**3GPP TSG-SA3 Meeting #120 S3-251039**

Athens, Greece, 17 - 21 February 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for 5G\_ProSe\_Sec\_Ph3 skeleton | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, China Telecom, Qualcomm Incorporated, Xiaomi Technology Spain S.L, InterDigital | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe\_Sec\_Ph3 | | | | |  | ***Date:*** | | | 2025-02-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | To initiate the normative work for 5G\_ProSe\_Sec\_Ph3, this document proposes a skeleton to contain the multi-hop relay scenarios based on the conlcusion of TR 33.743.  This draft CR includes the documents to spcify the Multi-hop UE-to-Network Relay and Multi-hop UE-to-UE relay scenarios, namely S3-251040, S3-25104, S3-251042, S3-251043, S3-251044, S3-251045, S3-251046, S3-251047 and , S3-251080. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Skeleton for the security normative work of 5G\_ProSe\_Sec\_Ph3 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Lack of the skeleton and potential tedious discussion of skeleton using other contributions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 1, 3.1, 4.2.1.2, 4.2.1.3, 4.2.2, 5.2.5.2, 6.1.1, 6.1.3.2.3, 6.1.3.X (new), 6.1.3.Y (new), 6.3.1, 6.3.Z (new), 6.6.XX (new), 7.2.1, 7.3.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* \* 1st change \* \* \* \*

# 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.

The 5G ProSe UE-to-Network Relay security includes the security aspects for single-hop and multi-hop scenarios for both Layer-2 and Layer-3 5G ProSe UE-to-Network Relay. The 5G ProSe UE-to-UE Relay security includes the security aspect of single-hop secenario for both Layer-2 and Layer-3 5G ProSe UE-to-UE Relay, and security aspect of Layer-3 multi-hop 5G ProSe UE-to-UE Relay scenario.

\* \* \* \* 2nd 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 Intermediate 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

\* \* \* \* 3rd 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 in following scenario:

- 5G ProSe UE-to-Network Relay:

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;

- 5G ProSe Multi-hop UE-to-Network Relay:

for discovery of a 5G ProSe UE-to-Network Relay by an Intermediate UE-to-Network Relay;

for discovery of an Intermediate UE-to-Network Relay by a 5G ProSe Remote UE;

for discovery of an Intermediate UE-to-Network Relay by an Intermediate UE-to-Network Relay (if there are multiply Intermediate UE-to-Network Relays);

for establishing secure PC5 communications links between a 5G ProSe UE-to-Network Relay and an Intermediate UE-to-Network Relay;

for establishing secure PC5 communications links between an Intermediate UE-to-Network Relay and a 5G ProSe Remote UE;

for establishing secure PC5 communications links between an Intermediate UE-to-Network Relay by a Intermediate UE-to-Network Relay (if there are multiply Intermediate UE-to-Network Relays);

- 5G ProSe UE-to-UE Relay:

for discovery of a 5G ProSe UE-to-UE Relay by a 5G ProSe End UE;

for establishing a secure PC5 communication link between a 5G ProSe End UE and a 5G ProSe UE-to-UE Relay;

- 5G ProSe Multi-hop UE-to-UE Relay:

for discovery of a 5G ProSe UE-to-UE Relay by a 5G ProSe End UE;

for establishing a secure PC5 communication link between a 5G ProSe End UE and a 5G ProSe UE-to-UE Relay;

for establishing a secure PC5 communication link between a 5G ProSe UE-to-UE Relay 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.

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

For 5G ProSe Multi-hop 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(s) 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.

\* \* \* \* 4th change \* \* \* \*

#### 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, for establishing secure PC5 communication links between a 5G ProSe Remote UE and 5G ProSe UE-to-Network Relay over one or more Intermediate UE-to-Network Relay(s) over Control Plane,for establishing a secure PC5 communication link between a 5G ProSe End UE and a 5G ProSe UE-to-UE Relay over Control Plane and for establishing a secure PC5 communication link between 5G ProSe End UEs over 5G ProSe UE-to-UE Relays 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, a 5G ProSe Intermediate UE-to-Network Relay 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.

\* \* \* \* 5th change \* \* \* \*

### 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, between the 5G PKMF of the 5G ProSe Remote UE and the 5G PKMF of the Intermediate UE-to-Network Relay, between the 5G PKMF of the Intermediate UE-to-Network Relay(s), between the 5G PKMF of theIntermediate UE-to-Network Relay and the 5G PKMF of the 5G ProSe UE-to-Network Relay, between the 5G PKMF of the 5G ProSe End UE and the 5G PKMF of the 5G ProSe UE-to-UE Relay and between the 5G PKMF of the 5G ProSe UE-to-UE Relay 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/5G ProSe Intermediate UE-to-Network Relay, 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 /5G ProSe Intermediate UE-to-Network Relay are 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.

