**3GPP TSG-SA3 Meeting #115 *draft\_S3-240506-r5***

**Athens, Greece, 26 February - 1 March 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0160** | **rev** | **x** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update to the identification of U2NW discovery security materials | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Nokia, Nokia Shanghai Bell, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Based on the current mechanism, the 5G DDNMF of the Remote UE can get the discovery security materials from 5G DDNMFs in different HPLMNs of potential Relay UEs, these different sets of discovery security materials are identified using the same RSC. In this case, UEs cannot identify which set of security materials is used. In addition, SA2 confirmed the RSC value used need to be unique across these involved PLMNs in the LS reply to SA3 (S3-240244/S2-2401587). SA2 also agreed a Rel-18 CR (S2-2401588/TS 23.304 CR 0370) to add clarifications to TS 23.304 regarding the use of the same Relay Service Code by UEs from different PLMNs.  This contribution also includes editorial chagnes.  Merger of S3-240506, S3-240610 and S3-240509. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | PLMN ID of the Announcing/Discoveree UE is provided by the 5G DDNMF of the Relay. Remote UE and the Relay use the PLMN ID to identify the security materials during discovery procedures. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | UEs cannot identify different discovery security materials during UE-to-Network Relay discovery procedures. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.2.1, 6.1.3.2.2.1, 6.1.3.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* \* First change \* \* \* \*

##### 6.1.3.2.1 General

The security for both models of restricted 5G ProSe Direct Discovery is similar to that of open 5G ProSe Direct Discovery described in clause 6.1.3.1. Both models also use a UTC-based counter (see step 9 in clause 6.1.3.1) to provide freshness for the protection of the restricted 5G ProSe Direct Discovery message on the PC5 interface. The parameters CURRENT\_TIME and MAX\_OFFSET are also provided to the UE from the 5G DDNMF in its HPLMN to ensure that the obtained UTC-based counter is sufficiently close to real time to protect against replays.

The major differences are that restricted 5G ProSe Direct Discovery requires confidentiality protection of the discovery messages (e.g. to ensure a UE's privacy is not disclosed to unauthorized parties or tracked due to constantly sending the same ProSe Restricted/Response Code in the clear) and that the MIC checking may be performed by the receiving UE (if allowed by the 5G DDNMF).

The security parameters needed by a sending UE to protect a discovery message (i.e. in Model A the Announcing UE and in Model B the Discoverer UE sending the ProSe Query Code and the Discoveree UE sending the ProSe Response Code) are provided in the Code-Sending Security Parameters. Similarly, the security parameters needed by a UE receiving a discovery message (i.e. in Model A the Monitoring UE and in Model B the Discoverer UE receiving a ProSe Response Code and the Discoveree receiving a ProSe Query Code) are provided in the Code-Receiving Security Parameters.

In addition to clause 6.1.3.4.1 in TS 33.303 [4], 5G Prose introduced two new features:

- During the discovery request procedure, 5G DDNMF may optionally provide the PC5 security policies to the UEs.

- A ciphering algorithm for message-specific confidentiality is configured at the UE during the Discovery Request procedure.

5G ProSe UE-to-Network Relay discovery is different from 5G ProSe Restricted Direct Discovery. In 5G ProSe UE‑to-Network Relay discovery, the discovery security materials are provided by the PKMF for RSC(s) representing user-plane based security procedure, and by the DDNMF or the PCF for RSC(s) with Control Plane Security Indicator set representing control-plane based security procedure. The 5G ProSe UE-to-Network Relay discovery procedures described in clause 6.1.3.2.2.1 and clause 6.1.3.2.2.2 apply with adjustment when 5G DDNMF or 5G PKMF is used for 5G ProSe UE-to-Network Relay discovery. In the case of UE-to-Network relays belonging to different HPLMNs serving the same RSC, distinct sets of discovery security materials for potential relays of different HPLMNs are provided to the 5G ProSe remote UE. HPLMN ID of the 5G DDNMF/5G PKMF of the potential 5G ProSe UE-to-Network Relays is carried in PC5 discovery messages to identify the corresponding discovery security materials.\* \* \* \* Second change \* \* \* \*

###### 6.1.3.2.2.1 Restricted 5G ProSe Direct Discovery Model A

The security procedure for restricted 5G ProSe Direct Discovery Model A is described as follows.



