**3GPP TSG-SA3 Meeting #107e draft\_S3-220816-r3**

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

**Source: LG Electronics, Interdigital, Huawei(?), HiSilicon(?)**

**Title: EN resolution for secondary authentication without N3IWF (Alt2)**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes EN resolution on secondary authentication for U2N relay in ProSe TS 33.503***

# 2 References

[1] TS 33.503 v.0.3.0 “Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS) (Release 17)”

# 3 Rationale

This contribution is prepared to resolve the below editor's notes, clarify some aspects and do some edits on secondary authentication for the Remote UE via L3 UE-to-network relay without N3IWF.

The below two editor's notes are removed as it is clarified how SMF gets SUPI from AMF in step 8 using 5GPRUK ID and PAnF and how SMF retrieves the remote UE's subscription data from the UDM using the received SUPI in step 9.

Editor’s Notes: How the SUPI of the remote UE is obtained by SMF is FFS.

Editor’s Notes: how SMF obtains the remote UE’s subscription info is FFS.

The below editor's note is removed as the roaming is not directly related to the secondary authentication. If there is a roaming issue, the main CP based authentication will not be successfully performed so there will be even no chance to initiate the secondary authentication procedure.

Editor’s Notes: It is FFS how to support secondary authentication when roaming..

Additionally,

1. It is clarified how the relay UE determines if SA is required for the DN that is associated with the RSC.
2. The relay session management context is reworded as U2N relay's SM context that is aligned with SA2 spec
3. Some editorial corrections and clarifications are also done

This proposal is prepared based on the main CP authentication procedure alternative#2 (deriving PRUK in AUSF)

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in [1].

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

##### 6.3.3.3.4 5G ProSe Remote UE Secondary Authentication via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF

###### 6.3.3.3.4.1 General

This clause specifies the secondary authentication between a 5G ProSe Remote UE via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF and an external data network (DN) based on network-controlled authorization (i.e., using 5G ProSe Remote UE primary authentication) as described in clause 6.3.3.3.2. This procedure is optional to support.

The SMF of the 5G ProSe UE-to-Network Relay triggers the secondary authentication of the 5G ProSe Remote UE based on the subscription information and the local configuration of the SMF when it receives a NAS message (e.g., Remote UE Report) from the 5G ProSe UE-to-Network Relay.

The EAP framework specified in RFC 3748 [12] shall be used for authentication between the 5G ProSe Remote UE and a DN-AAA server in the external data network.

Following clause describes the procedures for initial secondary authentication of the 5G ProSe Remote UE with the external DN-AAA server.

###### 6.3.3.3.4.2 PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay

The PDU session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay follows the steps described below on the Figure 6.3.3.3.4.2-1.



Figure 6.3.3.3.4.2-1: Procedure for PDU session secondary authentication of 5G ProSe Remote UE
via 5G ProSe Layer-3 UE-to-Network Relay

1. During the Registration procedure, authorization and provisioning are performed for 5G ProSe Remote UE(0a) and 5G ProSe Layer-3 UE-to-Network Relay(0b). When the 5G ProSe Remote UE is not in the coverage, the 5G ProSe Remote UE may use its preconfigured policy and parameter for PC5 discovery and communication to establish a PC5 connection with a 5G ProSe Layer-3 UE-to-Network Relay.

1. The 5G ProSe Layer-3 UE-to-Network Relay may establish a PDU session for relaying with default PDU session parameters received in step 0 or pre-configured in the 5G ProSe Layer-3 UE-to-Network Relay, e.g. S-NSSAI, DNN, SSC mode, or PDU Session Type.

2. Based on the authorization and provisioning in step 0, the 5G ProSe Remote UE performs the discovery of a 5G ProSe Layer-3 UE-to-Network Relay. As part of the discovery procedure, the 5G ProSe Remote UE learns about the connectivity service the 5G ProSe Layer-3 UE-to-Network Relay provides (e.g., based on a broadcasted service code).