\* \* \* \* 6th change \* \* \* \*

#### 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/5G ProSe Intermediate UE-to-Network Relay, PC5 communication with a 5G ProSe UE-to-Network Relay, discovery of a 5G ProSe UE-to-UE Relay/5G ProSe Intermediate UE-to-Network 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

\* \* \* \* 7th change \* \* \* \*

### 6.1.1 General

This clause describes the security requirements and procedures that are specifically applied to 5G ProSe Discovery defined in TS 23.304[2].

The security requirements for 5G ProSe Discovery are defined in clause 6.1.2.

The security procedures for open 5G ProSe Direct Discovery are defined in clause 6.1.3.1, the security procedures for restricted 5G ProSe Direct Discovery are defined in clause 6.1.3.2, the security procedures for 5G ProSe UE-to-UE Relay Discovery are defined in clause 6.1.3.3. The security requirements and security procedures for 5G ProSe multi-hop UE-to-Network Relay Discovery are defined in clause 6.1.3.X. The security requirements and security procedures for 5G ProSe Layer-3 multi-hop UE-to-UE Relay Discovery are defined in clause 6.1.3.Y.

\* \* \* \* 8th change \* \* \* \*

##### 6.1.3.2.3 Protection of discovery messages over PC5 interface

There are three types of security that are used to protect the restricted 5G ProSe Direct Discovery messages over the PC5 interface: integrity protection, scrambling protection, and message-specific confidentiality which are defined in clause 6.1.3.4.3 in TS 33.303 [4].

For the discovery messages that do not include HPLMN ID, the protection mechanisms specified in TS 33.303 [4] are reused with the following changes:

- Input parameters to integrity protection algorithm as specified in clause A.6 in the present document.

- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document.

- For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, the Message Type is replaced by Message Type and Message content type extensions.

- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the discovery message to be scrambled and set to Min (the length of discovery message - 16, 256).

- For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, in the above Min function the value of 16 is replaced by 24.

- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

XOR (0xFF..FF || time-hash-bitsequence) with the most significant (L + 16) bits of discovery message, where 0xFF..FF is 16 bits of length.

* For Multi-hop UE-to-Nework Relay Discovery and Multi-hop UE-to-UE Relay Discovery, the above value of 16 is replaced by 24.

NOTE 1: 16 is the size of Message Type and UTC-based counter LSB in bit length.

NOTE 1x: For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, 24 is the size of Message Type, Message content type extensions and UTC-based counter LSB in bit length.

NOTE 2: The maximum length of the discovery message to be scrambled is limited to 256 bits.

- Step 2 of clause 6.1.3.4.3.2 of TS 33.303 [4] becomes:

Calculate MIC if a DUIK was provided, otherwise set MIC to a 32-bit random string. Then, set the MIC IE to the MIC.

- Step 4 of clause 6.1.3.4.3.2 of TS 33.303 [4] is not processed.

NOTE 3: Protection for the discovery messages between the ProSe UEs is provided at the ProSe layer.

The discovery messages that include HPLMN ID are protected using the protection mechanism described above with the following changes:

- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document with the following changes:

- The input parameter LENGTH is set to LEN(discovery message) - (LEN(Message Type) + LEN(UTC-based counter LSB) + LEN(HPLMN ID) + LEN(MIC)), where LEN(x) is the length of x in number of bits.

- The KEYSTREAM is XORed with the discovery message for message-specific confidentiality protection excluding Message Type, UTC-based counter LSB, HPLMN ID and MIC.

- For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, the Message Type is replaced by Message Type and Message content type extensions.

- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the discovery message to be scrambled and set to Min (the length of discovery message – 16 – the length of HPLMN ID, 256).

- For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, in the above Min function the value of 16 is replaced by 24.

- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

XOR (0xFF..FF || time-hash-bitsequence) with the most significant (L + 16 + the length of HPLMN ID) bits of discovery message, where 0xFF..FF is (16 + the length of HPLMN ID) bits of length.

- For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, the above value of 16 is replaced by 24.

NOTE 1y: For Multi-hop UE-to-Network Relay Discovery and Multi-hop UE-to-UE Relay Discovery, 24 is the size of Message Type, Message content type extensions and UTC-based counter LSB in bit length.

