**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220371-r6***

**e-meeting, 14 - 25 February 2022 (merger of S3-220288 and S3-220371)**

**Source: Ericsson**

**Title: Alternative solution to handle PRUK and PRUK ID**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***This contribution attempts to resolve an editor note in control plane solution for UE-to-network relays in draft TS 33.503.***

# 2 References

[1] 3GPP TS 33.503 "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)"

[2] S3-220375 "Removal of PRUK ID in CP based solution"

# 3 Rationale

This contribution proposes to resolve the following editor note in control plane solution for UE-to-network relays in draft TS 33.503:

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

Considering the time plan of Release 17, we believe the most straightforward to address this EN would be to remove the 5G PRUK ID in the control plane solution for UE-to-network relays as proposed in S3-220375 [2].

This contribution proposes an alternative solution to introduce a new NF to handle PRUK and PRUK ID, which in our view introduces less impacts towards the existing NFs.

In EPC Prose solution or the UP solution of 5G Prose, PRUK ID is used by the PKMF to identify the PRUK and the remote UE, if the Remote UE has a PRUK generated already. Otherwise, the Remote UE shall use its permanent subscription ID in Direct Communication Request over the relay interface. That is, PRUK ID acts as a temporary UE ID over the relay interface to have certain UE ID privacy protection; PRUK ID is generated and used by a NF to identify the remote UE and the associated PRUK stored locally; PRUK ID enables the reuse of PRUK for U2N security of subsequent requests.

Come back to the CP solution of 5G Prose, obviously such usage of PRUK ID as UE ID or for UE ID privacy protection has overlapping with SUCI. The question is how PRUK could be reused for U2N security of subsequent requests in this context.

This contribution proposes a new NF Prose Anchor Function (PAnF for brevity) to manage PRUK and PRUK ID for the remote UE for the CP solution. PAnF is located in Remote UE’s HPLMN e.g. as AUSF and UDM.

This mechanism is based on a bit similar principle of the currently defined UP solution for 5G Prose and/or AKMA procedure of 5GS in general. But it operates in the control plane and participates UE authentication procedure. Mind that PAnF is deployed independent to PKMF or AAnF, but it could also be collocated with these nodes if needed or as per operators' policy.

The advantages with the introduction of the new PAnF (i.e. ProSe Anchor NF (Remote)) to manage PRUK and PRUK ID would be the following:

* Less impacts in the network.
* Clearer design for the baseline NFs, e.g. no need to introduce temporary UE ID handling logic to AUSF/UDM etc.
* Possibility of collocating PAnF and PKMF to enable synergy with UP solution and aligned operator policy for CP and UP solutions.

Below the signalling flow in clause 6.3.3.3.2 for the CP based solution in TS 33.503 have been updated and enhanced with the new ProSe Anchor NF (Remote), together with description of the new steps.



**Figure: UE-to-Network Relay security procedure with setup of network Prose security context during PC5 link establishment enhanced with the new ProSe Anchor NF (Remote)**

1-4. Same procedure as defined for CP solution in TS 33.503 [1]. In addition, the remote UE may use PRUK ID in Direct Communication Request, if the Remote UE has a PRUK generated already.

5. The relay AMF triggers UE authentication and requests KNR\_ProSe from PAnF.

6-12. If SUCI is received, the PANF shall select AUSF based on SUCI and forward authentication request to the AUSF. AUSF/UDM performs SUCI de-concealment and UE authentication. Based on a successful UE authentication, the AUSF generates PRUK and PRUK ID and sends to PAnF.

13-14. If PRUK ID is received from the relay AMF, the PAnF discovers the PRUK stored locally otherwise the PAnF receives PRUK from the AUSF. The PAnF generates then KNR\_ProSe and sends back to the relay AMF.

15-18. Same procedure as defined for CP solution in TS 33.503 [1]. Mind that PRUK ID is not needed to be sent over PC5 as the Remote UE can self-generate PRUK ID.

