**3GPP TSG-SA3 Meeting #108e *draft\_S3-221911-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0012** | **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 | **X** | Radio Access Network | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Rename 5GPRUK ID and 5GPRUK in CP based solution and rename PRUK and PRUK ID in UP based solution | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***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 are two solutions in TS 33.503 i.e. CP based solution in clause 6.3.3.3.2 and UP based solution in clause 6.3.3.2.2.  CP based solution uses the “5GPRUK” as the key and “5GPRUK ID” as the identifier of the 5GPRUK key.  The UP based solution uses “PRUK” as the key and “PRUK ID” as the identifier of the PRUK key.  This is creating some confusion in CT groups as the names of the identifiers and keys are very similar.  It is proposed to rename “5GPRUK ID” to “CP-PRUK ID” and “5GPRUK” to “CP-PRUK” in CP based solution.  It is proposed to rename “PRUK ID” to “UP-PRUK ID” and “PRUK” to “UP-PRUK” in UP based solution. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Rename “5GPRUK ID” to “CP-PRUK ID” and “5GPRUK” to “CP-PRUK”.  Rename “PRUK ID” to “UP-PRUK ID” and “PRUK” to “UP-PRUK”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification is unclear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.3, 4.2.1.2, 6.3.3.2.2, 6.3.3.2.3, 6.3.3.3.2, 6.3.3.3.3, 6.3.3.3.4, 6.3.5.1, 6.3.5.2, 6.3.5.3, 7.2.2.1, 7.3.2.1, 7.3.2.2, 7.5.1, 7.5.2.1, 7.5.2.2, 7.5.3.1, A.2, A.3, A.4, A.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\* START OF CHANGE \*\*\*\*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

5G DDNMF 5G Direct Discovery Name Management Function

5G PKMF 5G ProSe Key Management Function

CP-PRUK Control Plane ProSe Remote User Key

AF Application Function

AKMA Authentication and Key Management for Applications

AV Authentication Vector

BSF Bootstrapping Server Function

CP Control Plane

DCR Direct Communication Request

DUCK Discovery User Confidentiality Key

DUIK Discovery User Integrity Key

DUSK Discovery User Scrambling Key

GBA Generic Bootstrapping Architecture

GPI GBA Push Info

GPS Global Positioning System

MIC Message Integrity Check

NAI Network Access Identifier

NITZ Network Identity and Time Zone

NRPEK NR PC5 Encryption Key

NRPIK NR PC5 Integrity Key

NTP Network Time Protocol

ProSe Proximity-based Services

UP-PRUK User Plane Prose Remote User Key

RPAUID Restricted ProSe Application User ID

RSC Relay Service Code

SBI Service Based Interface

UP User Plane

UTC Universal Time Coordinated

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

#### 4.2.1.2 5G ProSe Key Management Function

In addition to the architectural reference model specified in TS 23.304 [2], the architectural reference model shall support the functional entity 5G ProSe Key Management Function (5G PKMF) which is the logical function handling network related actions required for the key management and the security material for discovery of a 5G ProSe UE-to-Network Relay by a 5G ProSe Remote UE, and for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay.

The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay know from which 5G ProSe Key Management Function(s) to get the needed discovery security materials for protecting discovery messages and UP-PRUK(s) for establishing a secure PC5 link between the 5G ProSe Remote UE and the UE-to-Network Relay as the address of the 5G PKMF(s) is either pre-provisioned or provided by the 5G DDNMF (or the PCF) in the HPLMN of the 5G ProSe Remote UE to the 5G ProSe Remote UE, and by the 5G DDNMF (or the PCF) in the HPLMN of the 5G ProSe UE-to-Network Relay to the 5G ProSe UE-to-Network Relay.

The 5G PKMF interacts with the 5G ProSe-enabled UE using procedures over PC8 reference point defined in clause 4.2.2. The protection for the key request/response messages are described in clause 5.2.5.