In 5G ProSe UE-to-UE Relay discovery, the End UE discovery infos to be included in the direct discovery set are protected using the protection mechanism described above with the following changes:

- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document with the following changes:

- discovery message is replaced by End UE discovery info

- The length of Message Type is set to zero

- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the End UE discovery info to be scrambled and set to Min (the length of End UE discovery info - 16, 256).

- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

XOR (0xFFFF || time-hash-bitsequence) with the most significant (L + 16) bits of the End UE discovery info.

NOTE 4: 16 is the size of the length field, spare field and UTC-based counter LSB field in bit length.

\* \* \* \* 9th change \* \* \* \*

#### 6.1.3.X 5G ProSe Multi-hop UE-to-Network Relay Discovery

##### 6.1.3.X.1 General

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

##### 6.1.3.X.2 Security requirements for 5G ProSe Multi-hop UE-to-Network Relay Discovery

The following security requirements apply to 5G ProSe multi-hop UE-to-Network Relay:

- The 5G System shall support confidentiality protection, integrity protection, and replay protection of discovery messages for multi-hop UE-to-Network Relay discovery.

- The 5G System shall provide means for mitigating trackability and linkability attacks on UEs during in multi-hop UE-to-Network Relay discovery.

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

##### 6.1.3.X.3 Security flows for 5G ProSe Multi-hop UE-to-Network Relay Discovery

###### 6.1.3.X.3.1 Discovery with Model A

The security procedure for multi-hop UE-to-Network Relay discovery with Model A is shown in Figure 6. 1.3.X.3.1-1.



Figure 6.1.3.X.3.1-1: Model A Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay/5G ProSe UE-to-Network Relay is provisioned with the discovery security materials associated with an RSC from the 5G PKMF/5G DDNMF of 5G ProSe Remote UE/Intermediate UE-to-Network Relay/5G ProSe UE-to-Network Relay’s HPLMN based on the procedure specified in clause 6.1.3.2. The discovery security materials shall contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Announcement.

Editor’s Note: Discovery security materials provisioning for inter-PLMN scenario is FFS.

1. The 5G ProSe UE-to-Network Relay shall protect a Relay Discovery Announcement using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. Then, the 5G ProSe UE-to-Network Relay broadcasts the Relay Discovery Announcement.

2a. The Intermediate UE-to-Network Relay shall process the received Relay Discovery Announcement message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. If the processing is successful and Intermediate UE-to-Network Relay does not have a PC5 link with the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay shall establish a PC5 link with the 5G ProSe UE-to-Network Relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication specified in clause 6.3.3.

2b. Once the PC5 link is established between the Intermediate UE-to-Network Relay and the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay shall update the path information (e.g., hop count, Relay Info.) and protect the updated message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. The Intermediate UE-to-Network Relay broadcasts the updated message.

3. Upon receiving the Relay Discovery Announcement message from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE shall process the received message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.

###### 6.1.3.X.3.2 Discovery with Model B

The security procedure for multi-hop UE-to-Network Relay discovery with Model B is shown in Figure 6.1.3.X.3. 2-1.



Figure 6.1.3.X.3.2-1: Model B Discovery operation supporting multi-hop UE-to-Network Relay

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay/5G ProSe UE-to-Network Relay is provisioned with the discovery security materials associated with an RSC from the 5G PKMF/5G DDNMF of 5G ProSe Remote UE/Intermediate UE-to-Network Relay/5G ProSe UE-to-Network Relay’s HPLMN based on the procedure specified in clause 6.1.3.2. The discovery security materials shall contain a Discovery User Integrity Key (DUIK) for the integrity protection of Relay Discovery Solicitation and Relay Discovery Response.

Editor’s Note: Discovery security materials provisioning for inter-PLMN scenario is FFS.

1. The 5G ProSe Remote UE shall protect a Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. Then, the 5G ProSe Remote UE broadcasts the Relay Discovery Solicitation.

2. The Intermediate UE-to-Network Relay shall process the received Relay Discovery Solicitation using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. If the processing is successful, the Intermediate UE-to-Network Relay shall update the path information (e.g., hop count) and protect the updated message using the discovery security materials associated with the RSC as specified in clause 6.3. Then, the Intermediate UE-to-Network Relay broadcasts the message.

3. Upon receiving the Relay Discovery Solicitation from the Intermediate UE-to-Network Relay, the 5G ProSe UE-to-Network Relay shall process the received message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. If the processing is successful, the 5G ProSe UE-to-Network Relay shall construct a Relay Discovery Response and protect it using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.

