**3GPP TSG-SA3 Meeting #108-e *draft\_S3-222076-r1***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0025** | **rev** | **<Rev#>** | **Current version:** | **17.0.1** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on 5G ProSe Remote UE specific authentication mechanism | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2022-08-15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Only EAP-AKA’ has been agreed to be used for 5G ProSe Remote UE specific authentication. Therefore, in such scenario, the UDM can only select EAP-AKA’.  In addition, the routing indicator is needed for the 5GPRUK Id generation. Therefore, the UDM must also include this parameter when providing the AV to the AUSF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add some context about the EAP-AKA’ usage for 5G ProSe Remote UE specific authentication.  Clarify the UDM selection of EAP-AKA’ after the remote UE authorization. And will send the AV, Routing indicator and SUPI to AUSF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect definition on 5G ProSe Remote UE specific authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 6.3.3.3, 6.3.3.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* \* First change \* \* \* \*

# 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)".

[9] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[10] 3GPP TS 23.502: "Procedures for the 5G System".

[11] 3GPP TS 33.102: "3G security; Security architecture".

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

[13] 3GPP TS 23.502: "Procedures for the 5G System".

[14] IETF RFC 7542: "The Network Access Identifier".

[xx] IETF RFC 9048: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

\* \* \* \* Second change \* \* \* \*

#### 6.3.3.3 Security procedure over Control Plane

##### 6.3.3.3.1 General

This clause describes the security mechanisms for the 5G ProSe Layer-3 UE-to-Network Relay authentication, authorization and key management using the 5G ProSe Remote UE specific authentication for PC5 keys establishment. EAP-AKA’, as specified in RFC 9048 [xx] shall be used for 5G ProSe Remote UE authentication. The EAP-AKA’ implementations shall comply with the EAP-AKA’ profile specified in Annex F of of TS 33.501 [3]. Network entities AMF, AUSF and UDM are involved for key derivation and distribution of keys used for 5G ProSe 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 clause 4.2.2 of TS 23.503 [7]. PCF shall provision the authorization policy and parameters for 5G ProSe UE-to-Network Relay discovery and communication as specified in clause 5.1.4 of TS 23.304 [2].

\* \* \* \* Third change \* \* \* \*

##### 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 clause describes the procedure for establishing a PC5 link between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. The procedure includes how the 5G ProSe Remote UE is authenticated by the AUSF of the 5G ProSe Remote UE via the 5G ProSe UE-to-Network Relay and the AMF of the 5G ProSe UE-to-Network Relay during 5G ProSe PC5 establishment. This mechanism can be used when the 5G ProSe Remote UE is 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 respectively during this authorization and information provisioning procedure.

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.

2. 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 signalling security policy in the DCR message as specified in TS 33.536 [6]. The message shall also include Relay Service Code, Nonce\_1.

If the 5G ProSe Remote UE does not have a valid 5G Prose Remote User Key (5GPRUK), the 5G ProSe Remote UE shall include SUCI in the DCR to trigger 5G ProSe Remote UE specific authentication and establish a 5GPRUK.

If the 5G ProSe Remote UE already has a valid 5GPRUK for Relay Service Code, the 5G ProSe Remote UE shall include the associated 5GPRUK ID in the DCR to indicate that the 5G ProSe Remote UE wants to get relay connectivity using the 5GPRUK.

3. 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 SUCI or 5GPRUK ID, RSC and Nonce\_1 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.

4. 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.

5. The AMF of the 5G ProSe UE-to-Network Relay shall select an AUSF based on SUCI or 5GPRUK ID 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 or 5GPRUK ID, Relay Service Code, Nonce\_1. If 5GPRUK ID is received from AMF of the 5G ProSe UE‑to‑Network Relay, the AUSF of the 5G ProSe Remote UE temporarily stores Nonce\_1 and skips steps 6-9. If the 5G ProSe Remote UE's SUCI is received from AMF of the 5G ProSe UE-to-Network Relay, the AUSF of the 5G ProSe Remote UE temporarily stores Nonce\_1 and Relay Service Code and skips step 10.