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 shall request the security materials (e.g. Knrp and Knrp freshness parameter) from the 5G PKMF of the 5G ProSe Remote UE for PC5 communication.

\*\*\*\* NEXT 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 (UP-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 UP-PRUK from the 5G PKMF. If the 5G ProSe Remote UE already has a UP-PRUK from this 5G PKMF, the message shall also contain the UP-PRUK ID of the UP-PRUK.

UP-PRUK ID shall take the form of either the NAI format or the 64-bit string. If the UP-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 UP-PRUK and UP-PRUK ID to the 5G ProSe Remote UE. If a UP-PRUK and UP-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 UP-PRUK ID or a SUCI if the Remote UE does not have a valid UP-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 UP-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. The 5G ProSe UE-to-Network Relay sends a Key Request message that contains UP-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 UP-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 UP-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 UP-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 UP-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 UP-PRUK ID in the P-TID field. On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the UP-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 UP-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 UP-PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the UP-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 UP-PRUK ID in the P-TID field. The 5G PKMF shall use Ks(\_ext)\_NAF as the UP-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 UP-PRUK identified by UP-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. UP-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 UP-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 UP-PRUK and obtain the UP-PRUK ID from the GPI.

The 5G ProSe Remote UE shall derive KNRP from its UP-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.

##### 6.3.3.2.3 PC5 Key Hierarchy over User Plane



Figure 6.3.3.2.3-1: PC5 Key Hierarchy for 5G ProSe UE-to-Network Relay security over User Plane

The different layers of keys (see figure 6.3.3.2.3-1) are the following:

- UP-PRUK: The root key of the PC5 unicast link.

- KNRP: The key is equivalent to KNRP as specified in TS 33.536 [6]. This key is derived as specified in clause A.8.

- KNRP-SESS: This key is derived as specified in TS 33.536 [6].

- NRPEK, NRPIK: These keys are derived as specified in TS 33.536 [6].

\*\*\*\* NEXT 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. 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].

##### 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 (CP-PRUK), the 5G ProSe Remote UE shall include SUCI in the DCR to trigger 5G ProSe Remote UE specific authentication and establish a CP-PRUK.

If the 5G ProSe Remote UE already has a valid CP-PRUK, the 5G ProSe Remote UE shall include the CP-PRUK ID in the DCR to indicate that the 5G ProSe Remote UE wants to get relay connectivity using the CP-PRUK.

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 CP-PRUK 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 CP-PRUK 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 CP-PRUK ID, Relay Service Code, Nonce\_1. If CP-PRUK 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 CP-PRUK as specified in clause A.2 and CP-PRUK ID.

The CP-PRUK 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 CP-PRUK ID\*, and the realm part includes Home Network Identifier. The CP-PRUK 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 CP-PRUK ID and send the SUPI, RSC, CP-PRUK and CP-PRUK ID in Npanf\_ProseKey\_Register Request message to the PAnF.

9b. The PAnF shall store the Prose context info (i.e. SUPI, RSC, CP-PRUK, CP-PRUK 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 CP-PRUK ID and send received CP-PRUK ID and RSC in Npanf\_ProseKey\_get Request message.

10b. The PAnF retrieves CP-PRUK based on the CP-PRUK 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 CP-PRUK is valid, the PAnF sends Npanf\_ProseKey\_get Response message with CP-PRUK to the AUSF.

11. The AUSF of the 5G ProSe Remote UE shall generate Nonce\_2 and derive the KNR\_ProSe key using CP-PRUK, 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 CP-PRUK 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 CP-PRUK 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 CP-PRUK 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.

##### 6.3.3.3.3 PC5 Key Hierarchy over Control Plane



Figure 6.3.3.3.3-1: PC5 Key Hierarchy for 5G ProSe 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 5G ProSe Remote UE specific authentication, only used to derive CP-PRUK.

- CP-PRUK: The root credential derived from KAUSF\_P that is the root of security of the PC5 unicast link used for 5G ProSe UE-to-Network Relay service.

- KNR\_ProSe: This is a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link.

