**3GPP TSG-SA3 Meeting #112 S3-234331**

**Goteborg, Sweden 14 - 18 August 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **xxxx** | **rev** |  | **Current version:** | **17.4.0** |  |
|  | | | | | | | | |
| *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:*** | CR to R-18 33.503 from Living document for 5G\_ProSe\_Ph2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe\_Ph2 | | | | |  | ***Date:*** | | | 2023-08-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | Add approved content to R-18 TS 33.503 according to the Living document for 5G\_ProSe\_Ph2 (S3-234251) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add following new features in R-18 ProSe Security:   * Security for 5G ProSe UE-to-UE Relay Communication * Security for emergency service from 5G ProSe Remote UE via 5G ProSe UE-to-Network Relay | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There will be no security features in R-18 ProSe | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 1, 3.1, 4.2, 5.2.5, 6.1.3.3, 6.3.6, 6.3.7, 6.6, 7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 CHANGES\*\*\*\*\*\*\*\*\*\*\*\*

# 1 Scope

The present document specifies the security and privacy aspects of the Proximity based Services (ProSe) in the 5G System (5GS). 5G ProSe security features include: 5G ProSe Direct Discovery security, 5G ProSe Direct communication security, 5G ProSe UE-to-Network Relay security, 5G ProSe UE-to-UE Relay security and security of emergency services for 5G ProSe Remote UE via 5G ProSe UE-to-Network Relay.

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

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms given in 3GPP TS 23.304 [2] apply:

5G ProSe Direct Communication

5G ProSe Direct Discover

5G ProSe-enabled UE

5G ProSe End UE

5G ProSe Remote UE

5G ProSe UE-to-Network Relay

5G ProSe UE-to-UE Relay

Direct Network Communication

Discovery Filter

Discovery Query Filter

Discovery Response Filter

Indirect Network Communication

Mode of communication

Model A

Model B

Open ProSe Discovery

ProSe Application Code

ProSe Application ID

ProSe Application Mask

ProSe Query Code

ProSe Response Code

ProSe Restricted Code

Restricted ProSe Application User ID

Restricted ProSe Discovery

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

## 4.2 Reference points and functional entities

### 4.2.1 Functional entities

#### 4.2.1.1 General

Architectural reference model is specified in clause 4.2.1, 4.2.2, 4.2.3, 4.2.7, and 4.2.8 of TS 23.304 [2].

#### 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, for establishing a secure PC5 communication link between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay, for discovery of a 5G ProSe UE-to-UE Relay by a 5G ProSe End UE, and for establishing a secure PC5 communication link between a 5G ProSe End UE and a 5G ProSe UE-to-UE Relay.

For 5G ProSe UE-to-Network Relay discovery and communication, 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 5G ProSe 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 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.

For 5G ProSe UE-to-UE Relay discovery and communication, the 5G ProSe End UE plays the role of the 5G ProSe Remote UE, and the 5G ProSe UE-to-UE Relay plays the role of 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.

#### 4.2.1.3 Prose Anchor Function

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

The PAnF shall store the Prose context info (i.e. SUPI, RSC, CP-PRUK, CP-PRUK ID) for a 5G ProSe Remote UE and the Prose context info for a 5G Prose End UE.

The PAnF interacts with AUSF using procedures over Npc11 reference point defined in clause 4.2.2. The PAnF interacts with UDM using procedures over Npc12 reference point defined in clause 4.2.2.

### 4.2.2 Reference points

In addition to the reference points are specified in clause 4.2.5 of TS 23.304 [2], the 5G Prose architectural reference model shall support the following reference points:

**PC8:** The reference point between the UE and the 5G ProSe Key Management Function (5G PKMF). PC8 relies on 5GC user plane for transport (i.e. an "over IP" reference point). It is used to transport security material to UEs for 5G ProSe UE-to-Network Relay discovery and communication, and to transport security material to UEs for 5G ProSe UE-to-UE Relay discovery and communication.

**Npc9:** The reference point between the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the 5G ProSe UE-to-Network Relay, and between the 5G PKMF of the 5G ProSe End UE and the 5G PKMF of the 5G ProSe UE-to-UE Relay. It is used to transport security material between two 5G PKMFs.

**Npc10:** The reference point between the UDM and the 5G PKMF. It is used to de-conceal SUCI to gain SUPI, obtain a GBA Authentication Vector (AV) for a UE, or request relay service authorization information from the UDM.

**Npc11:** The reference point between the AUSF and Prose Anchor Function (PAnF). It is used to store the Prose context info for a 5G ProSe Remote UE, and to store the Prose context info for a 5G ProSe End UE.

**Npc12:** The reference point between the PAnF and UDM. It is used to check with the UDM whether the Remote UE is authorized to use the UE-to-Network Relay service, and to check with the UDM whether the End UE is authorized to use the UE-to-UE Relay service.

