**3GPP TSG-SA3 Meeting #108-e *draft\_S3-222074-r2***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0023** | **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:*** | Resolution of the issue of authentication mechanism selection | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Interdigital, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***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:*** | | There is an EN on choice of authentication mechanism for 5G ProSe UE to Network Relay communication. And in TS 23.304, it has defined how to determine the security mechanism for 5G ProSe UE to Network Relay communication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Detele the EN and add the choice of authentication mechanism for 5G ProSe UE to Network Relay communication.  Merger fo S3-221760. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Choice of authentication mechanism for 5G ProSe UE to Network Relay communication is missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.3.1. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

## 6.3 Security for 5G ProSe UE-to-Network Relay Communication

### 6.3.1 General

This clause describes the security requirements and the procedures that are specifically applied to 5G ProSe UE‑to‑Network Relay communication defined in TS 23.304 [2]. The security requirements for 5G ProSe Layer‑3 UE-to-Network Relay and 5G ProSe Layer-2 UE-to-Network Relay are different and are defined in clause 6.3.3 and clause 6.3.4 respectively.

There are two security mechanism options for 5G ProSe UE-to-Network Relay: security procedure over User Plane as defined in clause 6.3.3.2 and security procedure over Control Plane as defined in clause 6.3.3.3. The 5G ProSe remote UE and 5G ProSe UE-to-Network Relay can determine the security mechanism based on the Control Plane Security Indicator associated with the RSC as specified in clause 5.1.4.3.2 of TS 23.304 [2], clauses 6.3.3.2.2 and 6.3.3.3.2 of the present document.

The functionality in this clause is supported by both 5G ProSe-enabled UEs for commercial services and public safety.

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

##### 6.3.3.2.2 5G ProSe Remote UE attaching to a 5G ProSe UE-to-Network Relay



Figure 6.3.3.2.2-1: Authorization and secure PC5 link establishment procedure  
for 5G ProSe UE-to-Network Relay

The 5G ProSe Remote UE is provisioned with the discovery security materials (see clause 6.1.3.2) and Prose Remote User Key (PRUK) when it is in coverage. These security materials are associated with an expiration time, after which they become invalid. If the UE does not have valid discovery security materials, the 5G ProSe Remote UE needs to connect to the 5G PKMF and obtain fresh ones to use the 5G ProSe UE-to-Network Relay services.

NOTE 1: The procedure is described for the scenario that the 5G PKMF of the 5G ProSe Remote UE is different from the 5G PKMF of the 5G ProSe UE-to-Network Relay. If both the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay are served by a single 5G PKMF, the 5G PKMF takes the role of the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the 5G ProSe UE-to-Network Relay and the inter-5G PKMF message exchanges are not needed.

NOTE 2: Steps 0a, 0b, 1a, 1b are performed when the 5G ProSe Remote UE is in coverage.

0a. The 5G ProSe Remote UE gets the 5G PKMF address from the 5G DDNMF of its HPLMN. Alternatively, the 5G ProSe Remote UE may be provisioned with the 5G PKMF address by PCF. If the 5G ProSe Remote UE is provisioned with the 5G PKMF address, the 5G ProSe Remote UE may access the 5G PKMF directly without requesting it from the 5G DDNMF. In case that the 5G ProSe Remote UE cannot access the 5G PKMF using the provisioned 5G PKMF address, the 5G ProSe Remote UE may request the 5G PMKF address to the 5G DDNMF.

0b. The 5G ProSe Remote UE shall establish a secure connection with the 5G PKMF via PC8 reference point. Security for PC8 interface relies on Ua security if GBA specified in TS 33.220 [8] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [5] is used (see clause 5.2.5.4). The 5G PKMF of the 5G ProSe Remote UE shall check whether the 5G ProSe Remote UE is authorized to receive UE-to-Network Relay service, and if the UE is authorized, the 5G PKMF of the 5G ProSe Remote UE provides the discovery security materials to the 5G ProSe Remote UE. If the 5G ProSe Remote UE provides a list of visited networks, the 5G PKMF of the 5G ProSe Remote UE shall request the discovery security materials from the 5G PKMFs of the potential 5G ProSe UE-to-Network Relays from which the 5G ProSe Remote UE gets the relay services. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to the 5G ProSe Remote UE.