- 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.

##### 6.3.3.3.4 5G ProSe Remote UE Secondary Authentication via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF

6.3.3.3.4.1 General

This clause specifies the 5G Prose Remote UE specific secondary authentication between a 5G ProSe Remote UE, which is different from the secondary authentication defined in TS 33.501 [3], via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF and an external Data Network (DN) based on network-controlled authorization (i.e. using 5G ProSe Remote UE specific authentication) as described in clause 6.3.3.3.2. This procedure is optional to support.

The SMF of the 5G ProSe UE-to-Network Relay triggers the secondary authentication of the 5G ProSe Remote UE based on the subscription information and the local configuration of the SMF when it receives a NAS message (e.g. Remote UE Report) from the 5G ProSe UE-to-Network Relay.

The EAP framework specified in IETF RFC 3748 [12] shall be used for authentication between the 5G ProSe Remote UE and a DN-AAA server in the external data network.

Following clause describes the procedures for initial secondary authentication of the 5G ProSe Remote UE with the external DN-AAA server.

6.3.3.3.4.2 PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay

The PDU session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay follows the steps described in figure 6.3.3.3.4.2-1.



Figure 6.3.3.3.4.2-1: Procedure for PDU session secondary authentication of 5G ProSe Remote UE   
via 5G ProSe Layer-3 UE-to-Network Relay

0. During the Registration procedure, authorization and provisioning are performed for 5G ProSe Remote UE(0a) and 5G ProSe Layer-3 UE-to-Network Relay(0b) as described in clause 5.1.4 of TS 23.304 [2].

1. The 5G ProSe Layer-3 UE-to-Network Relay may establish a PDU session for relaying with default PDU session parameters as described in clause 6.5.1.1 in TS 23.304 [2].

2. Based on the authorization and provisioning in step 0, the 5G ProSe Remote UE performs the discovery of a 5G ProSe Layer-3 UE-to-Network Relay. As part of the discovery procedure, the 5G ProSe Remote UE learns about the connectivity service the 5G ProSe Layer-3 UE-to-Network Relay provides (e.g. based on a broadcasted service code) as described in clause 6.3.1.2 or 6.3.1.3 of TS 23.304 [2].

3. The 5G ProSe Remote UE selects a 5G ProSe Layer-3 UE-to-Network Relay sends a DCR (Direct Communication Request) message including its SUCI or a CP-PRUK ID as described in clause 6.3.3.3.2.

4. The Remote UE runs CP based authentication as described in 6.3.3.3.2. In addition, the following procedure may happen in this step as described in clause 6.5.1.1 in TS 23.304 [2].

If there is no PDU session satisfying the requirements of the PC5 connection with the 5G ProSe Remote UE, e.g. S-NSSAI, DNN, QoS, UP security activation status, the 5G ProSe Layer-3 UE-to-Network Relay initiates a new PDU session establishment or modification procedure for relaying.

5. Upon successful network-controlled authentication of 5G ProSe Remote UE procedure, the 5G ProSe Layer-3 UE-to-Network Relay initiates a Direct Security Mode Command procedure with the 5G ProSe Remote UE as described in clause 6.2.3.

6. Upon successful security establishment, the 5G ProSe Layer-3 UE-to-Network Relay stores the CP-PRUK ID as described in clause 6.3.3.3.2 and sends a DCA (Direct Communication Accept) message to the Remote UE. The DCA may include an indication that a PDU Session with secondary authentication is pending if the L3 UE-to-Network Relay determines the DN that is associated with the relay service code requires secondary authentication for the 5G ProSe Remote UE based on the fact that the L3 UE-to-Network Relay performed secondary authentication with the same DN either in step 1 or step 4, and there is no stored authentication information associated with the Remote UE. Based on the indication in the DCA message, the 5G ProSe Remote UE may refrain from sending any data traffic over the PC5 link until successful completion of subsequent PDU Session secondary authentication.