**Npc13:** The reference point between the SMF and PKMF. It is used to obtain the SUPI of Remote UE from PKMF.

**Npc14:** The reference point between the SMF and PAnF. It is used to obtain the SUPI of Remote UE from PAnF.

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

### 5.2.5 Security for UE - 5G PKMF interface

#### 5.2.5.1 General

The 5G ProSe-enabled UEs have interactions with the 5G PKMF over the PC8 interface in the ProSe features described in clause 4.2.2.

#### 5.2.5.2 Security requirements

The 5G PKMF for commercial services and for public safety services provides the security keys and security material affecting the 5G ProSe-related network operations to the 5G ProSe-enabled UE for discovery of a 5G ProSe UE-to-Network Relay, PC5 communication with a 5G ProSe UE-to-Network Relay, discovery of a 5G ProSe UE-to-UE Relay, and PC5 communication with a 5G ProSe UE-to-UE Relay.

The 5G ProSe-enabled UE and the 5G PKMF shall mutually authenticate each other.

The 5G System shall support that the transmission of the security keys and security material between the 5G PKMF and the 5G ProSe-enabled UE shall be integrity protected.

The 5G System shall support that the transmission of the security keys and security material between the 5G PKMF and the 5G ProSe-enabled UE shall be confidentiality protected.

The 5G System shall support that the transmission of the security keys and security material between the 5G PKMF and the 5G ProSe-enabled UE shall be protected from replays.

The 5G System shall support that the transmission of the UE identity on the PC8 interface shall be confidentiality protected.

#### 5.2.5.3 Security procedures for PC8 using GBA

For the security procedures for protecting data transfer between the UE and the 5G PKMF on the PC8 interface, the use of either TLS v1.2 or TLS v. 1.3, as described in clause 5.3.3.2 of TS 33.303 [4] applies with the following modifications:

- The ProSe function is replaced by the 5G PKMF.

- Confidentiality protection shall be enabled.

#### 5.2.5.4 Security procedures for PC8 using AKMA

Security procedures specified in clause B.1.3.2 of TS 33.535 [5] is applicable with the additional change:

- The 5G PKMF takes the role of AF.

- Confidentiality protection shall be enabled.

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

#### 6.1.3.3 5G ProSe UE-to-UE Relay Discovery

##### 6.1.3.3.1 General

This clause describes the security requirements and the procedures for 5G ProSe UE-to-UE Relay Discovery defined in TS 23.304 [2].

Two sets of discovery security materials are used for UE-to-UE Relay discovery message protection. Direct Discovery security materials are used by 5G ProSe End UEs to protect a direct discovery set that is an end-to-end data element between 5G ProSe End UEs and is not processed by the 5G ProSe UE-to-UE Relay. UE-to-UE Relay Discovery security materials are used by 5G ProSe UE-to-UE Relay and 5G ProSe End UEs to protect 5G ProSe UE-to-UE Relay Discovery messages. The 5G ProSe UE-to-UE Relay Discovery message includes the protected direct discovery set.

Provisioning of the Direct Discovery security materials reuses the security materials provisioning mechanism for Restricted 5G ProSe Direct Discovery as specified in clause 6.1.3.2.

Provisioning of the UE-to-UE Relay Discovery security materials reuses the security materials provisioning mechanism for 5G ProSe UE-to-Network Relay discovery as specified in clause 6.1.3.2.

The protection of 5G ProSe UE-to-UE Relay Discovery message and direct discovery set is configurable based on the provisioned discovery security materials.

##### 6.1.3.3.2 Security requirements for 5G ProSe UE-to-UE Relay Discovery

5G ProSe UE-to-UE Relay Discovery addresses the following security requirements:

- The 5G System shall provide a means for confidentiality protection, integrity protection and replay protection of discovery messages for UE-to-UE Relay discovery.

- The 5G System shall provide a means to mitigate trackability and linkability attacks of 5G ProSe End UEs during UE-to-UE Relay discovery procedure.

- The 5G System shall provide a means to securely provision the security materials for UE-to-UE Relay discovery.

##### 6.1.3.3.3 Security flows

###### 6.1.3.3.3.1 Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A

The security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A is described as follows.



Figure 6.1.3.3.3.1-1: Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A

NOTE 1: The protection of direct discovery set and Announcement message reuses the protection mechanism specified in clause 6.1.3.2.3 of the present document.

1a. The monitoring 5G ProSe End UE and announcing 5G ProSe End UE are provisioned with the discovery security materials associated with a 5G ProSe Direct Discovery service based on the procedure specified in clause 6.1.3.2.2 of the present document.

1b. The monitoring 5G ProSe End UE, announcing 5G ProSe End UE, and 5G ProSe UE-to-UE Relay are provisioned with discovery security materials associated with an RSC based on the procedure specified in clause 6.1.3.2.2 of the present document.