6. 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 the same as defined in TS 33.501 [3].

The AUSF of the 5G ProSe Remote UE shall retrieve the Authentication Vectors and the Routing Indicator of the 5G ProSe Remote UE from the UDM via Nudm\_UEAuthentication\_GetProseAv Request message. Upon reception of the Nudm\_UEAuthentication\_GetProSeAv Request, the UDM shall invoke SIDF de-conceal SUCI to gain SUPI before UDM can process the request. The UDM checks whether the UE is authorized to use a ProSe UE-to-Network Relay service based on authorization information in UE's Subscription data. If the UE is authorized, the UDM shall use the EAP-AKA´ authentication method based on the received Nudm\_UEAuthentication\_GetProseAv Request. The UDM shall include the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´), Routing indicator and SUPI to AUSF in a Nudm\_UEAuthentication\_GetProSeAv Response message.

7a. The AUSF shall temporarily store XRES, Routing indicator and SUPI. 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 [3] 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 clause A.3 in TS 33.501 [3].

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 TS 33.501 [3].

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 and the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall derive the KAUSF\_P in the same way as KAUSF is derived in TS 33.501 [3].

8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall generate 5GPRUK as specified in clause A.2 and 5GPRUK ID.

The 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542 [14], i.e. username@realm. The username part includes the Routing Indicator from step 6 and the 5GPRUK ID\*, and the realm part includes Home Network Identifier. The 5GPRUK ID\* is specified in clause A.3.

9a. The AUSF of the 5G ProSe Remote UE shall select the PAnF (Prose Anchor Function) based on 5GPRUK ID and send the SUPI, RSC, 5GPRUK and 5GPRUK ID in Npanf\_ProseKey\_Register Request message to the PAnF.

9b. The PAnF shall store the Prose context info (i.e. SUPI, RSC, 5GPRUK, 5GPRUK ID) for the 5G ProSe Remote UE and send Npanf\_ProseKey\_Register Response message to the AUSF.

10a. The AUSF of the 5G ProSe Remote UE shall select the PAnF based on 5GPRUK ID and send received 5GPRUK ID and RSC in Npanf\_ProseKey\_get Request message.

10b. The PAnF retrieves 5GPRUK based on the 5GPRUK ID and checks whether the 5G ProSe Remote UE is authorized to use the UE-to-Network Relay service based on received RSC. If the 5G ProSe Remote UE is authorized and the retrieved 5GPRUK is valid, the PAnF sends Npanf\_ProseKey\_get Response message with 5GPRUK to the AUSF.

11. The AUSF of the 5G ProSe Remote UE shall generate Nonce\_2 and derive the KNR\_ProSe key using 5GPRUK, Nonce\_1 and Nonce\_2 as defined in clause A.4.

12. 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. EAP Success message shall be included if step 7 is performed successfully. The AUSF of the 5G ProSe Remote UE shall also include the 5GPRUK ID in the message if generated in step 8.

13. When receiving a KNR\_ProSe from the AUSF of the 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay, the 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality key Krelay-enc (if applicable) and integrity key Krelay-int from KNR**\_**ProSe, as defined in clause 6.3.3.3.3 of the present 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]. The EAP Success message and 5GPRUK ID are also sent from the AMF of the 5G ProSe UE‑to-Network Relay to UE-to-Network Relay if received from AUSF.

14. The 5G ProSe UE-to-Network Relay shall send the received Nonce\_2 and 5G ProSe Remote UE's PC5 signalling security policy to the 5G ProSe Remote UE in Direct Security mode command message, which is integrity protected using Krelay-int. EAP Success message shall be included if received from the AMF of the 5G ProSe UE-to-Network Relay.

15. 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 11. The 5G ProSe 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 13.

16. 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.

17. 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 and store the 5GPRUK ID in the security context associated to the PC5 link with the 5G ProSe Remote UE.

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

\* \* \* \* End of changes \* \* \* \*