7. For IP PDU Session Type and IP traffic over the PC5 reference point, the IPv6 prefix or IPv4 address is allocated for the 5G ProSe Remote UE as defined in clause 5.5.1.3 in TS 23.304 [2]. In addition, the 5G ProSe Layer-3 UE-to-Network Relay may configure a traffic filter (e.g. as a default filter for IP or non-IP traffic) for the PC5 link to prevent any data traffic until successful completion of subsequent PDU Session secondary authentication.

8. The 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report message to the SMF for the PDU session associated with the 5G ProSe Layer-3 UE-to-Network Relay. The 5G ProSe Layer-3 UE-to-Network Relay shall include the CP-PRUK ID as the Remote User ID and 5G ProSe Remote UE addressing info (e.g. IP or MAC address). The Remote UE Report message includes the 5G ProSe Remote UE info (Remote User ID, addressing info) and excludes other 5G ProSe Remote UEs info. The Relay shall additionally include the CP-PRUK ID in the subsequent NAS messages. The AMF shall select AUSF based on CP-PRUK ID and forwards the CP-PRUK ID to the AUSF in Nausf\_UEAuthentication\_ProseGet Request message. The AUSF shall select PAnF based on CP-PRUK ID and forwards the CP-PRUK ID to the PAnF in Npanf\_Get Request message. The PAnF shall retrieve the Remote UE's SUPI from the Prose context based on CP-PRUK ID and send the Remote UE's SUPI to the AUSF in the PAnF in Npanf\_Get Respone message. The AUSF shall forward Remote UE's SUPI to the AMF in Nausf\_UEAuthentication\_ProseGet Response message. The Relay AMF shall forward the received SUPI and the Remote UE Report message to the SMF in Nsmf\_PDUSession\_UpdateSMContext message.

Editor's Notes: How to support multiple Remote User IDs in Remote UE Report is FFS.

NOTE 1: In the case of Home Routed roaming, the SMF in the call flow is the H-SMF (and the V-SMF is not shown for simplicity). SMF selection by AMF is performed as per TS 23.502 [13], clause 4.3.2.2.3 (e.g. using PLMN ID of the SUPI, S-NSSAI, etc.).

9. When the SMF receives Remote UE Report the SMF retrieves Remote UE's SM subscription data from the UDM by triggering Nudm\_SDM\_Get service operation. The SMF may include DNN, S-NSSAI of the PDU Session for relaying in addition to the Remote UE's SUPI as input parameters. The SMF determines based on the subscription data of the 5G ProSe Remote UE (i.e. Secondary authentication indication as per TS 23.502 [13], Table 5.2.3.3.1). The SMF may also check whether the 5G ProSe Remote UE has been authenticated by the same DN as indicated in the subscription data and, if secondary authentication is required, the SMF triggers a PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay by sending PDU Session Authentication Command message to the 5G ProSe Layer-3 UE-to-Network Relay including the CP-PRUK ID of the Remote UE and an EAP-Request/Identity.

Editor's Notes: how SMF is notified with the 5G ProSe remote UE's subscription update is FFS.

Note 2: The information on a successful authentication between a 5G ProSe Remote UE and an SMF may be saved in SMF and/or UDM.

10. Based on the CP-PRUK ID, the 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP-Request/Identity to the 5G ProSe Remote UE via PC5 signalling(10a). The 5G ProSe Remote UE returns the EAP-Response/Identity to the 5G ProSe Layer-3 UE-to-Network Relay via PC5 signalling(10b).

11. The 5G ProSe Layer-3 UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including the CP-PRUK ID of the Remote UE and an EAP-Response/Identity received from the 5G ProSe Remote UE.

12. The SMF sends an EAP-Response/Identity to the DN-AAA.

13. The DN AAA server and the UE should exchange EAP messages, as required by the EAP method. The SMF and Relay shall include the CP-PRUK ID in the NAS messages transporting the EAP messages.