2. The announcing 5G ProSe End UE shall protect the direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3 of the present document. The 5G ProSe UE-to-UE Relay obtains the RSC and protected direct discovery set from the announcing 5G ProSe End UE in proximity (e.g., via a previous 5G ProSe UE-to-UE Relay Discovery or 5G ProSe UE-to-UE Relay Communication procedures) as specified in clause 6.3.2.4.2 of TS 23.304 [2]. When 5G ProSe UE-to-UE Relay Discovery is used to deliver the direct discovery set, the announcing 5G ProSe End UE shall include the RSC and protected direct discovery set in a discovery message that is protected using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. When 5G ProSe UE-to-UE Relay Communication is used to deliver the direct discovery set, the announcing 5G ProSe End UE shall use the secure PC5 unicast link with the 5G ProSe UE-to-UE Relay to send the RSC and protected direct discovery set. The 5G ProSe UE-to-UE Relay shall store the valid protected direct discovery set along with its validity time. A protected discovery set shall be removed once its validity time has expired. The validity time is determined from the UTC-based counter associated to the received direct discovery set that works as a timestamp.

NOTE 2: The protected direct discovery set remains valid as long as the 5G ProSe UE-to-UE Relay and Monitoring 5G ProSe End UE estimates the same UTC-based counter used by the Announcing ProSe End UE.

3. When broadcasting the Announcement message, the 5G ProSe UE-to-UE Relay shall include the list of valid protected direct discovery sets in the Announcement message and protect the Announcement message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. Then, the 5G ProSe UE-to-UE Relay sends the Announcement message.

4. On receiving the Announcement message from the 5G ProSe UE-to-UE Relay, the monitoring 5G ProSe End UE shall process the received Announcement message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. If the verification is successful, the monitoring 5G ProSe End UE shall extract the direct discovery set(s) from the Announcement message, and process the direct discovery set(s) using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3 of the present document.

###### 6.1.3.3.3.2 Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model B

The security procedure for 5G ProSe UE-to-UE Discovery with Model B is shown in Figure 6.1.3.3.3.2-1.



Figure 6.1.3.3.3.2-1: Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model B

0. The discoverer 5G ProSe End UE and discoveree 5G ProSe End UE are provisioned with the discovery security materials associated with a 5G ProSe Direct Discovery service based on the procedure defined in clause 6.1.3.2.2.2.

The discoverer 5G ProSe End UE, discoveree 5G ProSe End UE and 5G ProSe UE-to-UE Relay are provisioned with the discovery security materials associated with a RSC based on the procedures defined for UE-to-Network relay in clause 6.3.

1. The discoverer 5G ProSe End UE shall protect a direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. The direct discovery set shall include User Info ID of the discoverer 5G ProSe End UE and User Info ID of the discoveree 5G ProSe End UE. Then, the discoverer 5G ProSe End UE shall include the protected direct discovery set in the Solicitation message and protect the Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3. The solicitation message is sent to the 5G ProSe UE-to-UE Relay.

2. On receiving the 5G ProSe UE-to-UE Relay Discovery Solicitation message from the discoverer 5G ProSe End UE, the 5G ProSe UE-to-UE Relay shall process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the 5G ProSe UE-to-UE Relay shall modify the UE-to-UE Relay Discovery Solicitation message to include User Info ID of the 5G ProSe UE-to-UE Relay.

The 5G ProSe UE-to-UE Relay Discovery Solicitation message is protected using the security materials associated with the RSC as specified in clause 6.1.3.2.3.

Then, 5G ProSe UE-to-UE Relay sends the message to the discoveree 5G ProSe End UE.

3. The discoveree 5G ProSe End UE shall process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the discoveree 5G ProSe End UE shall extract the protected direct discovery set from the message and process the direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3.

The discoveree 5G ProSe End UE shall protect a direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. Then, the discoveree 5G ProSe End UE shall include the protected direct discovery set in the UE-to-UE Relay Discovery Response message and protect the UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3. The discoveree 5G ProSe End UE replies to the 5G ProSe UE-to-UE Relay with the UE-to-UE Relay Discovery Response message.

4. On receiving the UE-to-UE Relay Discovery Response message from the discoveree 5G ProSe End UE, the 5G ProSe UE-to-UE Relay shall process the received UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the 5G ProSe UE-to-UE Relay shall modify the UE-to-UE Relay Discovery Response message to include User Info ID of 5G ProSe UE-to-UE Relay.

The UE-to-UE Relay Discovery Response message is protected using the security materials associated with the RSC as specified in clause 6.1.3.2.3. Then, 5G ProSe UE-to-UE Relay sends the UE-to-UE Relay Discovery Response message to the discoverer 5G ProSe End UE.