NOTE 3: The 5G PKMF may be locally configured with the UE's authorization information. Otherwise, the 5G PKMF interacts with the UDM of the UE to retrieve the UE's authorization information.

NOTE 4: The 5G ProSe Remote UE is provisioned by PCF with a list of the potential visited networks for the 5G ProSe UE-to-Network Relay service (which is identified by RSC).

0c. The 5G ProSe UE-to-Network Relay gets the 5G PKMF address from its HPLMN in the same way as described in step 0a.

0d. The 5G ProSe UE-to-Network Relay shall establish a secure connection with the 5G PKMF via PC8 reference point as in step 0b. The 5G PKMF of the 5G ProSe UE-to-Network Relay shall check whether the 5G ProSe UE-to-Network Relay is authorized to provide 5G ProSe UE-to-Network Relay service, and if the UE is authorized, the 5G PKMF of the 5G ProSe UE-to-Network Relay provides the discovery security materials to the 5G ProSe UE-to-Network Relay. The 5G PKMF of the 5G ProSe UE-to-Network Relay may include the PC5 security policies to the 5G ProSe UE-to-Network Relay.

1a. The 5G ProSe Remote UE sends a PRUK Request message to its 5G PKMF. The message indicates that the 5G ProSe Remote UE is requesting a PRUK from the 5G PKMF. If the 5G ProSe Remote UE already has a PRUK from this 5G PKMF, the message shall also contain the PRUK ID of the PRUK.

PRUK ID shall take the form of either the NAI format or the 64-bit string. If the PRUK ID is in NAI format, i.e. username@realm, the realm part shall include Home Network Identifier (i.e. HPLMN ID).

1b. The 5G PKMF checks whether the 5G ProSe Remote UE is authorized to receive UE-to-Network Relay services. This is done by using the 5G ProSe Remote UE's identity associated with the key used to establish the secure connection between the 5G ProSe Remote UE and 5G PKMF in step 0b. If the 5G ProSe Remote UE is authorized to receive the service, the 5G PKMF sends a PRUK and PRUK ID to the 5G ProSe Remote UE. If a PRUK and PRUK ID are included, the 5G ProSe Remote UE shall store these and delete any previously stored ones for this 5G PKMF.

2. The discovery procedure is performed between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay using the discovery parameters and discovery security material as described in clause 6.1.3.2.

3. The 5G ProSe Remote UE sends a Direct Communication Request (DCR) that contains the PRUK ID or a SUCI if the Remote UE does not have a valid PRUK, Relay Service Code (RSC) of the 5G ProSe UE-to-Network Relay service and KNRP freshness parameter 1 to the 5G ProSe UE-to-Network Relay. If the PRUK ID is not in NAI format, the DCR message shall include the HPLMN ID of the 5G ProSe Remote UE. The PC5 security establishment procedure between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay including security parameters and 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. Only additional parameters required for the 5G ProSe Layer-3 UE-to-Network Relay scenario are described in this clause. The privacy and integrity protection of DCR are described in clause 6.3.5.

4a. If the Control Plane Security Indicator is not provided for the RSC in the DCR message, the 5G ProSe UE-to-Network Relay sends a Key Request message that contains PRUK ID or SUCI, RSC and KNRP freshness parameter 1 to its 5G PKMF. The Key Request message shall also include the HPLMN ID of the 5G ProSe Remote UE if it is included in the DCR.