14. The DN-AAA sends EAP-Success or EAP-Failure to the SMF.

15. Upon successful PDU Session secondary authentication via the Relay procedure, the SMF stores the 5G ProSe Remote UE information in the 5G ProSe Layer-3 UE-to-Network Relay's SM context including 5G ProSe Remote UE identity (e.g. GPSI, SUPI), individual authentication information received from DN‑AAA.

16. The SMF sends Remote UE Report Ack message to the 5G ProSe Layer-3 UE-to-Network Relay indicating the result of the PDU Session secondary authentication, including the CP-PRUK ID of the remote UE and an EAP success or failure message. In the case of successful secondary authentication, the message may include QoS authorization info for the 5G ProSe Layer-3 UE-to-Network Relay to enforce. In case the secondary authentication is failed, the NAS message may indicate that 5G ProSe Layer-3 UE-to-Network Relay should release the PC5 link with the 5G ProSe Remote UE.

17. In the case of successful secondary authentication for the 5G ProSe Remote UE, the 5G ProSe Layer-3 UE-to-Network Relay stores any received authentication info associated with the 5G ProSe Remote UE. In case the secondary authentication is failed, the 5G ProSe UE-to-Network Relay releases the PC5 link with the 5G ProSe Remote UE and may keep the PDU session as the default PDU session or release it if there is no more 5G ProSe Remote UE using the same PDU session.

6.3.3.3.4.3 Re-Authentication of Remote UE via L3 UE-to-Network Relay without N3IWF

The Re-Authentication of Remote UE via L3 UE-to-Network Relay follows the steps described in Figure 6.3.3.3.4.3-1. The call flow is based on the call flow in TS 33.501 [3], Figure 11.1.3-1 with the main difference that the EAP messages for Re-authentication are exchanged between the Remote UE and DN-AAA using PC5 transport provided via the PC5 link with the UE-to-Network Relay.



Figure 6.3.3.3.4.3-1: EAP Re-Authentication of Remote UE via L3 UE-to-Network Relay  
with an external AAA server

1-2. Secondary Authentication for the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay has been established according to the procedures specified in clause 6.3.3.3.4, PDU Session secondary authentication of the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay.

Secondary Re-authentication may either be initiated by the SMF or the external DN-AAA server. If Re-authentication is initiated by the SMF, the procedure proceeds with step 4 (skipping steps 4a and 4b). If Re‑authentication is initiated by the external DN/AAA server, the procedure proceeds with the alternative steps 4a and 4b.

3. The SMF decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.

3a. The DN AAA server decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.

3b. The DN AAA shall send a Secondary Re-Authentication request to UPF, and the UPF forwards it to the SMF. The Secondary Re-authentication request contains the GPSI, and the IP/MAC address of the UE allocated to the PDU Session and the MAC address if the PDU session is of Ethernet PDU type for the 5G ProSe Remote UE. The SMF retrieves the corresponding CP-PRUK ID from the 5G ProSe Layer-3 UE-to-Network Relay's SM context using the GPSI.

Editor's Notes: How the GPSI of the remote UE is obtained by SMF is FFS.

4. The SMF may send an EAP Request/Identity message to the 5G ProSe Layer-3 UE-to-Network Relay including CP-PRUK ID of the 5G ProSe Remote UE. In case the procedure is initiated by the DN AAA, the SMF retrieves the CP-PRUK ID that is mapped with the received GPSI.

5. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP message to the 5G ProSe Remote UE via PC5 signalling.

6. The 5G ProSe Remote UE may respond with an EAP Response/Identity message to the 5G ProSe Layer-3 UE‑to‑Network Relay via PC5 signalling.

7. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP Response/Identity to SMF.

8. SMF forwards the EAP Response/Identity to the UPF, selected during initial authentication, over N4 interface. Then, the UPF shall forward the EAP Response/Identity message to the DN AAA Server. This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.

9. The DN AAA server and the 5G ProSe Remote UE shall exchange EAP messages as required by the EAP method.

10. After the completion of the authentication procedure, DN AAA server either sends EAP Success or EAP Failure message to the SMF. This completes the Re-authentication procedure at the SMF.