On receiving the UE-to-UE Relay Discovery Response message, the discoverer 5G ProSe End UE shall process the UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the discoverer 5G ProSe End UE shall extract the protected direct discovery set from the UE-to-UE Relay Discovery Response message and process the direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3.

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

### 6.3.6 Security for emergency service from 5G ProSe Remote UE via 5G ProSe UE-to-Network Relay

#### 6.3.6.1 General

This clause describes the security requirements and the procedures that are specifically applied to support of emergency service via 5G ProSe Layer 2 UE‑to‑Network Relay and 5G ProSe Layer 3 UE-to-Network Relay defined in TS 23.304 [2].

When a 5G ProSe enabled UE does not have direct connection to the network for emergency service, the UE may attempt to obtain emergency service via 5G ProSe Layer-2 or Layer-3 UE-to-Network Relay. A 5G ProSe enabled UE acting as 5G ProSe UE-to-Network Relay shall have a normal registration to support for relaying emergency service. Dedicated RSC(s) are used for relaying of emergency service as specified in TS 23.304 [2].

Based on the regulatory requirements in some regions, emergency service over relay may be supported without PC5 link security. RSC(s) dedicated for emergency service needs to be provisioned in the 5G ProSe enabled UEs with capability of 5G ProSe UE-to-Network Relay and/or 5G ProSe Remote UE as specified in TS 23.304 [2] clause 5.1.4.Based on the regulation and the operator policy, there may or may not be discovery security materials provisioned for Emergency RSC.

#### 6.3.6.2 Security requirements

The 5G system shall support the establishment of PC5 communication for emergency service over UE-to-network relay with or without PC5 security.

The security requirements defined in clause 6.3.2 and clause 6.3.3.1 apply for the case PC5 link security establishment is required for relaying emergency service.

Otherwise, the following security requirements apply based on the regulatory requirements in some regions:

- For relaying emergency service without PC5 link security, protection is not required for emergency service discovery.

- For relaying emergency service without PC5 link security, the PC5 signalling security shall support NULL ciphering algorithm and NULL integrity protection algorithm.

- For relaying emergency service without PC5 link security, the PC5 user plane security shall support no integrity protection (by not inserting a MAC-I) and NULL ciphering algorithm.

NOTE: For layer 2 relaying emergency service, the user plane security shall be handled as specified in chapter 10 of TS 33.501[3].

- For relaying emergency service without PC5 link security, PEI may be used to identify the 5G ProSe Remote UE.

#### 6.3.6.3 Security for Emergency service via 5G ProSe Layer 2 UE-to-Network Relay and via 5G ProSe Layer-3 UE‑to-Network Relay

##### 6.3.6.3.1 Security procedure for supporting emergency service via 5G ProSe Layer 2 UE-to-Network Relay and via 5G ProSe Layer-3 UE‑to-Network Relay

A 5G ProSe Remote UE can establish a PC5 security link for Emergency service with a network, via both a 5G ProSe Layer 2 UE-to-Network Relay and a 5G ProSe Layer-3 UE‑to-Network Relay as specified in clause 6.3.3.

Based on the regulation, the operator policy and the UP security policies of the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay for the emergency RSC, the UP traffic may be transmitted via a PC5 link without security protection for case that relaying emergency service with PC5 link security is not required.

##### 6.3.6.3.1.1 PC5 security establishment for Emergency Service over UE-to-Network relay

Figure 6.3.6.3.1.1-1 shows the PC5 security establishment procedure for the 5G ProSe UE-to-Network Relay communication when an Emergency Relay Service Code is used. This procedure is based on the procedure in clause 6.3.3.2.2 and clause 6.3.3.3.2.

Figure 6.3.6.3.1.1-1: PC5 link security establishment for Emergency Service over UE-to-Network relay

If relaying emergency service with PC5 link security is not required for a 5G ProSe Remote UE has no USIM based on the regulation, there is no discovery security materials (and UP-PRUK in case of UP based security procedure) provisioned for an Emergency RSC.

0. The 5G ProSe UE retrieves discovery material with the procedures as specified in clause 6.1.3.2. For UP based security procedure, the 5G ProSe Remote UE retrieves UP-PRUK as specified in step 1 of clause 6.3.3.2.2.

If the 5G ProSe Remote UE has no USIM, this step is skipped. The discovery security materials, if exist, and the Emergency RSC are locally configured in the 5G ProSe UE.

1. The discovery procedure for the Emergency RSC is performed between a 5G ProSe Remote UE, and the 5G ProSe UE-to-Network Relay, using the discovery parameters and discovery security material that are obtained in step 0.

If no discovery security material is provisioned or locally configured, the announcement and discovery of Emergency RSC may be performed without security protection if the regulation allow.

2. If the 5G ProSe Remote UE has a USIM, the 5G ProSe Remote UE sends a Direct Communication Request (DCR) to trigger PC5 security establishment for Emergency RSC using UP based security procedure as specified in step 3 to 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2.

