**3GPP TSG-SA3 Meeting #111 S3‑233374**

**Berlin, Germany, 22 - 26 May 2023** *revision of* *S3-233025*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **3** | **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\_Ph2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe\_Ph2 | | | | |  | ***Date:*** | | | 2023-05-22 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | New WID on Security Aspects of Proximity-based Services in 5GS Phase 2 was approved in TSG SA Meeting #SP-99.  To begin normative work, a skeleton should be proposed for organizing the normative work approved in TR 33.740 in TS 33.503. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Skeleton for the security normative work of 5G\_ProSe\_Ph2 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Normative work cannot be started. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3, 3.1, 6.1.3, 6.3, 6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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.

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*

## 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

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*

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

##### 6.1.3.3.1 General

The two sets of discovery security materials are used for UE-to-UE Relay discovery message protection. One (i.e., Direct Discovery security materials) is used for protecting direct discovery set. The other one (i.e., UE-to-UE Relay Discovery security materials) is used for protecting the UE-to-UE relay discovery messages. The UE-to-UE relay discovery messages include the protected direct discovery set.

Provisioning of the Direct Discovery security materials reuses the security material provisioning mechanism for Restricted 5G ProSe Direct Discovery as specified in clause 6.1.3.3.

Provisioning of the UE-to-UE Relay Discovery security materials reuses the security material provisioning mechanism for 5G ProSe UE-to-Network Relay discovery as specified in clause 6.1.3.3.

The protection 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 ProSe 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.

Editor’s Note: How to provision the discovery security materials associated with a Prose service is FFS.

2. The announcing 5G ProSe End UE shall protect the direct discovery set using the discovery security materials associated with the ProSe service as specified in clause 6.1.3.2.3 of the present document. The 5G ProSe UE-to-UE Relay obtains the protected RSC and 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 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 protected direct discovery set. The 5G ProSe UE-to-UE Relay shall store the protected direct discovery set along with its validity time.

Editor’s Note: how to ensure that valid protected direct discovery sets are announced by the U2U relay is FFS.

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 decrypt and/or verify 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 decrypt and/or verify the direct discovery set(s) using the discovery security materials associated with the ProSe 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 ProSe 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.

Editor’s Note: How to provision the discovery security materials associated with a Prose service is FFS.

Editor’s Note: Details on how the direct discovery set and discovery messages are protected is FFS.

1. The discoverer 5G ProSe End UE shall protect a direct discovery set using the discovery security materials associated with the ProSe 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 decrypt and/or verify 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 decrypt and/or verify 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 decrypt and/or verify the direct discovery set using the discovery security materials associated with the ProSe 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 ProSe 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.

Editor’s Note: How to decrypt the direct discovery set by 5G Prose End UE is FFS.

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 decrypt and/or verify 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 decrypt and/or verify 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 decrypt and/or verify the direct discovery set using the discovery security materials associated with the ProSe 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

Editor’s Note: This clause describes the security procedure 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.

Editor’s Note: further detail is to be included.

#### 6.3.6.2 Security requirements

Editor’s Note: further detail is to be included.

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

Editor’s Note: further detail is to be included.

##### 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 intergrity 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\*\*\*\*\*\*\*\*\*\*\*\*

## 6.6 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 4a-4e in clause 6.3.3.2.2 and the steps 3-13 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, the Target End UE shall inform the UE-to-UE Relay to initiate the above steps.

Editor’s Note: The detailed message to trigger above steps is FFS.Editor’s Note: Additional details on the DCR message from the UE-to-UE Relay to target UE are FFS.

#### 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.

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

Editor’s Note: The choice and co-existence of the security mechanisms in different use cases (i.e., U2U Relay in and out of coverage) is FFS.

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

Editor’s Note: This clause describes security solution for protecting identity privacy for communication for 5G ProSe Layer-3 UE-to-UE Relay.

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

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

#### 6.6.4.1 Security procedure for 5G ProSe Layer-2 UE-to-UE Relay

Editor’s Note: This clause describes the security procedure for 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.

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