**3GPP TSG-SA3 Meeting #107-e *draft\_S3-221000-r3***

**e-meeting, 14 - 25 February 2022** Revision of S3-22xxxx

**Source: Qualcomm Incorporated, Philips International B.V., Ericsson, Huawei, HiSilicon**

**Title: Update on 5G ProSe restricted discovery procedure for U2N relay**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***This contribution proposes to update the texts in clause 6.1.3.2.2 in TS 33.503.***

# 2 References

[1] TS 33.503: “Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)”

[2] TS 33.303: “Proximity-based Services (ProSe); Security aspects”

[3] TS 24.554: “Proximity-services (ProSe) in 5G System (5GS) protocol aspects”

[4] TS 33.501: “Security architecture and procedures for 5G system”

[5] TS 24.334: “Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects”

# 3 Rationale

This contribution proposes to update the Restricted 5G ProSe Direct Discovery procedure to accommodate UE-to-Network (U2N) relay discovery procedure.

In clause 6.3.3, the U2N relay security procedure refers to the Restricted 5G ProSe Direct Discovery procedure for relay discovery. However, some of the procedures and parameters cannot be applied to U2N relay discovery. Thus, we propose to update the texts in the Restricted 5G ProSe Direct Discovery procedure to incorporate the U2N relay discovery procedure.

In particular, the following changes are proposed in this contribution:

* A NOTE describing the 5G PKMF takes the role of the 5G DDNMF when the user-plane procedure for the Layer-3 UE-to-network relay is used.
* In step 1 and 5, for 5G ProSe U2N Relay discovery, the Relay Service Code (RSC) is used instead of RPAUID.
* In step 4 and 9, for 5G ProSe U2N Relay discovery, the RSC is used instead of the ProSe Restricted/Query/Response Code.
* In step 9, DUIK shall be included in the code-receiving security parameters if MIC checking is used for a particular RSC.
* A NOTE describing the match report procedure is not used for MIC checking for the UE-to-network relay discovery.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the ProSe TS.

**\*\*\*\*\* START OF 1st CHANGES \*\*\*\*\***

#### 6.1.3.2 Restricted 5G ProSe Direct Discovery

##### 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 subclause 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 is not discovered by 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 a new feature:

- 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.

In case of 5G ProSe UE-to-Network Relay discovery, the discovery security materials are provided by the PKMF in case of user-plane based security procedure (as specified in clause 6.3.3.2), and by the DDNMF or the PCF in case of control-plane based security procedure (as specified in clause 6.3.3.3). 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 only when 5G DDNNF or 5G PKMF is used for 5G ProSe UE-to-Network Relay discovery.

##### 6.1.3.2.2 Security flows

###### 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 0: 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 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 Announcing UE sends a Discovery Key Request instead of a Discovery Request. The Discovery Key Request message includes the Relay Service Code (RSC). 2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server.

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

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, this step is skipped.

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 subclause 6.1.3.1 of the current specification. The 5G DDNMF in the HPLMN of the Announcing UE shall include the chosen PC5 ciphering algorithm in the Discovery Response message. The 5GDDNMF 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 Discovery Key Response is used instead of the Discovery Response with the following parameter change: the RSC is used instead of the ProSe Restricted Code.

NOTE 1: 5G DDNMF can 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 Monitoring UE sends a Discovery Key Request instead of the Discovery Request. The Discovery Key Request message includes the RSC.

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, this step is skipped.

7. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the 5G DDNMF in the HPLMN of the Monitoring UE contacts the indicated PLMN’s 5G DDNMF i.e., the 5G DDNMF in the HPLMN of the Announcing UE, by sending a Monitor Request message, including the PC5 UE security capability received in step 5.

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. 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 Discovery Key Response is used instead of the Discovery Response with the following parameter change: the RSC is used instead of the ProSe Restricted Code. Additionally, if MIC checking is used for a particular RSC, the DUIK shall be included in the Code-Receiving Security Parameters.NOTE x: Match Report is not used for MIC checking for 5G ProSe UE-to-Network Relay discovery.

 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 2: There are two configurations possible for integrity checking, namely, MIC checked by the 5G DDNMF of the Monitoring UE, and MIC checked at the Monitoring UE side. Which of the configuration is used is decided by the 5G DDNMF that assigned the ProSe Restricted Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

NOTE 3: The chosen PC5 ciphering algorithm is associated with the ProSe 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 subclause 6.1.3.1 of the current specification. The UE stores the Discovery Filter, Code-Receiving Security Parameters, and the chosen PC5 ciphering algorithm together with the ProSe Code.

 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.

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.

NOTE 4: 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.

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 authorised 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 include 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.

###### 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 0: 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 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 Discoveree UE sends a Discovery Key Request instead of a Discovery Request. The Discovery Key Request message includes the Relay Service Code (RSC).

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, this step is skipped.

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, this step is skipped.

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 subclause 6.1.3.1 of the current specification. 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 Code and the received PC5 UE security capability in step 1. The UE stores the chosen PC5 ciphering algorithm together with the ProSe 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 Discovery Key Response is used instead of the Discovery Response with the following parameter change: the RSC is used instead of ProSe Query Code and ProSe Response Code.

NOTE 1: 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 Discoverer UE sends a Discovery Key Request instead of the Discovery Request. The Discovery Key Request message includes the RSC.

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, this step is skipped.

7. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the 5G DDNMF in the HPLMN of the Discoverer UE contacts the indicated PLMN’s 5G DDNMF i.e., the 5G DDNMF in the HPLMN of the Discoveree UE, by sending a Discovery Request message, including the PC5 UE security capability in step 5.

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 Discovery Key Response is used instead of the Discovery Response with the following parameter change: the RSC is used instead of ProSe Query Code and ProSe Response Code. Additionally, if MIC checking is used for a particular RSC, the DUIK shall be included in the Code-Receiving Security Parameters.

NOTE x: Match Report is not used for MIC checking for 5G ProSe UE-to-Network Relay discovery.

NOTE 2: There are two configurations possible 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 assigned the ProSe Restricted Code, and signalled to the Discoverer UE in the Code-Receiving Security Parameters.

NOTE 3: The chosen PC5 ciphering algorithm is associated with the ProSe 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, this step is skipped.

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 subclause 6.1.3.1 of the current specification. 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 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.

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 Announcing 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.

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 Discoverer UE's ProSe clock. In order to find such a matching message, it processes the message.

NOTE 4: Match Reports are not used for the MIC checking of ProSe Query Codes.

14. The Discoveree 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.

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.

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.

NOTE 6: The security keys in the Code-Sending Security Parameters of discover 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.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 Monitoring 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 authorised 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 1st CHANGES \*\*\*\*\***