The 5G ProSe UE-to-Network Relay replies to the Intermediate UE-to-Network Relay with the Relay Discovery Response.

4. Upon receiving the Relay Discovery Response from the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay shall process the received message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. If the processing is successful, the Intermediate UE-to-Network Relay shall update the path information (e.g., hop count) and protect the updated message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2. Then, the Intermediate UE-to-Network Relay replies to the 5G ProSe Remote UE with the message.

5. Upon receiving the Relay Discovery Response from the Intermediate UE-to-Network Relay, the 5G ProSe Remote UE shall process the received message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.

\* \* \* \* 10th change \* \* \* \*

#### 6.1.3.Y 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery

##### 6.1.3.Y.1 General

This clause describes the security requirements and the procedures for 5G ProSe Layer-3 multi-hop UE-to-UE Relay Discovery defined in TS 23.304 [2], including the Layer-3 multi-hop UE-to-UE Relay discovery for IP PDU type and non-IP PDU type.

##### 6.1.3.Y.2 Security requirements for 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery

5G ProSe Layer-3 multi-hop 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 Layer-3 multi-hop UE-to-UE Relay discovery.

- The 5G System shall provide a means to mitigate trackability and linkability attacks on UEs in Layer-3 multi-hop discovery.

- The 5G System shall provide a means to securely provision the security materials for Layer-3 multi-hop UE-to-UE Relay discovery.

##### 6.1.3.Y.3 Security flows for 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery

Two types of 5G ProSe Layer-3 Multi-hop UE-to-UE Relay discovery are supported as specified in TS 23.304 [2], i.e., discovery for IP PDU type and discovery for non-IP PDU type (i.e., Ethernet or Unstructured), depends on the RSC for the discovery. Both Model A and Model B discovery are supported by the 5G ProSe Layer-3 Multi-hop UE-to-UE discovery.

###### 6.1.3.Y.3.Y1 Security of 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery for IP PDU type

The 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of IP PDU type consists of two types of relay discovery: one for Relay discovery among 5G ProSe UE-to-UE Relays and the other one for Relay discovery between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay as specified in clause 6.3.2.6.2 of TS 23.304[2]. The discovery of the target 5G ProSe End UEs are performed via DNS queries after establishing a secure PC5 link with the 5G ProSe Multi-hop UE-to-UE Relay(s).

6.1.3.Y.3.Y1.1 Relay discovery among 5G ProSe UE-to-UE Relays

For the provisioning of discovery security materials and discovery message protection based on the discovery security materials associated with an RSC for multi-hop UE-to-UE Relay, the security procedures for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.1.3.2.2 are reused with the following change:

- One 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe Remote UE and the other 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe UE-to-Network Relay.

6.1.3.Y.3.Y1.2 Relay discovery between a 5G ProSe End UE and 5G ProSe UE-to-UE Relay

For the provisioning of discovery security materials and discovery message protection based on the discovery security materials associated with an RSC for multi-hop UE-to-UE Relay, the security procedures for 5G ProSe UE-to-Network Relay discovery with Model A and Model B as specified in clause 6.1.3.2.2 are reused with the following change:

- A 5G ProSe End UE plays the role of a 5G ProSe Remote UE and a 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe UE-to-Network Relay.

###### 6.1.3.Y.3.Y2 Security procedure for 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of non-IP PDU type

Both Model A and Model B discovery are supported by the security procedures of 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of non-IP PDU type.

For Model A discovery in 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of non-IP PDU type, the UE-to-UE Relay has discovered End UEs in proximity and obtains the Direct Discovery Set(s) from End UE(s) in proximity per RSC as specified in TS 23.304 [2] (e.g. via a previous 5G ProSe UE-to-UE Relay Discovery or via secure PC5 connection between 5G ProSe U2U Relay and 5G ProSe End UE). As per TS 23.304 [2], for each received Direct Discovery Set, the UE-to-UE Relay also gets paths information, hop count and optionally maximum number of hops. Similar to the security principle of UE-to-UE Relay discovery as specified in 6.1.3.3, the Direct Discovery Set is End-to-End protected between End UEs, while other parameters in the discovery message are hop-by-hop protected between UE-to-UE Relay and End UE:

1a. To provide End-to-End protection of the Direct Discovery Set, the existing discovery security material provisioning procedure as specified in clause 6.1.3.2.2.1 is reused to provision the discovery security materials to the End UEs. The security materials are associated with 5G ProSe Direct Discovery service for Restricted 5G ProSe Direct Discovery.