11. If the authentication is successful, EAP-Success and CP-PRUK ID shall be sent to the 5G ProSe Layer-3 UE‑to-Network Relay.

12. The 5G ProSe Layer-3 UE-to-Network Relay shall forward the EAP-Success to the corresponding 5G ProSe Remote UE via PC5 signalling.

13. If authentication is not successful, EAP-Failure and CP-PRUK ID shall be sent to the 5G ProSe Layer-3 UE‑to-Network Relay.

14. The 5G ProSe Layer-3 UE-to-Network Relay shall forward EAP-Failure to the corresponding 5G ProSe Remote UE via PC5 signalling and shall release the PC5 link with the 5G ProSe Remote UE.

15. The 5G ProSe Layer-3 UE-to-Network Relay shall send a Remote UE Report message indicating the 5G ProSe Remote UE is disconnected to the SMF.

16. The SMF may release the PDU session that was used for the relay service.

Editor's Notes: It is FFS whether this procedure is needed, depending on the outcome of secondary Authentication and authorization procedure.

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

### 6.3.5 Direct Communication Request in 5G ProSe UE-to-Network Relay Communication

#### 6.3.5.1 General

This clause describes the mechanism to protect the privacy of the UP-PRUK ID and RSC in Direct Communication Request (DCR) message when restricted discovery is used for the UE-to-Network Relay service. This clause also describes a mechanism to integrity protect the DCR message when DUIK is provisioned for discovery.

#### 6.3.5.2 Privacy protection of UP-PRUK ID and RSC in DCR

The 5G ProSe Remote UE encrypts the UP-PRUK ID and RSC using the code-receiving security parameters used for discovery. The 5G ProSe UE-to-Network Relay, on receiving the DCR message, decrypts the encrypted UP-PRUK ID and RSC using the code-sending security parameters used for discovery and verifies if the RSC matches with the one that it sent in the discovery message. If the RSC does not match, the 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe UE-to-Network Relay shall decrypt the encrypted UP-PRUK ID and RSC as follows:

1) If the UE is configured with Discovery User Confidentiality Key (DUCK), the DCR ciphering key KDCR is set to DUCK. If the UE is configured with Discovery User Scrambling Key (DUSK) but not DUCK, KDCR is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and Steps 2-3 are skipped.

2) Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in clause A.5.

3) XOR the first L bits of the Keystream with the RSC where L is the length of the RSC, and XOR the remaining bits of the Keystream with the UP-PRUK ID.

NOTE 1: If UP-PRUK ID is in NAI format, encryption of the UP-PRUK ID is performed on the username part of the UP-PRUK ID.

The UE-to-network relay shall decrypt the encrypted UP-PRUK ID and RSC as follows:

1) If the UE is configured with DUCK, the DCR ciphering key KDCR is set to DUCK. If the UE is configured with DUSK but not DUCK, KDCR is set to DUSK. If the UE is neither configured with DUCK nor DUSK, the DCR message is not protected, and steps 2-3 are skipped.

2) Set Keystream to DCR confidentiality keystream calculated using KDCR, UTC-based counter and RSC as described in clause A.5.

3) XOR the first L bits of Keystream with the encrypted RSC where L is the length of the encrypted RSC, and XOR the remaining bits of Keystream with the encrypted UP-PRUK ID.

NOTE 2: If UP-PRUK ID is in NAI format, decryption of the UP-PRUK ID is performed on the username part of the UP-PRUK ID.

#### 6.3.5.3 Integrity protection of DCR

The 5G ProSe Remote UE integrity protects the DCR message using the code-receiving security parameters used for discovery. The integrity protection of the DCR message is performed after the privacy protection of UP-PRUK ID and RSC.

The 5G ProSe UE-to-Network Relay, on receiving the DCR message, verifies the integrity of the received DCR message using the code-sending security parameters used for discovery. If the integrity verification of the DCR fails, the 5G ProSe UE-to-Network Relay shall abort the PC5 direct link establishment procedure.