Figure 6.1.3.2.2.1-1: Security procedure for restricted 5G ProSe Direct Discovery Model A

NOTE 1: When the user-plane based security procedure for the UE-to-Network Relay is used, the 5G PKMF takes the role of the 5G DDNMF as described in clause 6.3.3.2 of the present document.

Steps 1-4 refer to an Announcing UE:

1. Announcing UE sends a Discovery Request message containing the Restricted ProSe Application User ID (RPAUID) to the 5G DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material. In addition, the Announcing UE shall include its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE in the Discovery Request message.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe UE-to-Network Relay plays the role of the Announcing UE and sends a Relay Discovery Key Request instead of a Discovery Request. The Relay Discovery Key Request message includes the Relay Service Code (RSC) and the 5G ProSe UE-to-Network Relay's PC5 security capability.

2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server.

For 5G ProSe UE-to-Network Relay discovery, the 5G DDNMF may check with the UDM whether the UE-to-Network relay is authorized to announce UE-to-Network relay discovery message.

3. If the Announcing UE is roaming, the 5G DDNMFs in the HPLMN and VPLMN of the Announcing UE exchange Announce Auth.

For 5G ProSe UE-to-Network Relay discovery, Npkmf\_Discovery\_AnnounceAuthorize service operation is used to obtain the authorization from the 5G PKMF for announcing in the PLMN.

4. The 5G DDNMF in the HPLMN of the Announcing UE returns the ProSe Restricted Code and the corresponding Code-Sending Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters. The Code-Sending Security Parameters provide the necessary information for the Announcing UE to protect the transmission of the ProSe Restricted Code and are stored with the ProSe Restricted Code. The Announcing UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of clause 6.1.3.1 of the present document. The 5G DDNMF in the HPLMN of the Announcing UE shall include the chosen PC5 ciphering algorithm in the Discovery Response message. The 5G DDNMF determines the chosen PC5 ciphering algorithm based on the ProSe Restricted Code and the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm together with the ProSe Restricted Code.

In addition, the 5G DDNMF in the HPLMN of the Announcing UE may associate the ProSe Restricted Code with the PC5 security policies and include the PC5 security policies in the Discovery Response message.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of the ProSe Restricted Code.

NOTE 2: 5G DDNMF may get the PC5 security policies in different ways (e.g. from PCF, from ProSe Application Server, or based on local configuration).

Steps 5-10 refer to a Monitoring UE:

5. The Monitoring UE sends a Discovery Request message containing the RPAUID and its PC5 UE security capability to the 5G DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application User IDs.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe Remote UE plays the role of the Monitoring UE and sends a Relay Discovery Key Request instead of the Discovery Request. The Relay Discovery Key Request message includes the RSC and the 5G ProSe Remote UE's PC5 security capability. The Remote UE may provide a list of PLMNs in which the UE is authorized to use a 5G ProSe UE-to-Network Relay. in the Relay Discovery Key Request.

6. The 5G DDNMF in the HPLMN of the Monitoring UE sends an authorization request to the ProSe Application Server. If, based on the permission settings, the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.

For 5G ProSe UE-to-Network Relay discovery, the 5G DDNMF of the Remote UE may check with the UDM whether the Remote UE is authorized to monitor UE-to-Network relay discovery.

7. If the Discovery Request is authorized, the 5G DDNMF in the HPLMN of the Monitoring UE contacts the 5G DDNMF in the HPLMN of the Announcing UE by sending a Monitor Request message, as specified in clause 6.3 of TS 23.304 [2], including the PC5 UE security capability received in step 5.

For 5G ProSe UE-to-Network Relay Discovery, Relay Discovery Key Request and RSC are used instead of Discovery Request and RPAUID. The 5G DDNMF of the remote UE discovers 5G DDNMF(s) of the potential 5G ProSe UE-to-Network relay(s) supporting the RSC based on HPLMNs of the potential 5G ProSe UE-to-Network relay(s) mapping to the RSC. Npkmf\_Discovery\_MonitorKey service operation is used to obtain the discovery key from the 5G PKMF for monitoring in the PLMN.

NOTE 2a: 5G DDNMF may get the HPLMNs of the potential 5G ProSe UE-to-Network relays in different ways (e.g. from PCF, or based on local configuration).