1b. To offer hop-by-hop protection of discovery messages, the existing discovery security material provisioning procedure as specified in clause 6.1.3.2.2.1 is reused to provision the discovery security materials to the End UEs and the UE-to-UE Relays. The security materials are associated RSC for the UE-to-UE Relay Discovery. The monitoring End UE plays the role of Remote UE while the UE-to-UE plays the role of UE-to-Network Relay.

2. The announcing End UE protects the Direct Discovery Set, using the security materials as specified in clause 6.1.3.2.3. The protects the Direct Discovery Set is sent to UE-to-UE Relay using either by a previous UE-to-UE Relay Discovery procedure or via secure PC5 connection between to the UE-to-UE Relay.

3. Before announcing the Announcement message, the UE-to-UE Relay prepares the message including the protected Direct Discovery Set(s), and other discovery parameters as specified in TS 23.304 [2], and protects the Announcement message using the discovery security materials in step 1b as specified in clause 6.1.3.2.3. The UE-to-UE relay needs to check the validity timer(s) associated with the protected Direct Discovery Set(s) as specified in clause 6.1.3.3.3, only valid protected Direct Discovery Set(s) are included in the Announcement message.

4. On receiving the Announcement message from the UE-to-UE Relay, the monitoring End UE uses the discovery security material received in step 1b to process the message as specified in clause 6.1.3.2.3. If the verification is successful, the monitoring End UE processs the Direct Discovery Set(s) in the message using the discovery security materials in step 1a as specified in clause 6.1.3.2.3.

Editor’s Note: The validity timer checking upon validity timer wrap around is FFS.

For Model B discovery in 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of non-IP PDU type,

- The 5G ProSe End UE and 5G ProSe UE-to-UE Relay are provisioned with the discovery security materials associated with an RSC from the 5G PKMF/5G DDNMF in their own HPLMN, reusing the procedures specified in clause 6.1.3.2.

- The 5G ProSe End UE and 5G ProSe UE-to-UE Relay use the mechanisms as specified in clause 6.1.3.3 to protect the discovery messages.

\* \* \* \* 11th change \* \* \* \*

### 6.3.1 General

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

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

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

The security requirements and security procedures for 5G ProSe Multi-hop UE-to-Network Relay is defined in clause 6.3.Z.

\* \* \* \* 12th change \* \* \* \*

### 6.3.Z Security for 5G ProSe Communication via 5G ProSe Multi-hop UE‑to-Network Relay

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

#### 6.3.Z.1 Security requirements

The following security requirements apply to 5G ProSe multi-hop UE-to-Network Relay:

- The 5G System shall support the authorization and authorisation of the UEs involving in the 5G ProSe multi-hop UE-to-Network Relay communication.

- The 5G System shall support confidentiality protection, integrity protection, and replay protection of the messages in the 5G ProSe multi-hop UE-to-Network Relay communication sceanrio.

- The 5G System shall provide means for mitigating trackability and linkability attacks on UEs involving in the 5G ProSe multi-hop UE-to-Network Relay communication.

#### 6.3.Z.2 Security procedure for 5G ProSe Multi-hop UE-to-Network Relay communication

The security procedure for 5G ProSe Multi-hop UE-to-Network Relay communication includes the PC5 security establishment procedures between Remote UE and Intermediate UE-to-Network Relay, between Intermediate UE-to-Network Relays, and between Intermediate UE-to-Network Relay and UE-to-Network Relay.

##### 6.3.Z.2.a1 Security procedure over Control Plane with multi-hop UE-to-Network Relay discovery with Model A



Figure 6.3.Z.2.a1-1: Security procedure over Control Plane for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model A is used

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.1.3.2.

1a. The UEs are discovered using multi-hop UE-to-Network Relay discovery with model A procedure, the 5G ProSe Intermediate UE-to-Network Relay receives an Announcement message from 5G ProSe UE-to-Network Relay or the upstream 5G ProSe Intermediate UE-to-Network Relay.

1b. If the Intermediate UE-to-Network Relay does not have an existing PC5 link with the UE-to-Network Relay or the upstream intermediate UE-to-Network relay when it successfully processes the Announcement message, the Intermediate UE-to-Network Relay establishes a PC5 link with the 5G ProSe UE-to-Network Relay or the upstream intermediate UE-to-Network relay using the security procedures over Control Plane as specified in clause 6.3.3.3.

1c. Once the PC5 link is established between the upstream Intermediate UE-to-Network Relay or the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network updates the Announcement message as specified in clause 6.3.2.5.2 of TS 23.304 [2], protects and sends the updated Announcement message.