4b. On receiving the Key Request message, the 5G PKMF of the 5G ProSe UE-to-Network Relay shall check if the 5G ProSe UE-to-Network Relay is authorized to provide relay service to the 5G ProSe Remote UE based on the 5G ProSe UE-to-Network Relay's identity associated with the key used to establish the secure PC8 connection and the received RSC. If the 5G ProSe UE-to-Network Relay's authorization information is not locally available, the 5G PKMF shall request the authorization information from the UDM of the 5G ProSe UE-to-Network Relay (not shown in the figure) using Nudm\_SDM\_Get service as described in TS 23.502 [13]. If the 5G ProSe UE-to-Network Relay is authorized to provide the relay service based on ProSe Subscription data as specified in TS 23.502 [10], the 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Request with the PRUK ID or the SUCI to the 5G PKMF of the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe UE-to-Network Relay identifies the 5G PKMF address of the 5G ProSe Remote UE based on the PRUK ID or HPLMN ID or SUCI of the 5G ProSe Remote UE if it is included in the Key Request message.

4c. On receiving the Key Request message from the 5G PKMF of the 5G ProSe UE-to-Network Relay, the 5G PKMF of the 5G ProSe Remote UE shall check if the 5G ProSe Remote UE is authorized to use the relay service. The relay service authorization check shall be based on the PRUK ID and RSC included in the Key Request message or the SUPI of the Remote UE and the RSC included in the Key Request message. If a SUCI is included in the Key Request message, the 5G PKMF of the 5G ProSe Remote UE shall request the UDM of the 5G ProSe Remote UE to de-conceal the SUCI to gain the SUPI using Nudm\_UEIdentifier\_Deconceal service, and the UDM invokes SIDF to de-conceal SUCI to gain SUPI. If the 5G ProSe Remote UE's authorization information is not locally available, the 5G PKMF shall request the authorization information from the UDM of the 5G ProSe Remote UE (not shown in figure 6.3.3.2.2-1).

NOTE 5: Privacy issues need to be considered while determining whether the SUPI is to be sent to the PKMF. For a privacy control, the UDM can authorize the PKMF based on its NF type or the service provider domain.

If a new PRUK is required, the 5G PKMF shall perform the one of the following procedures (as shown in the step 4c in figure 6.3.3.2.2-1):

- If the 5G PKMF of the 5G ProSe Remote UE supports the Zpn interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF of the 5G ProSe Remote UE may request a GBA Push Info (GPI - see TS 33.223 [9]) for the 5G ProSe Remote UE from the BSF. When requesting the GPI, the 5G PKMF shall include a PRUK ID in the P-TID field. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF of the 5G ProSe Remote UE supports the SBI interface to the BSF of the 5G ProSe Remote UE, the 5G PKMF may request the GPI via SBI interface as described in TS 33.223 [9]. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF of the 5G ProSe Remote UE supports the PC4a interface to the HSS of the UE, then the 5G PKMF of 5G ProSe Remote UE may request a GBA Authentication Vector (AV) for the 5G ProSe Remote UE from the HSS. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

- If the 5G PKMF of the 5G ProSe Remote UE is co-located or integrated with BSF functionality and supports the SBI interface to the UDM/HSS of the 5G ProSe Remote UE, the 5G PKMF may request the GBA AV via SBI interface as described in TS 33.220 [8]. On receiving the AV, the 5G PKMF locally forms the GPI including a PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.

NOTE 6: GPI is supported only when GBA is used.

4d. The 5G PKMF of the 5G ProSe Remote UE shall generate KNRP freshness parameter 2 and derive KNRP using the PRUK identified by PRUK ID, RSC, KNRP freshness parameter 1 and KNRP freshness parameter 2 as specified in A.8. Then, the 5G PKMF of the 5G ProSe Remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 to the 5G PKMF of the 5G ProSe UE-to-Network Relay. This message shall include GPI if generated. The 5G PKMF of the 5G ProSe Remote UE shall also include the Remote User ID of the 5G ProSe Remote UE in the Key Response message to the 5G ProSe UE-to-Network Relay. PRUK ID is used as a 5G ProSe Remote UE ID in the present document.