3. The 5G ProSe Remote UE selects a 5G ProSe Layer-3 UE-to-Network Relay sends a DCR (Direct Communication Request) message including its SUCI or a 5GPRUK ID as described in 6.3.3.3.2.

4. On the condition that the DCR message includes a SUCI, the 5G ProSe Layer-3 UE-to-Network Relay triggers a network-controlled authorization of 5G ProSe Remote UE, as described in 6.3.3.3.2. If the required identity parameter (e.g., SUCI) is missing, the 5G ProSe Layer-3 UE-to-Network Relay may send an identity request message to the 5G ProSe Remote UE to obtain the 5G ProSe Remote UE identity (e.g., SUCI) before triggering the network-controlled authorization procedure of 5G ProSe Remote UE.

 If there is no PDU session satisfying the requirements of the PC5 connection with the 5G ProSe Remote UE, e.g. S-NSSAI, DNN, QoS, UP security activation status, the 5G ProSe Layer-3 UE-to-Network Relay initiates a new PDU session establishment or modification procedure for relaying.

5. Upon successful network-controlled authorization of 5G ProSe Remote UE procedure the 5G ProSe Layer-3 UE-to-Network Relay initiates a Direct Security Mode Command procedure with the 5G ProSe Remote UE to establish the security of the PC5 link. The security of the PC5 link may be established as described in 6.2.3.

6. Upon successful security establishment, the 5G ProSe Layer-3 UE-to-Network Relay stores the 5GPRUK ID as described in 6.3.3.3.2 and sends a DCA (Direct Communication Accept) message to the Remote UE. The DCA may include an indication that a PDU Session with secondary authentication is pending if the L3 UE-to-Network Relay UE determines if the DN that is associated with the relay service code requires secondary authentication for the 5G ProSe Remote UE based on the fact that the L3 UE-to-Network Relay UE performed secondary authentication with the same DN either in step 1 or step 4, and there is no stored authentication information associated with the Remote UE. Based on the indication in the DCA message, the 5G ProSe Remote UE may refrain from sending any data traffic over the PC5 link until successful completion of subsequent PDU Session secondary authentication.

7. For IP PDU Session Type and IP traffic over the PC5 reference point, the IPv6 prefix or IPv4 address is allocated for the 5G ProSe Remote UE. The 5G ProSe Layer-3 UE-to-Network Relay may configure a traffic filter (e.g., as a default filter for IP or non-IP traffic) for the PC5 link to prevent any data traffic until successful completion of subsequent PDU Session secondary authentication.

8. The 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report message to the SMF for the PDU session associated with the 5G ProSe Layer-3 UE-to-Network Relay. The message may include the 5GPRUK ID as the Remote User ID and 5G ProSe Remote UE addressing info (e.g., IP or MAC address). The Relay UE shall additionally include the 5GPRUK ID in the subsequent NAS messages. The AMF shall select AUSF based on 5GPRUK ID and forwards the 5GPRUK ID to the AUSF in Nausf\_UEAuthentication\_ProseGet Request message. The AUSF shall select PAnF based on 5GPRUK ID and forwards the 5GPRUK ID to the PAnF in Npanf\_Get Request message. The PAnF shall retrieve the Remote UE's SUPI from the Prose context based on 5GPRUK ID and send the Remote UE's SUPI to the AUSF in the PAnF in Npanf\_Get Respone message. The AUSF shall forward Remote UE's SUPI to the AMF in Nausf\_UEAuthentication\_ProseGet Response message. The Relay AMF shall forward the Remote UE Report message with the retrieved SUPI to the SMF in Nsmf\_PDUSession\_UpdateSMContext message.

NOTE 1: In the case of Home Routed roaming, the SMF in the call flow is the H-SMF (and the V-SMF is not shown for simplicity). SMF selection by AMF is performed as per TS 23.502 [13], clause 4.3.2.2.3 (e.g., using PLMN ID of the SUPI, S-NSSAI, etc.).

