**3GPP TSG-SA3 Meeting #107-e *S3-22xxxx***

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

**Source: Interdigital, Samsung, LG Electronics, Nokia, Nokia Shanghai Bell, Ericsson, Verizon Wireless, MITRE, Convida Wireless LLC**

**Title: Security procedure over CP using PRUK ID in DCR**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes EN resolution for PRUK ID usage in CP procedure for U2N relay in TS 33.503.***

# 2 References

[1] 3GPP TS 33.503 v0.3.0

# 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.

It is based on S3-220371-r7 from SA3#106e, i.e., adding support for PRUK storage using the PAnF.

# 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

##### 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 5G ProSe Remote UE specific authentication for PC5 keys establishment. Network entities AMF, PAnF, 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: 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 respectively during this authorization and information provisioning procedure.

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.

2. 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 Relay Service Code and Nonce\_1.

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

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

3. 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 SUCI or 5GPRUK ID, RSC and Nonce\_1 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.

4. 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.

If 5GPRUK ID is received from the 5G ProSe UE-to-Network Relay, the AMF of the 5G ProSe UE-to-Network Relay selects the PAnF of the 5G ProSe Remote UE based on 5GPRUK ID and skips the steps 5-10.

5. 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 which shall contain the 5G ProSe Remote UE’s SUCI, Relay Service Code.

6. 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.

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\_P 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.

9a. The AUSF of the 5G ProSe Remote UE shall select the PAnF and send the SUPI, 5GPRUK, 5GPRUK ID, and RSC in Npanf\_ProseKey\_Register Request message to the PAnF.

9b. The PAnF shall store the Prose context info (i.e., SUPI, 5GPRUK, 5GPRUK ID, RSC) for the 5G ProSe Remote UE and send Npanf\_ProseKey\_Register Response message to the AUSF.

10. The AUSF of the 5G ProSe Remote UE shall send the Authentication result, 5GPRUK ID if the authentication is successful in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the AMF of the 5G ProSe UE-to-Network Relay.

11. The AMF of the 5G ProSe UE-to-Network Relay shall select the PAnF of the 5G ProSe Remote UE, based on 5GPRUK ID and forwards the 5GPRUK ID, Nonce\_1 and RSC in the Relay Key Request to the PAnF of the 5G ProSe Remote UE in Npanf\_ProseKey\_Get Request message.

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

13. The PAnF of the 5G ProSe Remote UE shall send the KNR\_ProSe key and Nonce\_2 in Npanf\_ProseKey\_Get Response message to the AMF of the 5G ProSe UE-to-Network Relay.

14. When receiving a KNR\_ProSe from the PAnF 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 AMF of the 5G ProSe UE-to-Network Relay shall send KNR\_ProSe , Nonce\_2 in Relay Key Response to the 5G ProSe UE-to-Network Relay. The AMF of the 5G ProSe UE-to-Network Relay shall also include the 5GPRUK ID in the message if received from the AUSF of the 5G ProSe Remote UE.

15. 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]. 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.

16. 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 12. 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 15.

17. 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.

18. 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 and store the 5GPRUK ID in the security context associated to the PC5 link with the 5G ProSe Remote UE.

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

##### 6.3.3.3.3 PC5 Key Hierarchy over Control Plane



**Figure 6.3.3.3.3-1: PC5 Key Hierarchy for 5G ProSe UE-to-Network Relay security over Control** **Plane**

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

- KAUSF\_P: A key derived based on Remote UE ProSe specific authentication and only used to derive 5GPRUK. It is different from KAUSF.

- 5GPRUK: The root credential derived from KAUSF\_P 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 (all text is new) \*\*\*\*\***

## 7.X. Prose Anchor Function Services

### 7.X.1 General

The Prose Anchor Function (PAnF) supports providing storage for the Prose context info (i.e., SUPI, 5GPRUK, 5GPRUK ID, RSC) for a 5G ProSe Remote UE and generation of KNR\_ProSe used by 5G ProSe UE-to-Network Relay for the security establishment of the PC5 link with 5G ProSe Remote UE. The following table shows the PAnF Service and the PAnF Service Operations.

Table 7.X.1-1: List of PAnF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation  Semantics | Example Consumer(s) |
| Npanf\_ProseKey | Npanf\_ProseKey\_Register | Request/Response | AUSF |
| Npanf\_ProseKey\_Get | Request/Response | AMF |

### 7.X.2 Npanf\_ProseKey service

##### 7.X.2.2.1 Npanf\_ProseKey\_Register service operation

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

**Description:** The NF consumer requests the PAnF to store the Prose context info (i.e., SUPI, 5GPRUK, 5GPRUK ID, RSC).

**Input, Required:** SUPI, 5G PRUK ID, 5GPRUK, Relay Service Code.

**Input, Optional:** None.

**Output, Required:** None.

**Output, Optional:** None.

##### 7.X.2.3.1 Npanf\_ProseKey\_Get service operation

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

**Description:** The NF consumer requests Prose Key from the PAnF.

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

**Input, Optional:** None.

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

**Output, Optional:** None.

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