2. After the multi-hop Relay discovery procedure, the Remote UE initiate a Direct Communication Request (DCR) message to request the security establishment between the intermediate relay at the next hop (denoted as the Intermediate UE-to-Network Relay-A), including the RSC, CP-PRUK ID or SUCI of the Remote UE as defined in clause 6.3.3.3.

3. The Intermediate UE-to-Network Relay-A uses the protected PC5 link established in step 1b to send the parameters in the DCR to the network. Based on the steps 3-13 of 6.3.3.3.2, the Intermediate UE-to-Network Relay-A interacts with the network, in order to get the KNR\_ProSe and freshness parameter to set up a secure connection with the Remote UE.

If Layer-3 connection is setup, the Intermediate UE-to-Network Relay-A sends/receives the Intermediate key request/response to the UE-to-Network Relay who forwards/receives the request/response over its own NAS connection to the UE-to-Network Relay’s AMF.

##### 6.3.Z.2.a2 Security procedure over Control Plane with multi-hop UE-to-Network Relay discovery with Model B



Figure 6.3.Z.2.a2-1: Security procedure over Control Plane for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model B is used

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.1.3.2.

1. The 5G ProSe Remote UE performs a multi-hop UE-to-Network Relay discovery with Model B procedure with the Intermediate UE-to-Network Relay and 5G ProSe UE-to-Network Relay.

2. After the multi-hop Relay discovery procedure, the Remote UE initiate a Direct Communication Request (DCR) message to request the security establishment between the intermediate relay at the next hop (denoted as the Intermediate UE-to-Network Relay-A), including the RSC, CP-PRUK ID or SUCI of the Remote UE as defined in clause 6.3.3.3.

3. Upon received the DCR message, the Intermediate UE-to-Network Relay-A checks whether or not has an existing PC5 link with the UE-to-Network Relay or the upstream Intermediate UE-to-Network Relay, and the upstream Intermediate UE-to-Network Relay is in-coverage.

NOTE 1: The upstream Intermediate UE-to-Network Relay is considered in-coverage if it has a connection to the network.

If PC5 link is not established with the UE-to-Network Relay or the upstream Intermediate UE-to-Network Relay, the Intermediate UE-to-Network Relay-A plays the role of the Remote UE to establish secured link with the UE-to-Network Relay or with the upstream Intermediate UE-to-Network Relay, reusing the CP-based procedure as specified in the in clauses 6.3.3.3. The DCR in this step includes the RSC, CP-PRUK ID or SUCI of the Intermediate UE-to-Network Relay-A as defined in clause 6.3.3.3.

Each of the Intermediate UE-to-Network Relay needs to establish secured PC5 link with the upstream node (Intermediate UE-to-Network Relay or the UE-to-Network Relay) before it can serve the Remote UE, or the Intermediate UE-to-Network Relay acting the role of the Remote UE. The Intermediate UE-to-Network Relay’s UDM checks whether the Intermediate UE-to-Network Relay is authorised to offer multi-hop UE-to-Network relay service based on the RSC.

4. The Intermediate UE-to-Network Relay-A uses the protected PC5 link established in step 3 to send the parameters in the DCR in step 2 to the network. Based on the steps 3-13 of 6.3.3.3.2, the Intermediate UE-to-Network Relay-A interacts with the network, in order to get the KNR\_ProSe and freshness parameter to set up the connection with the Remote UE.

If Layer-3 connection is setup, the Intermediate UE-to-Network Relay-A sends/receives the Intermediate key request/response to the UE-to-Network Relay who forwards/receives the request/response over its own NAS connection to the UE-to-Network Relay’s AMF.

5. The Intermediate UE-to-Network Relay-A uses the KNR\_ProSe and freshness parameter to establish secure PC5 link with the Remote UE.

##### 6.3.Z.2.b1 Security procedure over User Plane with multi-hop UE-to-Network Relay discovery with Model A

The security procedure over User Plane for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model A is used is shown in Figure 6.3.Z.2.b1-1.



Figure 6.3.Z.2.b1-1: Security procedure over User Plane for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model A is used

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3. In addition, the 5G ProSe Remote UE and Intermediate UE-to-Network Relay are provisioned with UP-PRUK and UP-PRUK ID from 5G PKMF as specified in step 1 in clause 6.3.3.2.2.

1a. During multi-hop UE-to-Network Relay discovery with model A procedure, the 5G ProSe UE-to-Network Relay broadcasts an Announcement message.

