**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220288-r3***

**e-meeting, 14 - 25 February 2022** *merger of S3-220288, S3-220100, S3-220103, S3-220104*

**Source: Samsung, Interdigital, LG Electronics, ZTE**

**Title: Resolving EN in ProSe CP based solution**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***It is requested to approve this pCR for TS 33.503.***

# 2 References

[1] 3GPP TR 33.847 Study on security aspects of enhancement for proximity-based services in the 5G System

# 3 Rationale

This contribution is proposed to resolve the following Editor’s Note in TS 33.503:

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

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.

For the above three ENs, following exception needs to be performed in case of ProSe relay specific authentication:

* The AMF/SEAF shall invoke the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. The Nausf\_UEAuthentication\_Authenticate Request message shall contain remote UE’s SUCI, Relay Service Code, Nonce\_1, with the additional parameters included. The AUSF shall determine if the request is for a ProSe relay specific authentication based on the ProSe specific parameters received. The serving network name handling is same as defined in TS 33.501[3].
* It is proposed that the anchor key KSEAF shall not be derived from KAUSF when performing ProSe relay specific authentication (and therefore is not sent to the AMF). After the UDM is informed that the UE has been successfully authenticated for ProSe, the UDM shall not store the AUSF instance which reported the successful authentication.
* With the above exception captured, it is clear that no new key name is not necessary for KAUSF derived for ProSe. Introducing a different key name for KAUSF would lead to adding duplicated text and create unnecessary maintenance in TS 33.501.

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

Need and Usage of 5GPRUK ID:

* If the Remote UE already has a 5GPRUK derived, the message shall also contain the 5GPRUK ID to indicate that the Remote UE wants to get relay connectivity, if the Remote UE has a 5GPRUK for this relay and an attempt to connect to this relay has not been rejected due to invalid 5GPRUK ID. In such cases, no new ProSe relay specific authentication shall be initiated.

# 4 Detailed proposal

***\*\*\*\*\*Start of 1st Change\*\*\*\*\****

##### 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 the 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. The 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 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 parameters received in Relay Key Request to the AUSF in Nausf\_UEAuthentication\_ProseAuthenticate Request message. The Nausf\_UEAuthentication\_ProseAuthenticate Request message shall contain remote UE’s SUCI, Relay Service Code, Nonce\_1, with the additional parameters included. The AUSF shall determine if the request is for a ProSe Remote UE specific authentication based on the ProSe specific parameters received (i.e., RSC, etc). The serving network name handling is same as defined in TS 33.501 [3].

If the Remote UE already has a 5GPRUK derived, the Remote UE may include the 5GPRUK ID in the DCR to indicate that the Remote UE wants to get relay connectivity using an already established 5GPRUK. If the Remote UE has a 5GPRUK for this relay and an attempt to connect to this relay has not been rejected due to invalid 5GPRUK ID, no new ProSe relay specific authentication shall be initiated.

6-7. The AUSF shall retrieve the Authentication Vectors from the UDM and trigger primary authentication of the Remote UE using existing procedure as specified in TS 33.501 [3]. This authentication is performed between the AUSF and the Remote UE via the Relay AMF and the Relay UE. The AUSF and Remote UE shall derive a new KAUSF\_P (different from KAUSF). . NAS SMC procedure is not performed between the Remote UE and the Relay AMF. The AUSF shall send the EAP-Request/AKA'-Challenge message to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response message as defined in TS 33.501 [3]. The anchor key KSEAF shall not be derived from KAUSF when performing ProSe relay specific authentication (and therefore is not sent to the AMF). After the UDM is informed that the UE has been successfully authenticated for ProSe, the UDM shall not store the AUSF instance, which reported the successful authentication. If a 5G PRUK ID is provided in the Nausf\_UEAuthentication\_Authenticate Request message, then the AUSF retrieves the 5GPRUK and may skip Remote UE ProSe specific authentication. The AUSF may use the retrieved 5GPRUK in the subsequent steps.

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

8. On successful primary authentication, the AUSF and the 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. If a valid 5GPRUK is retrieved based on a received 5GPRUK ID in step 6-7 then the AUSF may use that 5GPRUK instead. The AUSF stores the newly generated 5GPRUK and 5GPRUK ID.

NOTE: The AUSF stores the 5GPRUK and 5GPRUK ID locally or uses the service of a Prose Anchor Function (PAnF). The services provided by the PAnF are: registration/storage and retrieval of 5GPRUK.

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

10-11. The AUSF shall send the KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the UE-to-Network Relay via the Relay AMF. When receiving a KNR\_ProSe from the AUSF, the Relay AMF shall not attempt to trigger NAS SMC procedure with the Remote UE. The Relay UE 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 UE-to-Network Relay shall send the received Nonce\_2 to the Remote UE in Direct Security mode command message.

13-14. The Rremote UE shall use the 5GPRUK ID to locate the KAUSF\_P or /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 in the same way as defined in step 11. The Remote UE shall send the Direct Security mode complete message to the UE-to-Network Relay.

Further communication between the Remote UE and the 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.

***\*\*\*\*\*Next Change\*\*\*\*\****

##### 6.3.3.3.3 PC5 Key Hierarchy over control plane



Figure 6.3.3.3.3-1: PC5 Key Hierarchy for 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 primary authentication, 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.

***\*\*\*\*\*End of Change\*\*\*\*\****