of either the NAI format or the 64-bit string.

1b. The 5G PKMF checks that the 5G ProSe Remote UE is authorised to receive UE-to-Network relay services. This is done by using the 5G ProSe Remote UE’s identity associated with the key used to establish the secure connection between the 5G ProSe Remote UE and 5G PKMF in step 0b. If the 5G ProSe Remote UE is authorised to receive the service, the 5G PKMF sends a PRUK and PRUK ID to the 5G ProSe Remote UE. If a PRUK and PRUK ID are included, the 5G ProSe Remote UE shall store these and delete any previously stored ones for this 5G PKMF.

2. The discovery procedure is performed between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay using the discovery parameters and discovery security material as described in clause 6.1.3.2.

3. The 5G ProSe Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID or a SUCI if the Remote UE does not have a valid PRUK, Relay Service Code (RSC) of the 5G ProSe UE-to-Network Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-Network Relay. If PRUK ID does not contain the HPLMN ID of the 5G ProSe 5G ProSe Remote UE or the routing information to the 5G PKMF of the 5G ProSe Remote UE (e.g., realm part when the NAI format of PRUK ID is used), the DCR message shall include the HPLMN ID of the 5G ProSe Remote UE. The PC5 security establishment procedure between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay including security parameters and security policy negotiation and protection of messages hereafter shall follow the one-to-one security establishment described in clause 6.2.3 of the present document. Only additional parameters required for the 5G ProSe Layer-3 UE-to-Network Relay scenario are described in this subclause.

Editor’s Note: privacy of PRUK ID is FFS.

4a. The 5G ProSe UE-to-Network Relay sends a Key Request message that contains PRUK ID or SUCI, RSC and KNRP freshness parameter 1 to its 5G PKMF. The Key Request message shall also include the HPLMN ID of the 5G ProSe Remote UE if it is included in the DCR.

4b. On receiving the Key Request message, the 5G PKMF of the 5G ProSe UE-to-Network Relay shall check if the 5G ProSe UE-to-Network Relay is authorized to provide relay service to the 5G ProSe Remote UE based on the 5G ProSe UE-to-Network Relay’s identity associated with the key used to establish the secure PC8 connection and the received RSC. If the 5G ProSe UE-to-Network Relay’s authorization information is not locally available, the 5G PKMF shall request the authorization information to the UDM of the 5G ProSe UE-to-Network Relay (not shown in the figure). If the 5G ProSe UE-to-Network Relay is authorized to provide the relay service based on ProSe Subscription data as specified in TS 23.502 [10], the 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Request with the PRUK ID or the SUCI to the 5G PKMF of the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe UE-to-Network Relay identifies the 5G PKMF address of the 5G ProSe Remote UE based on the PRUK ID or HPLMN ID or SUCI of the 5G ProSe Remote UE if it is included in the Key Request message.

4c. On receiving the Key Request message from the 5G PKMF of the 5G ProSe UE-to-Network Relay, the 5G PKMF of the 5G ProSe Remote UE shall check if the 5G ProSe Remote UE is authorized to use the relay service. The relay service authorization check shall be based on the PRUK ID and RSC included in the Key Request message or the SUPI of the Remote UE and the RSC included in the Key Request message. If a SUCI is included in the Key Request message, the 5G PKMF of the 5G ProSe Remote UE shall request the UDM of the 5G ProSe Remote UE to de-conceal the SUCI to gain the SUPI. If the 5G ProSe Remote UE’s authorization information is not locally available, the 5G PKMF shall request the authorization information to the UDM of the 5G ProSe Remote UE (not shown in the figure).

If a new PRUK is required, the 5G PKMF shall perform the one of the following procedures (as shown in the step 4c in the figure):

- If the 5G PKMF of the 5G ProSe Remote UE supports the Zpn interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF of the 5G ProSe Remote UE may request a GBA Push Info (GPI – see TS 33.223[9]) for the 5G ProSe Remote UE from the BSF. When requesting the GPI, the 5G PKMF shall include a PRUK ID in the P-TID field. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF supports the SBI interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF may request the GPI via SBI interface as described in TS 33.223[9]. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF of the 5G ProSe Remote UE supports the PC4a interface to the HSS of the UE, then the 5G PKMF of 5G ProSe Remote UE may request a GBA Authentication Vector (AV) for the 5G ProSe Remote UE from the HSS. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF is co-located or integrated with BSF functionality and supports the SBI interface to the UDM/HSS of the 5G ProSe Remote UE, the 5G PKMF may request the GBA AV via SBI interface as described in TS 33.220 [8]. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

NOTE 5: GPI is supported only when GBA is used.