1b. If the Intermediate UE-to-Network Relay does not have an existing PC5 link with the 5G ProSe UE-to-Network Relay or an upstream intermediate UE-to-Network relay when it receives a valid discovery message (i.e., Announcement message in discovery model A), the Intermediate UE-to-Network Relay shall establish a PC5 link with the 5G ProSe UE-to-Network Relay or the upstream intermediate UE-to-Network relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane specified in clause 6.3.3.2.2.

1c. Once the PC5 link is established between the Intermediate UE-to-Network Relay and the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network shall update the path information (e.g., hop count) in the Announcement message and protect the updated message. Then, the Intermediate UE-to-Network Relay broadcasts the protected Announcement message.

2. After multi-hop UE-to-Network Relay discovery, the 5G ProSe Remote UE shall establish a PC5 link with the upstream Intermediate UE-to-Network Relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane specified in clause 6.3.3.2.2 with the Intermediate UE-to-Network Relay taking the role of the 5G ProSe UE-to-Network Relay.

NOTE 1: It is assumed that an Intermediate UE-to-Network Relay is able to access to the 5G PKMF of its HPLMN.

##### 6.3.Z.2.b2 Security procedure over User Plane after multi-hop UE-to-Network Relay discovery with Model B

The security procedure for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model B is used is shown in Figure 6.3.Z.2.b2-1.

Figure 6.3.Z.2.b2-1: Security procedure over User Plane for multi-hop UE-to-Network Relay communication when multi-hop UE-to-Network Relay discovery with Model B is used

0. The 5G ProSe Remote UE, Intermediate UE-to-Network Relay, and 5G ProSe UE-to-Network Relay are provisioned with the discovery security materials associated with an RSC based on the procedure specified in clause 6.3. In addition, the 5G ProSe Remote UE and Intermediate UE-to-Network Relay are provisioned with UP-PRUK and UP-PRUK ID from 5G PKMF as specified in step 1 in clause 6.3.3.2.2.

1. The 5G ProSe Remote UE performs a multi-hop UE-to-Network Relay discovery with Model B procedure with the Intermediate UE-to-Network Relay and 5G ProSe UE-to-Network Relay.

2. After multi-hop UE-to-Network Relay discovery procedure, the 5G ProSe Remote UE shall initiate a PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane with the Intermediate UE-to-Network Relay by sending Direct Communication Request message.

3. If the Intermediate UE-to-Network Relay does not have an existing PC5 link with the selected 5G ProSe UE-to-Network Relay or an Intermediate UE-to-Network relay on the path to the 5G ProSe UE-to-Network Relay, the Intermediate UE-to-Network Relay shall establish a PC5 link with the 5G ProSe UE-to-Network Relay or the intermediate UE-to-Network relay based on the PC5 security establishment for 5G ProSe UE-to-Network relay communication over User Plane specified in clause 6.3.3.2.2.

4. The Intermediate UE-to-Network Relay, then, performs the Key Request/Response procedure with the 5G PKMF/DDNMF of Intermediate UE-to-Network Relay using the parameters received in step 2.

NOTE 1: It is assumed that an Intermediate UE-to-Network Relay is able to access to the 5G PKMF of its HPLMN.

5. The Intermediate UE-to-Network Relay performs Direct Security Mode Command procedure with the 5G ProSe Remote UE and completes the PC5 security establishment with the rest of procedures as specified in clause 6.3.3.2.2.

\* \* \* \* 13th change \* \* \* \*

### 6.6.1 General

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

The security requirements for 5G ProSe Layer‑3 UE-to-UE Relay and 5G ProSe Layer-2 UE-to-UE Relay are defined in clause 6.6.2. The security procedures for 5G ProSe L3 UE-to-UE Relay and 5G ProSe Layer-2 UE-to-UE Relay are defined in clause 6.6.3 and clause 6.6.4 respectively. The security requirements and security procedures for 5G ProSe Multi-hop Layer‑3 UE-to-UE Relay is defined in clause 6.6.XX.

\* \* \* \* 14th change \* \* \* \*

### 6.6.XX Security for 5G ProSe Communication via 5G ProSe Layer-3 Multi-hop UE‑to-UE Relay

This clause describes the security requirements and the procedures for 5G ProSe Layer-3 multi-hop UE-to-UE Relay communication defined in TS 23.304 [2], including the Layer-3 multi-hop UE-to-UE Relay communication using IP PDU type and using non-IP PDU type.

#### 6.6.XX.1 Security requirements

The following security requirements apply to 5G ProSe Layer-3 multi-hop UE-to-UE Relay:

- The 5G System shall support the authorization and authorisation of the UEs in the 5G ProSe Layer-3 multi-hop UE-to-UE Relay communication scenario.