# 4 Detailed proposal

It is proposed that SA3 approve the below draft CR to TS 33.503 [1] which introduces the new ProSe Anchor NF.

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

#### 6.3.3.3 Security procedure over Control Plane

Editor’s Notes: This clause describes the security procedure that relies on primary authentication procedure to authenticate/authorize UE during 5G ProSe UE-to-Network Relay Communication.

##### 6.3.3.3.1 General

This subclause describes the security mechanisms for the L3 U2N Relay authentication, authorization and key management using the UE authentication towards its home network for PC5 keys establishment. Network entities AMF, AUSF and UDM are involved for key derivation and distribution of keys used for 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 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 UE-to-Network Relay connection with setup of network Prose security context during PC5 link establishment

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



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

Editor's note: Steps text below need to be aligned with the figure.

0. The Remote UE and relay UE shall be registered with the network. The UE-to-Network relay shall be authenticated and authorized by the network to support as a relay UE. Remote UE shall be authenticated and authorized by the network to act as a Remote UE.

1. The 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.

2. After the discovery of the UE-to-Network relay, the Remote UE shall send a Direct Communication Request to the Relay UE for establishing secure PC5 unicast link. The Remote UE shall include its security capabilities and security policy in the DCR message as specified in TS 33.536 [6]. The message shall also include Relay Service Code and Nonce\_1.

If the Remote UE does not have a valid 5GPRUK, the Remote UE shall include SUCI in the DCR to trigger primary authentication and establish a PRUK.

If the Remote UE already has a valid 5GPRUK, the Remote UE shall include the 5GPRUK ID in the DCR to indicate that the Remote UE wants to get relay connectivity using the 5GPRUK.

3. Upon receiving the DCR message, the Relay UE shall send the Relay Key Request to the Relay AMF, including the Remote UE ID (SUCI or PRUK ID), RSC and Nonce\_1 received in the DCR message.

4. The Relay AMF shall verify whether the relay UE is authorized to act as U2N relay.

5. If SUCI is received from the Relay UE, the relay AMF shall select AUSF based on SUCI and forward the parameters in the key request to the AUSF in Nausf\_UEAuthentication\_ProSeAuthenticate Request message.

If 5GPRUK ID is received from the relay UE, the relay AMF selects the PAnF and skips the step 6-12.

NOTE: The PAnF may be collocated with PKMF as per operator's locally policy.

6-9. The AUSF shall retrieve the Authentication Vectors from the UDM via Nudm\_UEAuthentication\_GetProseAv Request message and trigger authentication of the remote UE. This authentication is performed between the AUSF and the remote UE via the relay AMF and relay UE. AUSF shall not make the newly derived KAUSF as the latest KAUSF. At the remote UE, the newly derived KAUSF shall not be taken as latest KAUSF as NAS SMC procedure is not performed between remote UE and relay AMF.

Editor's note: Further details on authentication message handling in UE, Relay UE's AMF and AUSF are FFS.

Editor's note: There are essentially two different KAUSF keys. Different key names should be used to avoid confusion and misleading. This is FFS.

10. On successful authentication, the AUSF and 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.

11a . The AUSF shall select the PAnF and send the SUPI, 5GPRUK, 5GPRUK ID, Nonce\_1, and Relay Service Code (RSC) in Npanf\_ProseKey\_Register Request message to the PAnF.

11b. The PAnF shall store the Prose context info (i.e. SUPI, 5GPRUK, 5GPRUK ID, Relay Service Code) for the Remote UE and generate Nonce\_2 and the KNR\_ProSe key as defined in Annex A.4. The PAnF shall send the KNR\_ProSe key, Nonce\_2 in Npanf\_ProseKey\_Register Response message to the AUSF.

12. The AUSF shall send the KNR\_ProSe key, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate\_Response message to the relay AMF.

13. If the relay AMF receives a 5G PRUK ID from the relay UE, then the relay AMF shall select PAnF based on 5G PRUK ID and forwards the 5G PRUK ID, Nonce\_1 and Relay Service Code (RSC) in the key request to the PAnF in Npanf\_ProseKey\_Get Request message.