The 5G ProSe Remote UE shall integrity protect the DCR as follows:

1. If the UE is configured with DUIK, the DCR integrity key KINT is set to DUIK. Otherwise, the DCR message is not integrity protected, and steps 2-3 are skipped.

2. Calculate Message Integrity Check (MIC) using KINT, UTC-based counter and the DCR message as described in clause A.9.

3. Set the MIC IE to the calculated MIC.

The 5G ProSe UE-to-Network Relay shall verify the integrity of the received DCR message as follows:

1. If the UE is configured with DUIK, the DCR integrity key KINT is set to DUIK. Otherwise, the DCR message is not integrity protected, and step 2 is skipped.

2. Calculate a MIC using KINT, UTC-based counter and the received DCR message as described in clause A.9 and compare the calculated MIC with the MIC included in the DCR message. If they mismatch, the integrity check fails.

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

## 7.2 5G PKMF Services

### 7.2.1 General

The 5G PKMF supports the key request from another 5G PKMF in another PLMN via the new service operation Npkmf\_PKMFKeyRequest\_ProseKey.

Table 7.2.1-1 shows the services exposed by 5G PKMF supporting 5G ProSe.

Table 7.2.1-1: 5G ProSe Services provided by 5G PKMF

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Service Operations | Operation Semantics | Example Consumer(s) |
| Npkmf\_PKMFKeyRequest | ProseKey | Request/Response | 5G PKMF |

### 7.2.2 Npkmf\_PKMFKeyRequest service

#### 7.2.2.1 Npkmf\_PKMFKeyRequest\_ProseKey service operation

**Service operation name:** Npkmf\_PKMFKeyRequest\_ProseKey.

**Description:** Provides ProSe related keying material.

**Input, Required:** Relay Service Code, KNRP freshness parameter 1:

1) In the initial Key Request: SUCI of the 5G ProSe Remote UE or UP-PRUK ID.

2) In the subsequent Key Requests for Synchronization Failure handling: RAND, AUTS.

**Input, Optional:** None.

**Output, Required:** KNRP, KNRP freshness parameter 2.

**Output, Optional:** GPI.

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

## 7.3 AUSF Services

### 7.3.1 General

The AUSF of the 5G ProSe Remote UE supports the 5G ProSe Remote UE specific authentication of a 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay and 5G ProSe UE-to-Network Relay via the new service operation Nausf\_UEAuthentication\_ProseAuthenticate for the existing Nausf\_UEAuthentication service.

Table 7.3.1-1 shows the services exposed by AUSF supporting 5G ProSe.

Table 7.3.1-1: 5G ProSe Services provided by AUSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Service Operations | Operation Semantics | Example Consumer(s) |
| Nausf\_UEAuthentication | ProseAuthenticate | Request/Response | (Relay) AMF |

### 7.3.2 Nausf\_UEAuthentication Service

#### 7.3.2.1 Nausf\_UEAuthentication\_ProseAuthenticate service operation

**Service operation name:** Nausf\_UEAuthentication\_ProseAuthenticate.

**Description:** Authenticate the 5G ProSe Remote UE and provides Prose related keying material.

**Input, Required:** One of the options below:

1) In the initial authentication request: SUCI or CP-PRUK ID of the 5G ProSe Remote UE, Relay Service Code, Nonce\_1.

2) In the subsequent authentication requests: EAP message.

**Input, Optional:** None.

**Output, Required:** EAP message, Authentication result and if success KNR\_ProSe, Nonce\_2 and CP-PRUK ID.

**Output, Optional:** None.

#### 7.3.2.2 Nausf\_UEAuthentication\_ProseGet service operation

**Service operation name:** Nausf\_UEAuthentication\_ProseGet.

**Description:** Provides the 5G ProSe Remote UE's SUPI.

**Input, Required:** CP-PRUK ID.

**Input, Optional:** None.

**Output, Required:** 5G ProSe Remote UE's SUPI.

**Output, Optional:** None.

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

## 7.5 Prose Anchor Function Services

### 7.5.1 General

The Prose Anchor Function (PAnF) supports providing storage for the Prose context info (i.e. SUPI, CP-PRUK, CP-PRUK ID, RSC) for a 5G ProSe Remote UE.

