**3GPP TSG-SA3 Meeting #107-e *S3-221141***

**e-meeting, 16 - 20 May 2022** revision of S3-22xxxx

**Source: Philips International B.V.**

**Title: Relay Discovery clarifications**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes to clarify the security procedures used for U2N relay discovery in TS 33.503.***

# 2 References

[1] 3GPP TS 33.503 v0.3.0

# 3 Rationale

The security procedures for ProSe UE-to-Network relay discovery rely on the ProSe restricted direct discovery procedures. However, the CP and UP security procedures relate to the discovery procedures needs to be clarified.

# 4 Detailed proposal

It is proposed that SA3 approve the below draft CR to TS 33.503 [1] to clarify the UE-to-NW relay discovery procedures used for the UP and CP security procedures.

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

#### 6.3.3.2 Security procedure over User Plane

##### 6.3.3.2.1 General

This clause describes a mechanism to setup a PC5 link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay. The mechanism includes how a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay get authorized by the 5G ProSe Key Management Function (5G PKMF) and verify each other’s role.

##### 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, following the procedures in clause 6.1.3.2. 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, following the procedures in clause 6.1.3.2. 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. 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. 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.

5e. The 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE after the successful verification to finish the PC5 connection establishment procedures.

6. The 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay continues the rest of procedure for the relay service over the secure PC5 link.

##### 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].

- KNRP-SESS: The key is equivalent to KNRP-sess as specified in TS 33.536 [6].

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

#### 6.3.3.3 Security procedure over Control Plane

##### 6.3.3.3.1 General

This subclause describes the security mechanisms for the 5G ProSe Layer-3 UE-to-Network Relay authentication, authorization and key management using the primary authentication for PC5 keys establishment. Network entities AMF, AUSF and UDM are involved for key derivation and distribution of keys used for 5G ProSe UE-to-Network Relay communication. The UE shall be provisioned with necessary policies and parameters to use 5G ProSe services, as part of the UE ProSe Policy information as defined in TS 23.503 [7] clause 4.2.2. PCF shall provision the authorization policy and parameters for 5G ProSe UE-to-Network Relay discovery and communication as specified in 5.1.4 in TS 23.304 [2].

##### 6.3.3.3.2 Connection with 5G ProSe UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment

This subclause describes a procedure for a 5G ProSe Remote UE to establish a PC5 link between a 5G ProSe Remote UE and a 5G ProSe UE-to-Network Relay. The procedure includes how the 5G ProSe Remote UE is authenticated by AUSF via 5G ProSe UE-to-Network Relay and 5G ProSe UE-to-Network Relay's AMF during 5G ProSe PC5 establishment. The mechanism can be used by a 5G ProSe Remote UE while out of coverage.



Figure 6.3.3.3.2-1: 5G ProSe UE-to-Network Relay security procedure with setup of network Prose security context during PC5 link establishment

0. The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay shall be registered with the network. The 5G ProSe UE-to-Network Relay shall be authenticated and authorized by the network to provide UE-to-Network relay service. The 5G ProSe Remote UE shall be authenticated and authorized by the network to receive UE-to-Network relay service. PC5 security policies are provisioned to the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay by their own respective PCF (not shown in the figure) during this authorization and information provisioning procedure. The discovery security materials are provisioned as per clause 6.1.3.2.

1. The 5G ProSe Remote UE shall initiate discovery procedure using any of Model A or Model B method as specified in clause 6.3.1.2 or 6.3.1.3 of TS 23.304 [2] respectively, following the security procedures in clauses 6.1.3.2.2.1 and 6.1.3.2.2.2.

2-5. After the discovery of the 5G ProSe UE-to-Network Relay, the 5G ProSe Remote UE shall send a Direct Communication Request to the 5G ProSe UE-to-Network Relay for establishing secure PC5 unicast link. The 5G ProSe Remote UE shall include its security capabilities and PC5 security signalling policy in the DCR message as specified in TS 33.536 [6]. The message shall also include SUCI, Relay Service Code, Nonce\_1. Upon receiving the DCR message, the 5G ProSe UE-to-Network Relay shall send the Relay Key Request to the AMF of the 5G ProSe UE-to-Network Relay, including partial parameters received in the DCR message. The 5G ProSe UE-to-Network Relay shall also include in the message a transaction identifier that identifies the 5G ProSe Remote UE for the subsequent messages over 5G ProSe UE-to-Network Relay's NAS messages and PC5 messages. The AMF of the 5G ProSe UE-to-Network Relay shall verify whether the 5G ProSe UE-to-Network Relay is authorized to provide the UE-to-Network relay service. The AMF of the 5G ProSe UE-to-Network Relay shall select an AUSF based on SUCI and forward the parameters received in Relay Key Request to the AUSF in Nausf\_UEAuthentication\_ProseAuthenticate Request message. The Nausf\_UEAuthentication\_ProseAuthenticate Request message shall contain the 5G ProSe Remote UE’s SUCI, Relay Service Code, Nonce\_1. The AUSF shall initiate a 5G ProSe Remote UE specific authentication using the ProSe specific parameters received (i.e., RSC, etc.). The serving network name handling is same as defined in TS 33.501 [3]. The 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.

6. The AUSF of the 5G ProSe Remote UE shall retrieve the Authentication Vectors from the UDM via Nudm\_UEAuthentication\_GetProseAv Request message and trigger authentication of the 5G ProSe Remote UE . This authentication is performed between the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay and the 5G ProSe UE-to-Network Relay. Based on SUPI, the UDM shall choose the authentication method.

7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE shall trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf\_UEAuthentication\_ProSeAuthenticate Response message.

7b. The AMF of the 5G ProSe UE-to-Network Relay shall forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay shall forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102 [11].

For EAP-AKA', the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' according to Annex A.3 in TS 33.501.

7d. The 5G ProSe Remote UE shall return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf\_UEAuthentication\_ProSeAuthenticate Request.

The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information as described in TS33.501.

For EAP-AKA’, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA’-Notification and EAP-Response /AKA’-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculatingthe KSEAF.

The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall derive a new KAUSF\_P (different from KAUSF). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall generate 5GPRUK as specified in Annex A.2 and 5GPRUK ID as specified in Annex A.3 using the newly derived KAUSF\_P.

9. The AUSF of the 5G ProSe Remote UE shall generate the KNR\_ProSe key as defined in Annex A.4.

10-11. The AUSF of the 5G ProSe Remote UE shall send the KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the 5G ProSe UE-to-Network Relay via the AMF of the 5G ProSe UE-to-Network Relay. When receiving a KNR\_ProSe from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay shall not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality and integrity keys from KNR**\_**ProSe, as defined in clause 6.3.3.3.3 of this document. KNR\_ProSe ID and Krelay-sess ID are established in the same way as KNRP ID and KNRP-sess ID in TS 33.536 [6].

12. The 5G ProSe UE-to-Network Relay shall send the received Nonce\_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

13-15. The 5G ProSe Remote UE shall use the 5GPRUK ID to locate the KAUSF\_P/5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE shall generate the KNR\_ProSe key to be used for Remote access via the 5G ProSe UE-to-Network Relay in the same way as defined in step 9. The 5G ProSe Remote UE shall derive PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe the same way as defined in step 11. The 5G ProSe Remote UE shall send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

Further communication between the 5G ProSe Remote UE and the Network takes place securely via the 5G ProSe UE-to-Network Relay.

Editor's note: Further details on the needs and usage of 5GPRUK ID are FFS.

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