14. When 5GPRUK ID, Nonce\_1 and RSC are received from the relay AMF, the PAnF discovers the 5G PRUK stored locally for the Remote UE. The PAnF shall generate Nonce\_2 and the KNR\_ProSe key as defined in Annex A.4.

15. The PAnF shall send the KNR\_ProSe key and Nonce\_2 in Npanf\_ProseKey\_Get Response message to the relay AMF.

NOTE: The PAnF may be collocated with PKMF as per operator's locally policy.

15. When receiving a KNR\_ProSe from the PAnF, the relay AMF shall not attempt to trigger NAS SMC procedure with Remote UE.

16.The Relay UE derives PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe, using the KDF 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].

17. The UE-to-Network relay shall send the received Nonce\_2 to the Remote UE in Direct Security mode command message.

18. The remote UE shall generate the KNR\_ProSe key to be used for Remote access via the Relay UE in the same way as defined in step 13. The Remote UE shall derive PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe the same way as defined in step 15.

19. The Remote UE shall send the Direct Security mode complete message to the UE-to-Network relay.

Further communication between Remote UE and Network takes place securely via the UE-to-Network relay.

##### 6.3.3.3.3 PC5 Key Hierarchy



Figure 6.3.3.3.3-1: PC5 Key Hierarchy for UE-to-Network Relay security

The different layers of keys (see Figure 6.3.3.3.3-1) are the following:

- 5GPRUK: The root credential derived from KAUSF that is the root of security of the PC5 unicast link.

- KNR\_ProSe: This is a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link. It may be refreshed by re-running the authentication to derive a fresh 5GPRUK.

- Krelay-sess: This is the 256-bit key that is derived by UE from KNR\_ProSe and is used derive keys that to protect the transfer of data between the UEs. The Krelay-sess is derived per unicast link same as KNRP-sessspecified in TS 33.536 [6]. During activated unicast communication session between the UEs, the Krelay-sess may be refreshed by running the rekeying procedure. The keys for confidentiality and integrity algorithms are derived directly from Krelay-sess. The 16-bit Krelay-sess ID identifies the Krelay-sess.

- Krelay-int, Krelay-enc: The Krelay-int and Krelay-enc are used in the chosen confidentiality and integrity algorithms respectively for protecting PC5-S signalling, PC5 RRC signalling, and PC5 user plane data. These keys are equivalent to NRPIK and NRPEK as specified in TS 33.536 [6]. They are derived from Krelay-sess and are refreshed automatically every time Krelay-sess is changed.

**\*\*\*\*\* NEXT CHANGE \*\*\*\*\***

# Annex X (normative): Support of SBA for ProSe

## X.2.1 Prose Anchor Function Services

### X.2.3.1 General

The Prose Anchor Function provides ProSe Key services to the requester NF by Npanf\_ProseKey.

The AUSF shall select PAnF and forward the key register to the PAnF in Npanf\_ProseKey\_Register Request message.

The relay AMF shall select PAnF based on 5GPRUK ID and forward the key request to the PAnF in Npanf\_ProseKey\_Get Request message

### X.2.3.2 Npanf\_ProseKey service

##### X.2.3.2.1 Npanf\_ProseKey\_Register Request service operation

**Service operation name:** Npanf\_ProseKey\_Register Request

**Description:** Provides Prose related keying material.

**Input, Required:** SUPI, 5G PRUK ID, PRUK, Relay Service Code, Nonce\_1.

**Input, Optional:** None.

**Output, Required:** KNR\_ProSe and Nonce\_2.

**Output, Optional:** None.

##### X.2.3.2.1 Npanf\_ProseKey\_Get Request service operation

**Service operation name:** Npanf\_ProseKey\_Get Request

**Description:** Provides Prose related keying material.

**Input, Required:** 5G PRUK ID, Relay Service Code, Nonce\_1.

**Input, Optional:** None.

**Output, Required:** KNR\_ProSe and Nonce\_2.

**Output, Optional:** None.

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