8. The 5G DDNMF in the HPLMN of the Announcing UE may exchange authorization messages with the ProSe Application Server.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

9. If the PC5 UE security capability in step 5 includes the chosen PC5 ciphering algorithm, the 5G DDNMF in the HPLMN of the Announcing UE responds to the 5G DDNMF in the HPLMN of the Monitoring UE with a Monitor Response message including the ProSe Restricted Code, the corresponding Code-Receiving Security Parameters, an optional Discovery User Integrity Key (DUIK), and the chosen PC5 ciphering algorithm (based on the information/keys stored in step 4). The Code-Receiving Security Parameters provide the information needed by the Monitoring UE to undo the protection applied by the Announcing UE. The DUIK shall be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Monitoring UE use Match Reports for MIC checking. The 5G DDNMF in the HPLMN of the Monitoring UE stores the ProSe Restricted Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters).

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Monitor Response, and the RSC and the HPLMN ID of the 5G ProSe UE-to-Network Relay (i.e. the Announcing UE) are used instead of the ProSe Restricted Code. The HPLMN ID of the 5G ProSe UE-to-Network Relay is used to identify the discovery security materials. Npkmf\_Discovery\_MonitorKey service operation is used to obtain the discovery key from the 5G PKMF for monitoring in the PLMN. The 5G DDNMF of the remote UE may receive multiple Relay Discovery Key Responses if multiple 5G DDNMFs/PKMFs of the potential relays supporting the RSC are discovered in step 7.

The 5G DDNMF in the HPLMN of the Announcing UE may send the PC5 security policies associated with the ProSe Restricted Code to the 5G DDNMF in the HPLMN of the Monitoring UE.

NOTE 3: For 5G ProSe Direct Discovery, there are two possible configurations for integrity checking, namely, MIC checked by the 5G DDNMF of the Monitoring UE, and MIC checked at the Monitoring UE side. Which configuration to use is decided by the 5G DDNMF, which assigns the monitored ProSe Restricted Code and signals the Monitoring UE in the Code-Receiving Security Parameters.

For 5G ProSe UE-to-Network Relay discovery, MIC checking is performed only at the Remote UE and the 5G DDNMF of the Remote UE does not need to configure integrity checking for UE-to-Network Relay discovery.

NOTE 4: The chosen PC5 ciphering algorithm is associated with the ProSe Restricted Code.

10. The 5G DDNMF in the HPLMN of the Monitoring UE returns the Discovery Filter and the Code-Receiving Security Parameters, along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Monitoring UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the present document. The UE stores the Discovery Filter, Code-Receiving Security Parameters, and the chosen PC5 ciphering algorithm together with the ProSe Restricted Code.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is returned instead of the Discovery Response, and the RSC is included instead of the ProSe Restricted Code. The response message contains the discovery security materials and the HPLMN ID as contained in step 9. The Relay Discovery Key Response includes multiple sets of discovery security materials and the associated HPLMN IDs of the potential relays if multiple 5G DDNMFs/PKMFs of the potential relays supporting the RSC are discovered in step 7.

If the 5G DDNMF in the HPLMN of the Monitoring UE receives the PC5 security policies associated with the ProSe Restricted Code in step 9, the Monitoring UE's 5G DDNMF forwards the PC5 security policies to the Monitoring UE.

Steps 11 and 12 occur over PC5:

11. The UE starts announcing, if the UTC-based counter provided by the system associated with the discovery slot is within the MAX\_OFFSET of the Announcing UE's ProSe clock and if the Validity Timer has not expired. The UE forms the discovery message and protects it. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.

For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Response Code and the announcing message also includes the HPLMN ID in cleartext to identify the discovery security materials.

12. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the monitoring UE's ProSe clock. In order to find such a matching message, it processes the message. If the Monitoring UE was not asked to send Match Reports for MIC checking, it stops at this step from a security perspective. Otherwise, it proceeds to step 13.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe remote UE decides the discovery security materials to process the discovery message by using the HPLMN ID in the announcing message.

NOTE 5: The UE checking the integrity of the discovery message on its own does not prevent the UE from sending a Match Report due to requirements in TS 23.304 [2]. If such a Match Report is sent, then there is no security functionality involved.

Steps 13-16 refer to a Monitoring UE that has encountered a match:

NOTE 6: For 5G ProSe UE-to-Network Relay discovery, the steps 13-16 are skipped.

13. If the UE has either not had the 5G DDNMF check the MIC for the discovered ProSe Restricted Code previously or the 5G DDNMF has checked a MIC for the ProSe Restricted Code and the associated Match Report refresh timer (see step 15 for details of this timer) has expired, or as required based on the procedure specified in TS 23.304 [2], then the Monitoring UE sends a Match Report message to the 5G DDNMF in the HPLMN of the Monitoring UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the Monitoring UE's UTC-based counter associated with the discovery slot where it heard the announcement, and other discovery message parameters including the ProSe Restricted Code and MIC. The 5G DDNMF checks the MIC.

