**3GPP TSG-SA3 Meeting #106e draft\_S3-220161-r8**

**e-meeting, 14 - 25 February 2022**

**Source: LG Electronics, Interdigital**

**Title: Procedure for secondary authentication without N3IWF**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***This contribution proposes a text on secondary authentication for U2N relay in ProSe TS 33.503***

# 2 References

[1] S3-220159 “Discussion on Secondary Authentication and NSSAA for Remote UE over L3 U2N relay without using N3IWF”

[2] TS 33.503 v.0.2.0 “Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS) (Release 17)”

# 3 Rationale

This contribution proposes to add a content for secondary authentication for the Remote UE via L3 UE-to-network relay without N3IWF, based on the discussion paper provided in [1].

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in [2].

**\*\*\*\*\* 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.x Remote UE Secondary Authentication via a L3 UE-Network Relay without N3IWF

###### 6.3.3.3.x.1 General

This clause specifies the secondary authentication between a Remote UE via a L3 UE-to-Network Relay UE without N3IWF and an external data network (DN) based on network-controlled authorization (i.e., using Remote UE primary authentication) as described in clause 6.3.3.3.2. This procedure is optional to support.

The SMF of Relay UE triggers the secondary authentication of the 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 Relay UE

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

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

###### 6.3.3.3.x.2 PDU Session secondary authentication of Remote UE via L3 UE-to-Network Relay UE

The PDU session secondary authentication of Remote UE via L3 UE-to-Network Relay UE follows the steps described below on the Figure 6.3.3.3.x.2-1.



Figure 6.3.3.3.X.2-1: Procedure for PDU session secondary authentication of Remote UE   
via L3 UE-to-Network Relay UE

1. During the Registration procedure, authorization and provisioning are performed for Remote UE(0a) and L3 UE-to-Network Relay UE(0b). When the Remote UE is not in the coverage, the Remote UE may use its preconfigured policy and parameter for PC5 discovery and communication to establish a PC5 connection with a L3 UE-to-Network Relay UE.

1. The L3 UE-to-Network Relay UE may establish a PDU session for relaying with default PDU session parameters received in step 0 or pre-configured in the L3 UE-to-Network Relay UE, e.g. S-NSSAI, DNN, SSC mode, or PDU Session Type.

2. Based on the authorization and provisioning in step 0, the Remote UE performs the discovery of a L3 UE-to-Network Relay UE. As part of the discovery procedure, the Remote UE learns about the connectivity service the L3 UE-to-Network Relay UE provides (e.g., based on a broadcasted service code).

3. The Remote UE selects a L3 UE-to-Network Relay UE and may determine from the configuration in step 0 that the service code is associated with a DN that requires secondary authentication. Based on this determination, the Remote UE sends a DCR (Direct Communication Request) message including its identity (e.g., SUCI).

4. On the condition that the DCR message includes a SUCI, the L3 UE-to-Network Relay UE triggers a network-controlled authorization of Remote UE, as described in 6.3.3.3.2. If the required identity parameter (e.g., SUCI) is missing, the L3 UE-to-Network Relay UE may send an identity request message to the Remote UE to obtain the Remote UE identity (e.g., SUCI) before triggering the network-controlled authorization procedure of Remote UE.

If there is no PDU session satisfying the requirements of the PC5 connection with the Remote UE, e.g. S-NSSAI, DNN, QoS, UP security activation status, the L3 UE-to-Network Relay UE initiates a new PDU session establishment or modification procedure for relaying.

5. Upon successful network-controlled authorization of Remote UE procedure the L3 UE-to-Network Relay UE initiates a Direct Security Mode Command procedure with 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 L3 UE-to-Network Relay UE sends a DCA (Direct Communication Accept) message that may include an indication that a PDU Session with secondary authentication is pending. Based on the indication in the DCA message, the 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 Remote UE. The L3 UE-to-Network Relay UE 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 L3 UE-to-Network Relay UE sends a Remote UE Report message to the SMF for the PDU session associated with the L3 UE-to-Network Relay UE. The message may include the Remote User ID and Remote UE addressing info (e.g., IP or MAC address). The SMF receives the message from AMF which includes the Remote UE's SUPI, obtained by AMF during a controlled authorization of Remote UE procedure as described in 6.3.3.3.2.

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

NOTE: 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 [b], clause 4.3.2.2.3 (e.g., using PLMN ID of the SUPI, S-NSSAI, etc.).

9. When the SMF received Remote UE Report the SMF determines based on the subscription data of the Remote UE (i.e., Secondary authentication indication as per TS 23.502 [b], 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 Remote UE has been authenticated by the same DN as indicated in the subscription data and, if negative, triggers a PDU Session secondary authentication of Remote UE via L3 UE-to-Network Relay UE by sending PDU Session Authentication Command message to the L3 UE-to-Network Relay UE including Remote User ID and an EAP-Request/Identity.

NOTE: 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 Remote UE.

10. The L3 UE-to-Network Relay UE sends an EAP message to the Remote UE via PC5 signalling(10a). The Remote UE sends an EAP-Request/Identity to the L3 UE-to-Network Relay UE via PC5 signalling(10b).

11. The L3 UE-to-Network Relay UE sends PDU Session Authentication Complete message to the SMF including Remote User ID and an EAP-Response/Identity received from the 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.

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 Remote UE information in the Relay Session Management context including Remote UE identity (e.g., GPSI), individual authorization information (e.g., QoS parameters) received from DN-AAA.

16. The SMF sends Remote UE Report Ack message to the L3 UE-to-Network Relay UE indicating the result of the PDU Session secondary authentication, including an identity of the Remote UE (e.g., GPSI, Remote User Id), an EAP success or failure message. In the case of successful secondary authentication, the message may include QoS authorization info for the L3 UE-to-Network Relay UE to enforce. In case the secondary authentication is failed, the NAS message may indicate that L3 UE-to-Network Relay UE should release the PC5 link with the Remote UE.

17. In the case of successful secondary authentication for the Remote UE, the L3 UE-to-Network Relay UE stores any received authorization info associated with the Remote UE. In case the secondary authentication is failed, the 5G ProSe UE-to-Network Relay releases the PC5 link with the Remote UE and may keep the PDU session as the default PDU session or release it if there is no more Remote UE using the same PDU session.

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

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[4] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[5] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[6] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[7] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[a] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[b] 3GPP TS 23.502: "Procedures for the 5G System".

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