If the 5G ProSe Remote UE has no USIM, then the 5G ProSe Remote UE sends a Direct Communication Request that contains PEI and Emergency RSC to the 5G ProSe UE-to-Network Relay. The Direct Communication Request message including PEI and Emergency RSC may be sent without protection if no discovery security material is provisioned or locally configured in the 5G ProSe Remote UE.

If UP/CP-PRUK ID or SUCI is received from the 5G ProSe Remote UE, the 5G ProSe UE-to-Network Relay performs UP based security procedure as specified in step 3 to 4 of clause 6.3.3.2.2 or CP based security procedure as specified in step 3 to step 13 of clause 6.3.3.3.2.

If only PEI and Emergency RSC are received from the 5G ProSe Remote UE, the 5G ProSe UE-to-Network Relay skips step 4 of clause 6.3.3.2.2 for UP based security procedure or step 3 to step 13 of clause 6.3.3.3.2 for CP based security procedure if the regulation and the operator policy allow. The 5G ProSe UE-to-network relay shall store the PEI.

3a. If step 2 was successfully performed, then the 5G ProSe UE-to-Network Relay shall proceed with the Direct Security Mode procedure as specified in steps 5a-5d in clause 6.3.3.2.2 for UP based security procedure or step 14 to step 16 of clause 6.3.3.3.2 for CP based security procedure.

If step 2 failed or was skipped, the 5G ProSe UE-to-Network Relay shall send Direct Security Mode Command message to the 5G ProSe Remote UE indicating NULL ciphering algorithm and NULL integrity protection algorithm as chosen algorithms if the regulation and the operator policy allow.

When there has been no successful run of authentication of the 5G ProSe Remote UE, the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay independently generate the KNRPor KNR\_ProSe in an implementation defined way. All key derivations proceed as if they were based on a KNRPor KNR\_ProSe generated from a successful authentication run.

If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating NULL integrity algorithm and NULL encryption algorithm as chosen algorithms, then the 5G ProSe Remote UE shall accept NULL ciphering and NULL integrity algorithms indicated in Direct Security Mode Command message if, and only if, the 5G ProSe Remote UE has sent an Emergency RSC in step 2. The 5G ProSe Remote UE shall set the UP integrity protection as not activated for this connection.

3b. If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating non-NULL integrity and non-NULL encryption algorithm then the 5G ProSe Remote UE proceeds step 5a-5d in clause 6.3.3.2.2 for UP based security procedure or step 14- step 16 of clause 6.3.3.3.2 for CP based security procedure.

If the 5G ProSe Remote UE receives the Direct Security Mode Command message indicating NULL integrity and NULL encryption algorithm in step 3a and has accepted the message, then the 5G ProSe Remote UE shall send an Direct Security Mode Complete message and shall include the UP integrity protection policy as NOT NEEDED in the Direct Security Mode Complete message.

If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message with no protection, the 5G ProSe UE-to-Network Relay shall only accept the message if 5G ProSe UE-to-Network Relay sent Direct Security Mode Command message including NULL integrity and NULL encryption algorithm in step 3a and if the 5G ProSe Remote UE has sent an Emergency RSC in step 3.

4a. If steps 2 failed or was skipped and PEI is not received from Direct Communication Request, the 5G ProSe UE-to-Network Relay sends a Remote Identity Request message to the 5G ProSe Remote UE to retrieve the PEI based on the regulation and the operator policy.

4b. When the 5G ProSe Remote UE receives a Remote Identity Request message from the 5G ProSe Remote UE, then the 5G ProSe Remote UE sends a Remote Identity Response message including its PEI to the 5G ProSe UE-to-network relay. The 5G ProSe UE-to-network relay shall store the PEI.

5. If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message in step 3b, and after successful verification, the 5G ProSe UE-to-Network Relay responds with a protected Direct Communication Accept message to the 5G ProSe Remote UE to complete the PC5 connection establishment procedure.

If the 5G ProSe UE-to-network relay receives the Direct Security Mode Complete message with no protection, and the 5G ProSe UE-to-Network Relay has accepted the message based on the conditions described in step 3b, the 5G ProSe UE-to-Network Relay shall send Direct Communication Accept message with not protection to the 5G ProSe Remote UE.

The 5G ProSe UE-to-Network Relay includes the configuration of UP integrity and confidentiality protection based on the agreed UP security policy in the Direct Communication Accept message as specified in TS 33.536[9].

6. The 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay continues the rest of procedure for the emergency service over relay as specified in TS 23.304 [2]. The 5G ProSe UE-to-Network Relay sends a Remote UE Report to the SMF for the Emergency RSC, the 5G ProSe UE-to-Network Relay includes Remote User ID i.e. (UP-/CP-) PRUK ID if UP or CP based security procedure is successfully performed. Otherwise, the 5G ProSe UE-to-Network Relay includes the PEI of the 5G ProSe Remote UE in the Remote UE Report.