14. The 5G DDNMF in the HPLMN of the Monitoring UE may exchange an Auth Req/Auth Resp with the ProSe Application Server to ensure that Monitoring UE is authorized to discover the Announcing UE.

15. The 5G DDNMF in the HPLMN of the Monitoring UE returns to the Monitoring UE an acknowledgement that the integrity check passed. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock. The 5G DDNMF in the HPLMN of the Monitoring UE included the Match Report refresh timer in the message to the Monitoring UE. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe Restricted Code.

16. The 5G DDNMF in the HPLMN of the Monitoring UE may send a Match Report Info message to the 5G DDNMF in the HPLMN of the Announcing UE.

\* \* \* \* Third change \* \* \* \*

###### 6.1.3.2.2.2 Restricted 5G ProSe Direct Discovery Model B

The security procedure for restricted 5G ProSe Direct Discovery Model B is described as follows.



Figure 6.1.3.2.2.2-1: Security procedure for restricted 5G ProSe Direct Discovery Model B

NOTE 1: When the user-plane based security procedure for the UE-to-Network Relay is used, the 5G PKMF takes the role of the 5G DDNMF as described in clause 6.3.3.2 of the present document.

Steps 1-4 refer to a Discoveree UE:

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to get Discovery Query Filter(s) to monitor a query, the ProSe Response Code to announce and associated security materials. The command indicates that this is for ProSe Response (Model B) operation, i.e. for a Discoveree UE. In addition, the Discoveree UE shall include its PC5 UE security capability that contains the list of supported ciphering algorithms by the UE in the Discovery Request message.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe UE-to-Network Relay plays the role of the Discoveree UE and sends a Relay Discovery Key Request instead of a Discovery Request. The Relay Discovery Key Request message includes the Relay Service Code (RSC) and the 5G ProSe UE-to-Network Relay's PC5 security capability.

2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server depending on 5G DDNMF configuration.

For 5G ProSe UE-to-Network Relay discovery, the 5G DDNMF may check with the UDM whether the UE-to-Network relay is authorized to announce UE-to-Network relay discovery.

3. The 5G DDNMFs in the HPLMN and VPLMN of the Discoveree UE exchange Announce Auth. Messages. If the Discoveree UE is not roaming, these steps do not take place.

For 5G ProSe UE-to-Network Relay discovery, Npkmf\_Discovery\_AnnounceAuthorize service operation is used to obtain the authorization from the 5G PKMF for announcing in the PLMN.

4. The 5G DDNMF in the HPLMN of the Discoveree UE returns the ProSe Response Code and the Code-Sending Security Parameters, Discovery Query Filter(s), Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Code-Sending Security Parameters provide the necessary information for the Discoveree UE to protect the transmission of the ProSe Response Code and are stored with the ProSe Response Code. The Code-Receiving Security Parameters provide the information needed by the Discoveree UE to undo the protection applied to the ProSe Query Code by the Discoverer UE. The Code-Receiving Security Parameters indicate a Match Report will not be used for MIC checking. The UE stores each Discovery Filter with its associated Code-Receiving Security Parameters. The Discoveree UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of clause 6.1.3.1 of the present document. The 5G DDNMF in the HPLMN of the Discoveree UE shall include the chosen PC5 ciphering algorithm in the Discovery Response message. The 5G DDNMF determines the chosen PC5 ciphering algorithm based on the ProSe Response Code and the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm together with the ProSe Response Code.

In addition, the 5G DDNMF in the HPLMN of the Discoveree UE may associate the ProSe Response Code with the PC5 security policies and include the PC5 security policies in the Discovery Response message.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of ProSe Query Code and ProSe Response Code.

NOTE 2: 5G DDNMF may get the PC5 security policies in different ways (e.g. from PCF, from ProSe Application Server, or based on local configuration).

Steps 5-10 refer to a Discoverer UE:

5. The Discoverer UE sends a Discovery Request message containing the RPAUID and its PC5 UE security capability to the 5G DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application User IDs.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe Remote UE plays the role of the Discoverer UE and sends a Relay Discovery Key Request instead of the Discovery Request. The Relay Discovery Key Request message includes the RSC and the 5G ProSe Remote UE's PC5 security capabilities. The Remote UE may provide a list of PLMNs in which the UE is authorized to use a 5G ProSe UE-to-Network Relay. in the Relay Discovery Key Request.