- The 5G System shall support confidentiality protection, integrity protection, and replay protection for secure communication messages in the 5G ProSe Layer-3 multi-hop UE-to-UE Relay communication scenario.

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

#### 6.6.XX.2 Security procedure for 5G ProSe Layer-3 Multi-hop UE-to-UE Relay communication

The security procedures for 5G ProSe Layer-3 Multi-hop UE-to-UE Relay covers the procedures of security establishment of both IP PDU type and non-IP PDU type.

###### 6.6.XX.2.1 Security procedure for security establishment of 5G ProSe Layer-3 Multi-hop UE-to-UE Relay of IP PDU type

The 5G ProSe Layer-3 Multi-hop UE-to-UE Relay communication consists of two types of PC5 link establishment: one for PC5 link establishment among 5G ProSe UE-to-UE Relays and the other one for PC5 link establishment between an 5G ProSe End UE and 5G ProSe UE-to-UE Relay as specified in clause 6.7.5.2.1 of TS 23.304 [2].

For both types of PC5 link establishment, the security procedure for unicast mode 5G ProSe Direct Communication specified in clause 6.2 is reused with the following modifications:

- The RSC is included in the Direct Communication Request (DCR) message.

- The DCR message is protected based on the security mechanism defined in clause 6.3.5 with a modification that the UP-PRUK ID/CP-PRUK ID is not used in clause 6.3.5.2.

###### 6.6.XX.2.2 Security procedure for security establishment of 5G ProSe Layer-3 Multi-hop UE-to-UE Relay Discovery of non-IP PDU type

If 5G ProSe UE-to-UE Relays uses the RSC associated with the security procedures without network assistance, the security procedure specified in clause 6.2 is reused to establish a secure PC5 link for each hop among 5G ProSe End UEs and 5G ProSe UE-to-UE Relays, with the following modifications:

- The RSC is included in the Direct Communication Request (DCR) message.

- The DCR message is protected reusing the security mechanism defined in clause 6.3.5 with a modification that the length of the UP-PRUK ID/CP-PRUK ID is set to zero in clause 6.3.5.2.

Both UP-based and CP-based security procedures specified in clauses 6.3.3.2 and 6.3.3.3 are reused to establish secure PC5 link establishment for each hop among 5G ProSe End UEs and 5G ProSe UE-to-UE Relays if 5G ProSe UE-to-UE Relays are in-coverage.

\* \* \* \* 15th change \* \* \* \*

### 7.2.1 General

For UE-to-Network discovery, the 5G PKMF supports the authorization request from the 5G PKMF in another PLMN via the new service Npkmf\_Discovery. 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 discovery and communication between Intermediate UE-to-Network Relay and the next Intermediate UE-to-Network Relay, the Intermediate UE-to-Network Relay plays the role of the Remote UE, and the next Intermediate UE-to-Network Relay plays the role of the UE-to-Network Relay. For discovery and communication between Intermediate UE-to-Network Relay and the UE-to-Network Relay, the Intermediate UE-to-Network Relay plays the role of the Remote UE.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.

For discovery and communication between End UE and the UE-to-UE Relay, the End UE plays the role of the Remote UE, and the UE-to-UE Relay plays the role of the UE-to-Network Relay. For discovery and communication between UE-to-UE Relay and the next UE-to-UE Relay, the UE-to-UE Relay plays the role of the 5G ProSe Remote UE, and the next UE-to-UE Relay plays the rols of the 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\_Discovery | AnnounceAuthorize | Request/Response | 5G PKMF |
| MonitorKey | Request/Response | 5G PKMF |
| DiscoveryKey | Request/Response | 5G PKMF |
| Npkmf\_PKMFKeyRequest | ProseKey | Request/Response | 5G PKMF |
| Npkmf\_ResolveRemoteUserId | Npkmf\_ResolveRemoteUserId\_Get | Request/Response | SMF, 5G PKMF |

\* \* \* \* 16th change \* \* \* \*

### 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 discovery and communication between Intermediate UE-to-Network Relay and the next Intermediate UE-to-Network Relay, the Intermediate UE-to-Network Relay plays the role of the Remote UE, and the next ntermediate UE-to-Network Relay plays the role of the UE-to-Network Relay. For discovery and communication between Intermediate UE-to-Network Relay and the UE-to-Network Relay, the Intermediate UE-to-Network Relay plays the role of the Remote UE.

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.

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

\* \* \* \* End of change(s) \* \* \* \*