If UP confidentiality protection is not activated for this connection, the UP confidentiality protection algorithm is the same as the selected signalling confidentiality algorithm as specified in TS 33.536[9].

If UP integrity protection is not activated for this connection, the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay do not put MAC-I into PDCP packet.

UP protection for the layer 2 relaying emergency service shall be handled as specified in chapter 10 of TS 33.501[3].

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

### 6.3.7 Security mechanism selection in path switching between two 5G ProSe UE-to-Network Relays

Based on the UE-to-Network relay reselection mechanism as per clause 5.15 of TS 23.304 [2], the Remote UE performs the path switching between two UE-to-Network Relays with the following additional security considerations:

- The Remote UE first selects the RSC indicating the same security mechanism with the original path (i.e. User Plane based solution as specified in clause 6.3.3.2 or Control Plane based solution as specified in clause 6.3.3.3.2) to establish the PC5 security link with the new UE-to-Network Relay.

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

## 6.6 Security for 5G ProSe UE-to-UE Relay Communication

### 6.6.1 General

Editor’s Note: This clause describes the general description of the security for 5G ProSe UE-to-UE Relay Communication.

### 6.6.2 Security requirements

The following security requirements apply to both 5G ProSe Layer-3 UE-to-UE Relay and 5G ProSe Layer-2 UE-to-UE Relay:

- The 5G System shall support the authorization of the UE as a 5G ProSe UE-to-UE Relay in the 5G ProSe UE-to-UE Relay scenario.

- The 5G System shall support the authorization of the UE as a 5G ProSe End UEs in the 5G ProSe UE‑to‑UE Relay scenario.

- The 5G System shall support confidentiality protection, integrity protection, and replay protection for secure communication between the 5G ProSe End UEs via 5G ProSe UE-to-UE Relays.

- The 5G System shall provide means for mitigating trackability and linkability attacks on peer 5G ProSe End UEs during communications over a UE-to-UE Relay.

- The PCF shall be able to provision the PC5 security policies to the 5G ProSe End UEs and the 5G ProSe UE-to-UE Relay per Relay Service Code during service authorization and information provisioning procedure as defined in TS 23.304 [2].

- The 5G Prose End UEs shall support to establish a secure PC5 link with the 5G Prose UE-to-UE Relay, with or without the network assistance.

- The 5G ProSe End UEs shall establish a different PC5 security context with each different 5G ProSe UE-to-UE Relay and for each different Relay Service Code.

- The 5G system shall support a means to protect security (i.e., the integrity, confidentiality, and replay protection) of user-plane and control-plane messages, including during 5G ProSe UE-to-UE Relay path switch.

### 6.6.3 Security for 5G ProSe Communication via 5G ProSe Layer-3 UE-to-UE Relay

#### 6.6.3.1 Security of 5G ProSe PC5 Communication for 5G ProSe Layer-3 UE-to-UE Relay with network assistance

The User Plane (UP) based procedures as specified in clause 6.3.3.2 and the Control Plane (CP) based procedures as specified in clause 6.3.3.3 are used to provide authentication, authorisation and security establishment between the 5G ProSe Layer-3 UE-to-UE Relay and Source End UE with the following modification:

- The Remote UE is replaced by the Source End UE.

- The UE-to-Network Relay is replaced by the UE-to-UE Relay.

The User Plane (UP) based procedures as specified in clause 6.3.3.2 and the Control Plane (CP) based procedures as specified in clause 6.3.3.3 are used to provide authentication, authorisation and security establishment between the 5G ProSe Layer-3 UE-to-UE Relay and the Target End UE with the following modification:

- The Remote UE is replaced by the Target End UE.

- The UE-to-Network Relay is replaced by the UE-to-UE Relay.

- The procedure is initiated after security establishment between the 5G ProSe Layer-3 UE-to-UE Relay and the Source End UE is successfully completed, as specified in clause 6.7 of TS 23.304 [8].

- The steps 4-5d in clause 6.3.3.2.2 and the steps 3-16 in clause 6.3.3.3.2 are not triggered by the Direct Communication Request (DCR) message sent by the UE-to-UE Relay. Upon receiving the DCR message from the UE-to-UE Relay which includes an RSC and if the Network Assistance Security Indicator associated with the RSC indicates the security procedures with network assistance are required which triggers the second hop PC5 link security establishment, the Target End UE shall inform the UE-to-UE Relay to initiate the above steps with the message pair Direct Communication Security Request and Direct Communication Security Accept. The Direct Communication Security Request message shall include the SUCI or UP-/CP-PRUK ID of Target End UE, Relay Service Code and freshness\_parameter\_1. Upon receiving the Direct Communication Security Request message, the UE-to-UE Relay needs to make sure it is inside network coverage prior to initiating the security procedures.