6. The 5G DDNMF in the HPLMN of the Discoverer UE sends an authorization request to the ProSe Application Server. If the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.

For 5G ProSe UE-to-Network Relay discovery, the 5G DDNMF of the Remote UE may check with the UDM whether the Remote UE is authorized to monitor UE-to-Network relay discovery.

7. If the Discovery Request is authorized, the 5G DDNMF in the HPLMN of the Discoverer UE contacts the 5G DDNMF in the HPLMN of the Discoveree UE by sending a Discovery Request message, as specified in clause 6.3 of TS 23.304 [2], including the PC5 UE security capability in step 5.

For 5G ProSe UE-to-Network Relay Discovery, Relay Discovery Key Request and RSC are used instead of Discovery Request and RPAUID. The 5G DDNMF of the remote UE discovers 5G DDNMF(s) of the potential 5G ProSe UE-to-Network relay(s) supporting the RSC based on HPLMNs of the potential 5G ProSe UE-to-Network relay(s) mapping to the RSC. Npkmf\_Discovery\_DiscoveryKey service operation is used to obtain the discovery key from the 5G PKMF for a discoverer UE in the PLMN.

NOTE 2a: 5G DDNMF may get the HPLMNs of the potential 5G ProSe UE-to-Network relays in different ways (e.g. from PCF, or based on local configuration).

8. The 5G DDNMF in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.

For 5G ProSe UE-to-Network Relay discovery, this step is skipped.

9. If the PC5 UE security capability in step 5 includes the chosen PC5 ciphering algorithm, the 5G DDNMF in the HPLMN of the Discoveree UE responds to the 5G DDNMF in the HPLMN of the Discoverer UE with a Discovery Response message including the ProSe Query Code(s) and their associated Code-Sending Security Parameters, ProSe Response Code and its associated Code-Receiving Security Parameters, an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code, and a chosen PC5 ciphering algorithm. The Code-Receiving Security Parameters provide the information needed by the Discoverer UE to undo the protection applied by the Discoveree UE. The DUIK shall be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Discoverer UE use Match Reports for MIC checking. The 5G DDNMF in the HPLMN of the Discoverer UE stores the ProSe Response Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters). The Code-Sending Security Parameters provide the information needed by the Discoverer UE to protect the ProSe Query Code.

The 5G DDNMF in the HPLMN of the Discoveree UE may send the PC5 security policies associated with the ProSe Response Code to the 5G DDNMF in the HPLMN of the Discoverer UE.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC and the HPLMN ID of the 5G ProSe UE-to-Network Relay (i.e. the Discoveree UE) are used instead of ProSe Query Code and ProSe Response Code. The HPLMN ID of the 5G ProSe UE-to-Network Relay is used to identify the discovery security materials. Npkmf\_Discovery\_DiscoveryKey service operation is used to obtain the discovery key from the 5G PKMF for a discoverer UE in the PLMN. The 5G DDNMF/PKMFs of the remote UE may receive multiple Relay Discovery Key Responses if multiple 5G DDNMFs/PKMFs of the potential relays supporting the RSC are discovered in step 7.

NOTE 3: For 5G ProSe Direct Discovery, there are two possible configurations for integrity checking, namely, MIC checked by the 5G DDNMF of the Discoverer UE, and MIC checked at the Discoverer UE side; this is decided by the 5G DDNMF that assigns the ProSe Restricted Code, and signals the Discoverer UE in the Code-Receiving Security Parameters.

For 5G ProSe UE-to-Network Relay discovery, MIC checking is performed only at the Remote UE and the 5G DDNMF of the Remote UE does not need to configure integrity checking for UE-to-Network Relay discovery.

NOTE 4: The chosen PC5 ciphering algorithm is associated with the ProSe Response Code.

10. The 5G DDNMFs in the HPLMN and VPLMN of the Discoverer UE exchange Announce Auth. messages. If the Discoverer UE is not roaming, these steps do not take place.

For 5G ProSe UE-to-Network Relay discovery, Npkmf\_Discovery\_AnnounceAuthorize service operation is used to obtain the authorization from the 5G PKMF for discovering in the PLMN.