Table 7.5.1-1 shows the PAnF Service and the PAnF Service Operations.

Table 7.5.1-1: List of PAnF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation  Semantics | Example Consumer(s) |
| Npanf\_ProseKey | Npanf\_ProseKey\_Register | Request/Response | AUSF |
| Npanf\_ProseKey\_Get | Request/Response | AUSF |

### 7.5.2 Npanf\_ProseKey service

#### 7.5.2.1 Npanf\_ProseKey\_Register service operation

**Service operation name:** Npanf\_ProseKey\_Register.

**Description:** The NF consumer requests the PAnF to store the Prose context info (i.e. SUPI, CP-PRUK, CP-PRUK ID, RSC).

**Input, Required:** SUPI, CP-PRUK ID, CP-PRUK, Relay Service Code.

**Input, Optional:** None.

**Output, Required:** None.

**Output, Optional:** None.

#### 7.5.2.2 Npanf\_ProseKey\_Get service operation

**Service operation name:** Npanf\_ProseKey\_Get.

**Description:** The NF consumer requests CP-PRUK from the PAnF.

**Input, Required:** CP-PRUK ID, Relay Service Code.

**Input, Optional:** None.

**Output, Required:** CP-PRUK.

**Output, Optional:** None.

### 7.5.3 Npanf\_get service

#### 7.5.3.1 Npanf\_Get service operation

**Service operation name:** Npanf\_Get.

**Description:** The NF consumer requests Remote UE's SUPI from the PAnF.

**Input, Required:** CP-PRUK ID.

**Input, Optional:** None.

**Output, Required:** Remote UE's SUPI.

**Output, Optional:** None.

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

# A.2 CP-PRUK derivation function

When deriving a CP-PRUK from KAUSF\_P, the following parameters shall be used to form the input S to the KDF:

- FC = 0xXX;

- P0 = SUPI;

- L0 = length of SUPI;

- P1 = relay service code;

- L1 = length of relay service code.

The input key KEY is KAUSF\_P.

SUPI shall behave the same value as parameter P0 in clause A.7.0 of TS 33.501 [3].

# A.3 Derivation of CP-PRUK ID\*

When deriving the CP-PRUK ID from KAUSF\_P, the following parameters are used to form the input S to the KDF:

- FC = 0xAA (to be allocated by 3GPP);

- P0 = "PRUK-ID";

- L0 = length of "PRUK-ID";

- P1 = relay service code;

- L1 = length of relay service code;

- P2 = SUPI;

- L2 = length of SUPI.

The input key KEY is KAUSF\_P.

# A.4 KNR\_ProSe derivation function

When deriving the KNR\_ProSe from CP-PRUK key, the following parameters shall be used to form the input S to the KDF:

- FC = 0xZZ;

- P0 = Nonce\_2;

- L0 = length of Nonce\_2;

- P1 = Nonce\_1;

- L1 = length of Nonce\_1.

The input key KEY shall be CP-PRUK key.

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

# A.8 Calculation of KNRP for UE-to-Network relays

When calculating KNRP from UP-PRUK, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [5]:

- FC = 0xYY

- P0 = Relay Service Code

- L0 = length of Relay Service Code (i.e. 0x00 0x03)

- P1 = KNRP freshness parameter 1

- L1 = length of KNRP freshness parameter 1 (i.e. 0x00 0x10)

- P2 = KNRP freshness parameter 2

- L2 = length of KNRP freshness parameter 2 (i.e. 0x00 0x10)

The input key shall be the 256-bit UP-PRUK.

\*\*\*\* END OF CHANGE \*\*\*\*