4e. The 5G PKMF of the 5G ProSe UE-to-Network Relay sends the Key Response message to the 5G ProSe UE-to-Network Relay, which includes Remote User ID, KNRP, KNRP freshness parameter 2, the PC5 security policies of the relay service, the GPI if used to calculate a fresh PRUK to the UE-to-Network Relay.

5a. The 5G ProSe UE-to-Network Relay shall derive the session key (KNRP-SESS) from KNRP and then derive the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies as specified in TS 33.536 [6]. The 5G ProSe UE-to-Network Relay shall store the Remote User ID received in step 4d. The 5G ProSe UE-to-Network Relay sends a Direct Security Mode Command message to the 5G ProSe Remote UE. This message shall also include the KNRP Freshness Parameter 2 in addition to the parameters specified in TS 33.536 [6] and shall be protected as specified in TS 33.536 [6].

5b. If the 5G ProSe Remote UE receives the message containing the GPI, it processes the GPI as described in TS 33.223 [9]. The 5G ProSe Remote UE shall derive the PRUK and obtain the PRUK ID from the GPI.

The 5G ProSe Remote UE shall derive KNRP from its PRUK, RSC, KNRP Freshness Parameter 1 and the received KNRP Freshness Parameter 2 as specified in A.8. It shall then derive the session key (KNRP-SESS) and the confidentiality key (NRPEK) (if applicable) and integrity key (NRPIK) based on the PC5 security policies in the same manner as the 5G ProSe UE-to-Network Relay and process the Direct Security Mode Command. Successful verification of the Direct Security Mode Command assures the 5G ProSe Remote UE that the 5G ProSe UE-to-Network Relay is authorized to provide the relay service.

Handling of synchronization failure (for details of synchronization failures - see TS 33.102 [11]) when UE processes the authentication challenge in the GPI is performed similarly to clause 6.7.3.2.1.2 in TS 33.303 [4]. The 5G ProSe Remote UE shall send Direct Security Mode Failure message and include RAND and AUTS in the message. The 5G ProSe UE-to-Network Relay shall send the key request message to the 5G PKMF of the 5G ProSe Remote UE via the 5G PKMF of the 5G ProSe UE-to-Network Relay upon receiving the Direct Security Mode Failure message from the 5G ProSe Remote UE. The key request message shall include the HPLMN ID of the 5G ProSe Remote UE, Relay Service Code and KNRP freshness parameter 1 together with the RAND and the AUTS received from the 5G ProSe Remote UE. If the 5G PKMF of the 5G ProSe Remote UE decides to retry GBA Push procedure, the 5G PKMF of the 5G ProSe Remote UE shall request GPI as described in step 4c.

5c. The 5G ProSe Remote UE responds with a Direct Security Mode Complete message to the 5G ProSe UE‑to‑Network Relay as specified in TS 33.536 [6].

5d. On receiving the Direct Security Mode Complete message, the 5G ProSe UE-to-Network Relay shall verify the Direct Security Mode Complete message. Successful verification of the Direct Security Mode Complete message assures the 5G ProSe UE-to-Network Relay that the 5G ProSe Remote UE is authorized to get the relay service.

5e. After successful verification, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to complete the PC5 connection establishment procedure.

6. The 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay continues the rest of procedure for the relay service over the secure PC5 link such as establishing a new PDU session or modifying an existing PDU session for relaying, if needed etc.

When the 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report to the SMF as specified in TS 23.304 [2], the 5G ProSe Layer-3 UE-to-Network Relay shall include Remote User ID received in step 4d.

\* \* \* \* 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, the 5G ProSe Remote UE shall include the 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, if the Control Plane Security Indicator is provided for the RSC in 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 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 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 choose the authentication method based on SUPI.

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 [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 \* \* \* \*