11. The 5G DDNMF in the HPLMN of the Discoverer UE returns the Discovery Response Filter and the Code-Receiving Security Parameters, the ProSe Query Code, the Code-Sending Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters and the chosen PC5 ciphering algorithm. The Discoverer UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of clause 6.1.3.1 of the present document. The UE stores the Discovery Response Filter and its Code-Receiving Security Parameters and the ProSe Query Code and its Code-Sending Security Parameters, and the chosen PC5 ciphering algorithm together with the ProSe Response Code.

If the 5G DDNMF in the HPLMN of the Discoverer UE receives the PC5 security policies associated with the ProSe Response Code in step 9, the Discoverer UE's 5G DDNMF forwards the PC5 security policies to the Discoverer UE.

For 5G ProSe UE-to-Network Relay discovery, a Relay Discovery Key Response is used instead of the Discovery Response, and the RSC is used instead of the ProSe Restricted Code. The response message contains the discovery security materials and the HPLMN ID as contained in step 9. The Relay Discovery Key Response includes multiple sets of discovery security materials and the associated HPLMN IDs of the potential relays if multiple 5G DDNMFs/PKMFs of the potential relays supporting the RSC are discovered in step 7.

Steps 12 to 15 occur over PC5:

12. The Discoverer UE sends the ProSe Query Code and also listens for a response message if the UTC-based counter provided by the system associated with the discovery slot is within the MAX\_OFFSET of the Discoverer UE's ProSe clock and if the Validity Timer has not expired. The Discoverer UE forms the discovery message and protects it. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.

For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Query Code.

NOTE 5: The 5G ProSe Remote UE may send multiple discovery messages protected with different discovery security materials, until receiving matched discovery response.

13. The Discoveree UE listens for a discovery message that satisfies its Discovery Filter if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the Discoveree UE's ProSe clock. In order to find such a matching message, it processes the message.

For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Query Code.

NOTE 6: Match Reports are not used for the MIC checking of ProSe Query Codes.

14. The Discoveree UE sends the ProSe Response Code associated with the discovered ProSe Query Code. The Discoveree UE forms the discovery message and protects it. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.

For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Response Code and the discovery message also includes the HPLMN ID in cleartext to identify the discovery security materials.

15. The Discoverer UE listens for a discovery message that satisfies its Discovery Filter. In order to find such a matching message, it processes the message. If the Discoverer UE was not asked to send Match Reports for MIC checking, it stops at this step from a security perspective. Otherwise, it proceeds to step 16.

For 5G ProSe UE-to-Network Relay discovery, the 5G ProSe UE-to-Network remoteUE decides the discovery security materials to process the discovery message by using the HPLMN ID in the discovery message.

NOTE 7: The UE checking the integrity of the discovery message on its own does not prevent the UE from sending a Match Report due to requirements in TS 23.304 [2]. If such a Match Report is sent, then there is no security functionality involved.

NOTE 8: The security keys in the Code-Sending Security Parameters of Discoverer UE and the security keys in the Code-Sending Security Parameters of Discoveree UE need to be generated independently and randomly.

Steps 16-19 refer to a Discoverer UE that has encountered a match:

NOTE 9: For 5G ProSe UE-to-Network Relay discovery, the steps 16-19 are skipped.

16. If the Discoverer UE has either not had the 5G DDNMF check the MIC for the discovered ProSe Response Code previously or the 5G DDNMF has checked a MIC for the ProSe Response Code and the associated Match Report refresh timer (see step 18 for details of this timer) has expired, or as required based on the procedure specified in TS 23.304 [2], then the Discoverer UE sends a Match Report message to the 5G DDNMF in the HPLMN of the Discoverer UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the Discoverer UE's UTC-based counter associated with the discovery slot where it heard the announcement, and other discovery message parameters including the ProSe Response Code and MIC. The 5G DDNMF checks the MIC.

17. The 5G DDNMF in the HPLMN of the Discoverer UE may exchange an Auth Req/Auth Resp with the ProSe Application Server to ensure that Discoverer UE is authorized to discover the Discoveree UE.

18. The 5G DDNMF in the HPLMN of the Discoverer UE returns to the Discoverer UE an acknowledgement that the integrity check passed. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock. The 5G DDNMF in the HPLMN of the Discoverer UE include the Match Report refresh timer in the message to the Discoverer UE. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe Response Code.

19. The 5G DDNMF in the HPLMN of the Discoverer UE may send a Match Report Info message to the 5G DDNMF in the HPLMN of the Discoveree UE.

\* \* \* \* End of changes \* \* \* \*