- The Direct Communication Request sent by UE-to-UE relay to target End UE does not include a PRUK-ID, and thus, the security mechanism in clause 6.3.5 is modified to only protect the RSC by modifying Annex A.7 to generate a keystream of the length of the RSC.

* The Direct Communication Security Request message is protected by reusing the protection method defined in clause 6.3.5.

Figure 6.6.3.1-1 shows the high level flow for the second hop PC5 link security between the 5G ProSe Layer-3 UE-to-UE Relay and the Target End UE.



Figure 6.6.3.1-1: PC5 security establishment procedure between 5G ProSe UE-to-UE Relay and the Target 5G ProSe End UE

#### 6.6.3.2 Security of 5G ProSe PC5 Communication for 5G ProSe Layer-3 UE-to-UE Relay without network assistance

The security procedure in clause 6.2 is used to establish a secure PC5 link between the End UE and the 5G ProSe Layer-3 UE-to-UE Relay without network assistance with the following modifications.

- The RSC is included in the DCR message.

- The Direct Communication Accept message is sent to the Source End UE after security establishment between the 5G ProSe Layer-3 UE-to-UE Relay and the Target End UE is successfully completed.

#### 6.6.3.3 Selection between mechanisms with or without network assistance

A Network Assistance Security Indicator per RSC is provisioned in the 5G ProSe End UEs and 5G ProSe UE-to-UE Relay to indicate which mechanism is to be used between the security procedures with the network assistance and the security procedures without network assistance. The 5G ProSe End UEs shall select the mechanism between security procedures with network assistance and security procedures without network assistance based on the Network Assistance Security Indicator, while the 5G ProSe UE-to-UE Relay shall select the mechanism between security procedures with network assistance and security procedures without network assistance based on the Network Assistance Security Indicator and its 3GPP coverage status.

For 5G ProSe UE-to-UE Relay Communication with model A discovery, the 5G ProSe UE-to-UE Relay may select both RSCs associated with the security procedures with network assistance and the security procedures without network assistance when the 5G ProSe UE-to-UE Relay is in 3GPP coverage. The 5G ProSe UE-to-UE Relay shall only select the RSC associated with the security procedures without network assistance when the 5G ProSe UE-to-UE Relay is out of 3GPP coverage. Then, the 5G ProSe UE-to-UE Relay broadcasts a Discovery Announcement message including the selected RSC. The End UE shall use the security procedures with network assistance if the Network Assistance Security Indicator associated with an RSC indicates the security procedures with network assistance (as described in clause 6.6.3.1). Otherwise, if the Network Assistance Security Indicator associated with an RSC indicates the security procedures without network assistance, the End UE shall use the security procedures without network assistance (as described in clause 6.6.3.2).

For 5G ProSe UE-to-UE Relay Communication with model B discovery, the source End UE may select both RSCs associated with the security procedures with network assistance and the security procedures without network assistance, based on the desired mechanism. Then, the source End UE broadcasts a Discovery Solicitation message including the selected RSC. The UE-to-UE Relay shall use the security procedures with network assistance if the Network Assistance Security Indicator associated with the RSC indicates the security procedures with network assistance and it is inside 3GPP coverage. Otherwise, if the Network Assistance Security Indicator associated with the RSC indicates the security procedures without network assistance, the UE-to-UE Relay shall use the security procedures without network assistance.

#### 6.6.3.4 Identity privacy for communication for 5G ProSe Layer-3 UE-to-UE Relay

The privacy protection procedure in clause 6.2.4 of the present document is used for the privacy protection of the communication between the 5G ProSe End UE and the 5G ProSe Layer-3 UE-to-UE Relay, in addition to the link identifier update procedure in clause 6.7.1.2 of TS 23.304 [2].

### 6.6.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-UE Relay

#### 6.6.4.1 General

The security procedure in clause 6.6.3 is used to establish a secure PC5 signalling between the End UE and the 5G ProSe Layer-2 UE-to-UE Relay.

The security procedure in clause 6.2 is used to establish End-to-End security link between the End UEs via the 5G ProSe Layer-2 UE-to-UE Relay

#### 6.6.4.2 Identity privacy for communication for 5G ProSe Layer-2 UE-to-UE Relay

The privacy protection procedure in clause 6.2.4 of the present document is used for the privacy protection of the End-to-End communication between the 5G ProSe End UEs via a 5G ProSe Layer-2 UE-to-UE Relay and the communication between the 5G ProSe End UE and the 5G ProSe Layer-2 UE-to-UE Relay.