9. When the SMF receives Remote UE Report the SMF retrieves Remote UE's SM subscription data from the UDM by triggering Nudm\_SDM\_Get service operation. The SMF may include DNN, S-NSSAI of the PDU Session for relaying in addition to the Remote UE's SUPI as input parameters. The SMF determines based on the subscription data of the 5G ProSe Remote UE (i.e., Secondary authentication indication as per TS 23.502 [13], Table 5.2.3.3.1) and the local configuration of the SMF that the requested DN is subject to secondary authentication. The SMF may also check whether the 5G ProSe Remote UE has been authenticated by the same DN as indicated in the subscription data and, if secondary authentication is required, the SMF triggers a PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay by sending PDU Session Authentication Command message to the 5G ProSe Layer-3 UE-to-Network Relay including the 5GPRUK ID of the Remote UE and an EAP-Request/Identity.

Note 2: The information on a successful authentication between a 5G ProSe Remote UE and an SMF may be saved in SMF and/or UDM.

NOTE 3: The local configuration of the SMF is set by the operator. If it indicates that secondary authentication is not required, the SMF does not perform secondary authentication for the 5G ProSe Remote UE.

10. Based on the 5GPRUK ID, the 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP-Request/Identity to the 5G ProSe Remote UE via PC5 signalling(10a). The 5G ProSe Remote UE returns the EAP-Response/Identity to the 5G ProSe Layer-3 UE-to-Network Relay via PC5 signalling(10b).

11. The 5G ProSe Layer-3 UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including the 5GPRUK ID of the Remote UE and an EAP-Response/Identity received from the 5G ProSe Remote UE.

12. The SMF sends an EAP-Response/Identity to the DN-AAA.

13. The DN AAA server and the UE should exchange EAP messages, as required by the EAP method. The SMF and Relay shall include the 5GPRUK ID in the NAS messages transporting the EAP messages.

14. The DN-AAA sends EAP-Success or EAP-Failure to the SMF.

15. Upon successful PDU Session secondary authentication via the Relay procedure, the SMF stores the 5G ProSe Remote UE information in the 5G ProSe Layer-3 UE-to-Network Relay's SM context and/or Remote UE's UDM including 5G ProSe Remote UE identity (e.g., GPSI, SUPI), individual authorization information (e.g., QoS parameters) received from DN-AAA.

16. The SMF sends Remote UE Report Ack message to the 5G ProSe Layer-3 UE-to-Network Relay indicating the result of the PDU Session secondary authentication, including the 5GPRUK ID of the remote UE and an EAP success or failure message. In the case of successful secondary authentication, the message may include QoS authorization info for the 5G ProSe Layer-3 UE-to-Network Relay to enforce. In case the secondary authentication is failed, the NAS message may indicate that 5G ProSe Layer-3 UE-to-Network Relay should release the PC5 link with the 5G ProSe Remote UE.

17. In the case of successful secondary authentication for the 5G ProSe Remote UE, the 5G ProSe Layer-3 UE-to-Network Relay stores any received authentication info associated with the 5G ProSe Remote UE. In case the secondary authentication is failed, the 5G ProSe UE-to-Network Relay releases the PC5 link with the 5G ProSe Remote UE and may keep the PDU session as the default PDU session or release it if there is no more 5G ProSe Remote UE using the same PDU session.

**\*\*\*\*\* NEXT CHANGES \*\*\*\*\***

## 7.X. Prose Anchor Function Services

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

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

**Service operation name:** Npanf\_Get

**Description:** The NF consumer requests Remote UE's SUPI from the PAnF.

**Input, Required:** 5GPRUK ID.

**Input, Optional:** None.

**Output, Required:** Remote UE's SUPI.

**Output, Optional:** None.

### 7.3.2 Nausf\_UEAuthentication Service

#### 7.3.2.X Nausf\_UEAuthentication\_ProseGet service operation

**Service operation name:** Nausf\_UEAuthentication\_ProseGet

**Description:** Provides the 5G ProSe Remote UE's SUPI

**Input, Required:** 5GPRUK ID

**Input, Optional:** None.

**Output, Required:** 5G ProSe Remote UE's SUPI.

**Output, Optional:** None.

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