4d. The 5G PKMF of the 5G ProSe Remote UE shall generate KNRP freshness parameter 2 and derive KNRP using the PRUK identified by PRUK ID, RSC, KNRP freshness parameter 1 and KNRP freshness parameter 2 as specified in A.XX. Then, the 5G PKMF of the 5G ProSe Remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 and the PC5 security policies of the relay service to the 5G PKMF of the 5G ProSe UE-to-Network Relay. This message shall include GPI if generated.

4e. The 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Response message to the 5G ProSe UE-to-Network Relay, which includes the PC5 security policies of the relay service.

5a. The 5G ProSe UE-to-Network Relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.536 [6]. The 5G ProSe UE-to-Network Relay sends a Direct Security Mode Command message to the 5G ProSe Remote UE. This message shall include the KNRP Freshness Parameter 2 and the PC5 security policies, and shall be protected as specified in TS 33.536 [6].

5b. If the 5G ProSe Remote UE receives the message containing the GPI, it processes the GPI as described in TS 33.223[xx]. The 5G ProSe Remote UE shall derive the PRUK and obtain the PRUK ID from the GPI.

The 5G ProSe Remote UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2 as specified in A.XX. It shall then derive the session key (KNRP-SESS) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the 5G ProSe UE-to-Network Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the 5G ProSe Remote UE that the 5G ProSe UE-to-Network Relay is authorized to provide the relay service.

Handling of synchronization failure (for details of synchronization failures – see TS 33.102[11]) when UE processes the authentication challenge in the GPI is performed similarly to clause 6.7.3.2.1.2 in TS 33.303 [4]. The 5G ProSe UE-to-Network Relay shall send the key request message to the 5G PKMF of the 5G ProSe Remote UE via the 5G PKMF of the 5G ProSe UE-to-Network Relay upon receiving the Direct Security Mode Failure message from the 5G ProSe Remote UE. The key request message shall include the RAND and AUTS received from the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe Remote UE shall request GPI as described in step 4c.

5c. The 5G ProSe Remote UE responds with a Direct Security Mode Complete message to the 5G ProSe UE-to-Network Relay as specified in TS 33.536 [6].

5d. On receiving the Direct Security Mode Complete message, the 5G ProSe UE-to-Network Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-Network Relay that the 5G ProSe Remote UE is authorized to get the relay service.

…

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

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

##### 6.3.3.2.3 PC5 Key Hierarchy over User Plane



Figure 6.3.3.2.3-1: PC5 Key Hierarchy for 5G ProSe UE-to-Network Relay security over User Plane

The different layers of keys (see Figure 6.3.3.2.3-1) are the following:

- PRUK: The root credential of security of the PC5 unicast link.

- KNRP: The key is equivalent to KNRP as specified in TS 33.536 [6]. This key is derived as specified in Annex A.XX.

- KNRP-SESS: This key is derived as specified in TS 33.536 [6].

- NRPEK, NRPIK: These keys are derived as specified in TS 33.536 [6].

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

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

Annex <A> (normative):
Key derivation functions

# A.1 KDF interface and input parameter construction

## A.1.1 General

All key derivations for 5G ProSe shall be performed using the key derivation function (KDF) specified in Annex B.2.2 of TS 33.220 [8].

This clause specifies how to construct the input string, S, and the input key, KEY, for each distinct use of the KDF. Note that "KEY" is denoted "Key" in TS 33.220 [8].

## A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [8], FC values allocated for the present document are : 0xXX, , 0xAA , 0xZZ, 0xYY.

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

**\*\*\*\*\* START OF 4th CHANGES \*\*\*\*\***

# A.XX Calculation of KNRP for UE-to-network relays

When calculating KNRP from PRUK, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [5]:

- FC = 0xYY

- P0 = Relay Service Code

- L0 = length of Relay Service Code (i.e., 0x00 0x03)

- P1 = KNRP freshness parameter 1

- L1 = length of KNRP freshness parameter 1 (i.e., 0x00 0x10)

- P2 = KNRP freshness parameter 2

- L2 = length of KNRP freshness parameter 2 (i.e., 0x00 0x10)

The input key shall be the 256-bit PRUK.

**\*\*\*\*\* END OF 4th CHANGES \*\*\*\*\***