During the negotiated 5G ProSe Layer-2 UE-to-UE Relay reselection defined in clause 6.7.4.2 of TS 23.304 [2], a new KNRP ID is agreed between the 5G ProSe End UEs via a first 5G ProSe Layer-2 UE-to-UE Relay as specified in clause 5.3.3.2.2.2 of TS 33.536 [9] with the following modification:

- A new KNRP ID is agreed using a Layer-2 Link Modification procedure via the first 5G ProSe Layer-2 UE-to-UE Relay instead of Layer-2 link release procedure. The 5G ProSe End UEs use the new KNRP ID to establish a connection via the second 5G ProSe Layer-2 UE-to-UE Relay.

### 6.6.5 Security for 5G ProSe UE-to-UE Relay Communication with integrated Discovery

Editor’s Note: This clause describes the security procedure for 5G ProSe UE-to-UE Relay Communication with integrated Discovery.

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

# 7 5G ProSe services

## 7.1 General

This clause provides the present document of the SBA services defined for 5G ProSe.

## 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. The 5G PKMF also provides Remote User ID of a 5G ProSe Remote UE to be used in Remote UE Report and supports resolving Remote User ID to SUPI.

For the ProSe UE-to-UE Relay discovery and communication, the 5G ProSe End UE plays the role of the 5G ProSe Remote UE, and the 5G ProSe UE-to-UE Relay plays the role of the 5G ProSe UE-to-Network Relay.

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 |
| Npkmf\_ResolveRemoteUserId | Npkmf\_ResolveRemoteUserId\_Get | Request/Response | SMF, 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.

### 7.2.3 Npkmf\_ResolveRemoteUserId service

#### 7.2.3.1 Npkmf\_ResolveRemoteUserId\_Get service operation

**Service operation name:** Npkmf\_ResolveRemoteUserId\_Get

**Description:** The NF consumer requests the PKMF to resolve the Remote User ID.

**Input, Required:** Remote User ID (UP-PRUK ID).

**Input, Optional:** HPLMN ID.

**Output, Required:** SUPI.

**Output, Optional:** None.

## 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.

For the 5G ProSe UE-to-UE Relay discovery and communication, the 5G ProSe End UE plays the role of the 5G ProSe Remote UE, and the 5G ProSe UE-to-UE Relay plays the role of the 5G ProSe UE-to-Network Relay.

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, UE-to-Network Relay’s serving network name.

2) In the subsequent authentication requests: EAP message.

**Input, Optional:** None.

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

1) EAP message,

2) Authentication result and if success KNR\_ProSe, Nonce\_2 and CP-PRUK ID.

**Output, Optional:** None.

#### 7.3.2.2 Void

## 7.4 UDM Services

### 7.4.1 General

A UDM supports providing the authentication vector for 5G ProSe Remote UE specific authentication and for 5G ProSe End UE specific authentication via the new service operation Nudm\_UEAuthentication\_GetProseAv service operation of the existing Nudm\_UEAuthentication service.

Table 7.4.1-1 shows the services exposed by UDM supporting 5G ProSe.

Table 7.4.1-1: 5G ProSe Services provided by UDM

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Service Operations | Operation Semantics | Example Consumer(s) |
| Nudm\_UEAuthentication | GetProseAv | Request/Response | AUSF |
| Nudm\_UEIdentifier | Deconceal | Request/Resonse | PKMF |

### 7.4.2 Nudm\_UEAuthentication Service

#### 7.4.2.1 Nudm\_UEAuthentication\_GetProseAv service operation

**Service operation name:** Nudm\_UEAuthentication\_GetProseAv.

**Description:** Requester NF gets the authentication data for ProSe from UDM.

**Inputs, Required:** SUCI, Relay Service Code, Serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS).

**Outputs, Required:** Authentication Vector for Prose, SUPI.

**Outputs, Optional:** None.

### 7.4.3 Nudm\_UEIdentifier Service

#### 7.4.3.1 Nudm\_UEIdentifier\_Deconceal service operation

**Service operation name:** Nudm\_UEIdentifier\_Deconceal.

**Description:** Requester NF gets the SUPI from the UDM.

**Inputs, Required:** SUCI.

**Inputs, Optional:** None.

**Outputs, Required:** SUPI.

**Outputs, Optional:** None.

## 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 and the Prose context info for a 5G ProSe End UE. The PAnF also provides Remote User ID of a 5G ProSe Remote UE to be used in Remote UE Report and supports resolving Remote User ID to SUPI.

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 |
| Npanf\_ResolveRemoteUserId | Npanf\_ResolveRemoteUserId\_Get | Request/Response | SMF |

### 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 Void

### 7.5.4 Npanf\_ResolveRemoteUserId service

#### 7.5.4.1 Npanf\_ResolveRemoteUserId\_Get service operation

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

**Description:** The NF consumer requests the PAnF to resolve the Remote User ID.

**Input, Required:** Remote User ID (CP-PRUK ID).

**Input, Optional:** None.

**Output, Required:** SUPI.

**Output, Optional:** None.

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