**3GPP TSG-SA3 Meeting #105-e draft\_S3-214140-r1**

**e-meeting, 8 - 19 November 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated, Ericsson**

**Title: User-plane UE-to-network relay connection procedure**

**Document for: Approval**

**Agenda Item: 4.21**

# 1 Decision/action requested

***This contribution proposes a text on User-plane U2N relay for ProSe TS***

# 2 References

[1] TR 33.847 v.0.8.0 “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 User-plane UE-to-network relay 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 CHANGES \*\*\*\*\***

## 6.4.3.2 Security procedure over User Plane

### 6.4.3.2.1 General

This clause describes a mechanism to setup a PC5 link between a remote UE and UE-to-network relay. The mechanism includes how a Remote UE and UE-to-network relay get authorized by the ProSe Key Management Function (PKMF) and verify each other’s role.

Editor’s Note: Co-existence with CP based solution is FFS

### 6.4.3.2.2 Remote UE attaching to a ProSe UE-to-network relay



Figure 6.4.3.2.2-1: Authorization and secure PC5 link establishment procedure for UE-to-network relay

The remote UE is provisioned with the discovery security materials (see clause w.x.y.z) 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 Remote UE needs to connect to the PKMF and obtain fresh ones to use the UE-to-Network relay services.

NOTE 1: The procedure is described for the scenario that the PKMF of the remote UE is different from the PKMF of the UE-to-network relay. If both the remote UE and the UE-to-network relay are served by a single PKMF, the PKMF takes the role of the PKMF of the remote UE and the PKMF of the UE-to-network relay and the inter-PKMF message exchanges are not needed.

NOTE 2: Steps 0a, 0b, 1a, 1b are performed when the remote UE is in coverage.

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

0b. The remote UE shall establish a secure connection with the PKMF via PCx reference point. Security for PCx interface relies on Ua security if GBA [zz] is used (see Clause 5.Y.Y.4) or Ua\* security if AKMA [aa] is used (see Clause 5.Y.Y.5). The PKMF shall check whether the Remote UE is authorized to receive UE-to-network relay service and if the UE is authorized, the PKMF provides the discovery security materials to the Remote UE. The PKMF of the remote UE shall request the discovery security materials to the PKMFs of the potential relay UEs from which the remote UE gets the relay services, if the Remote UE provided the list of the visited networks.

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

NOTE 4: The remote UE is provisioned by PCF with the list of the potential visited networks for the UE-to-network relay service (which is identified by RSC).

0c. The UE-to-network relay gets the ProSe Key management function (PKMF) address from its HPLMN in the same way as described in step 0a.

0d. The UE-to-network relay shall establish a secure connection with the PKMF via PCx reference point as in step 0b. The PKMF shall check whether the UE-to-network relay is authorized to act as a relay and if authorized, the PKMF provides the discovery security materials to the UE-to-network relay.

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

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

2. The discovery procedure is performed between the Remote UE and the UE-to-network Relay using the discovery parameters and discovery security material as described in X.Y.Z.

3. The Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID, Relay Service Code (RSC) of the UE-to-network relay service and KNRP freshness parameter 1 to the UE-to-network relay. If PRUK ID does not contain the HPLMN ID of the Remote UE or the routing information to the PKMF of the 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 Remote UE. The PC5 security establishment procedure between the Remote UE and the 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 x.y.z.w of the present document. Only additional parameters required for the Layer-3 UE-to-network relay scenario are described in this subclause.

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

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

4b. On receiving the Key Request message, the PKMF of the UE-to-network relay shall check if the UE-to-network relay is authorized to act as a relay to the Remote UE based on the UE-to-network relay’s identity associated with the key used to establish the secure PCx connection. If the UE-to-network relay’s authorization information is not locally available, the PKMF shall request the authorization information to the UDM of the UE-to-network relay (not shown in the figure). If the UE-to-network relay is authorized to provide the relay service, the PKMF of the UE-to-network relay sends the Key Request with the PRUK to the PKMF of the remote UE. The PKMF identifies the PKMF address of the Remote UE based on the PRUK ID or HPLMN ID of the Remote UE if it is included in the Key Request message.

Editor’s Note: PKMF’s authorization check of the UE with UDM requires alignment with SA2.

4c. On receiving the Key Request message from the PKMF of the UE-to-network relay, the PKMF of the Remote UE shall check if the Remote UE is authorized to use the relay service based on the PRUK ID and RSC included in the Key Request message. If the Remote UE’s authorization information is not locally available, the PKMF shall request the authorization information to the UDM of the Remote UE (not shown in the figure).

If the PKMF determines a PRUK to be refreshed, the PKMF shall perform the one of the following procedures:

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

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

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

Editor’s Note: GBA push info (GPI) aspects are still under discussion in TR 33.847 [x] therefore additional details for GPI handling are FFS.

 The PKMF of the 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. Then, the PKMF of the remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the PKMF of the UE-to-network relay. This message shall include GPI if generated.

4d. The PKMF of the UE-to-network relay sends the Key Response message to the UE-to-network relay.

5a. The UE-to-network relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) and integrity key (NRPIK) as specified in TS 33.536 [ww]. The UE-to-network relay sends a Direct Security Mode Command message to the Remote UE. This message shall include the KNRP Freshness Parameter 2 and be protected as specified in TS 33.536 [ww].

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

The Remote UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2. It shall then derive the session key (KNRP-SESS) in the same manner as the UE-to-network relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the Remote UE that the UE-to-network relay is authorized to provide the relay service.

5c. The Remote UE responds with a Direct Security Mode Complete message to the UE-to-network relay.

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

6. The remote UE and UE-to-network relay continues the rest of procedure for the relay service over the secure PC5 link.

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