**3GPP TSG-SA3 Meeting #107-e *S3-221141***

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

**Source: Philips International B.V.**

**Title: Relay Discovery clarifications**

**Document for: Approval**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution proposes to clarify the security procedures for U2N relay discovery in TS 33.503.***

# 2 References

[1] 3GPP TS 33.503 v0.3.0

# 3 Rationale

The security procedures for ProSe UE-to-Network relay discovery rely on the ProSe restricted direct discovery procedures. However, the procedures, in particular the differences between the security material used for ProSe UE-to-NW relay discovery and ProSe direct discovery and how this security material is provisioned, needs to be further clarified.

# 4 Detailed proposal

It is proposed that SA3 approve the below draft CR to TS 33.503 [1] to clarify the UE-to-NW relay discovery procedures.

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

##### 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: 5G ProSe 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 by their own respective PCF (not shown in the figure) during this authorization and information provisioning procedure. The discovery security materials are provisioned as per clause 6.1.3.2.

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, following the security procedures in clauses 6.1.3.2.2.1 and 6.1.3.2.2.2.

2-5. 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 SUCI, Relay Service Code, Nonce\_1. 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 partial parameters 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. 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. 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. The Nausf\_UEAuthentication\_ProseAuthenticate Request message shall contain the 5G ProSe Remote UE’s SUCI, Relay Service Code, Nonce\_1. 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.

6. 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 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.

9. The AUSF of the 5G ProSe Remote UE shall generate the KNR\_ProSe key as defined in Annex A.4.

10-11. The AUSF of the 5G ProSe Remote UE shall send the KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the 5G ProSe UE-to-Network Relay via the AMF of the 5G ProSe UE-to-Network Relay. When receiving a KNR\_ProSe from the AUSF 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 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].

12. 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.

13-15. The 5G ProSe Remote UE shall use the 5GPRUK ID to locate the KAUSF\_P/5GPRUK to be used for the PC5 link security. 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 9. 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 11. 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. 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.

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

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

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