**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220372-r2***

**e-meeting, 14 - 25 February 2022 merger of S3-220182, S3-220288, S3-220372**

**Source: Ericsson, Interdigital, Huawei, HiSilicon (?)**

**Title: Authentication flow over PC5 for Prose CP based solution for L3 U2N security**

**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] S3-220367 "SBA service operations and key hierarchy for Prose CP based solution for L3 U2N security"

# 3 Rationale

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

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

This contribution introduces detailed authentication flows over PC5 interface. Since NAS procedure is not performed between remote UE and relay AMF, 5G AKA cannot be supported. It is proposed that only EAP-AKA' procedure is supported.

This contribution is based on S3-220367, i.e. with new proposed SBA operations for AUSF and UDM.

# 4 Detailed proposal

It is proposed that SA3 approve the below draft CR to TS 33.503 [1].

**\*\*\*\*\* 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)".

[x] 3GPP TS33.102: "3G security; Security architecture".

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

#### 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

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.

2-5. 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 SUCI, Relay Service Code, Nonce\_1. Upon receiving the DCR message, the Relay UE shall send the relay key request to the relay AMF, including the parameters received in the DCR message. The Relay UE shall also include in the message a Temp ID that identifies the Remote UE for the subsequent messages over Relay UE's NAS messages and PC5 messages. The Relay AMF shall verify whether the relay UE is authorized to act as U2N relay. The relay AMF shall select AUSF based on SUCI and forward the key request to the AUSF in Nausf\_UEAuthentication\_ProseAuthenticate Request message.

6. 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 remote AUSF and the remote UE via the relay AMF and relay UE. Based on SUPI, the UDM shall choose the authentication method.

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

Editor's note: A new service operations should be used for Prose authentication to distinguish it from primary authentication defined in 33.501, to separate the different function and service logic. This is FFS.

7a. If EAP-AKA' is selected by UDM, the remote AUSF shall trigger authentication of the remote UE based on EAP-AKA'. The remote AUSF 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 relay AMF in a Nausf\_UEAuthentication\_ProSeAuthenticate Response message.

7b. The relay AMF shall forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the relay UE over NAS message, including the Temp ID of the remote UE in the message. The NAS message is protected using the NAS security context created for the relay UE.

7c. The relay UE shall forward the Relay Authentication Request to the Remote UE over PC5 messages, including the Temp ID in the message.

The USIM in the remote UE verifies the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102 [x].

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 remote UE shall return EAP-Response/AKA'-Challenge to the Relay UE in a NAS message Relay Authentication Response.

7e. The relay UE forwards the EAP-Response/AKA'-Challenge to the relay AMF in a NAS message Relay Authentication Response.

7f. The relay AMF forwards EAP-Response/AKA'-Challenge to the remote AUSF via Nausf\_UEAuthentication\_ProSeAuthenticate Request.

The remote AUSF performs the UE authentication by verifying the received information as described in TS33.501.

For EAP-AKA’, the remote AUSF and the remote UE may exchange EAP-Request/AKA’-Notification and EAP-Response /AKA’-Notification messages via the relay AMF. After the exchanges, the remote AUSF derives KAUSF without calculatingthe KSEAF.

The remote

8. 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.

9. The AUSF shall generate the KNR\_ProSe key as defined in Annex A.4.

10-11. The AUSF shall send the 5GPRUK ID, KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the UE-to-Network relay via relay AMF. When receiving a KNR\_ProSe from AUSF, the AMF shall not attempt to trigger NAS SMC procedure with Remote UE. Relay UE derives PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe, using the KDF defined in clause 6.3.3.3.4 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 UE-to-Network relay shall send the received 5GPRUK ID, Nonce\_2 to the Remote UE in Direct Security mode command message.

13-14. The remote UE shall use the 5GPRUK ID to locate the KAUSF/5GPRUK to be used for the PC5 link security. 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 9. 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 11. 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.

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

##### 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.

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