**3GPP TSG-SA3 Meeting #105e draft\_S3-214147-r5**

**e-meeting, 8 - 19 November 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated, CATT , ZTE, Huawei, HiSilicon**

**Title: CR to ProSe TS – Direct Discovery**

**Document for: Approval**

**Agenda Item: 4.21**

# 1 Decision/action requested

***This contribution proposes a text on Direct Discovery for ProSe TS***

# 2 References

[1] TR 33.847 v.0.8.0 “Study on security aspects of enhancement for proximity based services in the 5G System (5GS)”

[2] TS 23.304 v.2.0.0 “Proximity based Services (ProSe) in the 5G System (5GS)”

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

# 3 Rationale

This contribution proposes to add a content for ProSe Direct Discovery based on the conclusion in TR 33.847 [1]. The descriptions for open and restricted discovery are based on solutions #3 and #4 in TR 33.847 respectively. The detailed changes are as below:

Common:

* The description of procedure is moved below the figures.
* The reference TS 23.303 is changed to TS 23.304.

In clause 6.1.3.1 Open discovery,

* 6.1.3.1 Section name is added.
* Typos (PMLN to PLMN) in the figure are fixed.
* In step 4 and 9, SIB16 is changed to SIB9 as SIB9 carries UTC time in 5G.
* In step 8, “If MIC needs to be checked by …” is deleted because match report is consumed by HPLMN of announcing UE’s 5G DDNMF during discovery reporting procedure as specified in TS 23.304[2] clause 6.3.1.5.
* In step 9 and 10, the last sentence is deleted as MIC checking needs to be done in the HPLMN of the announcing UE’s 5G DDNMF to integrity check the received Match Report.
* In step 11, the description is modified to bring the exact conditions for performing the Match Report based on the description in TS 33.303 [3] clause 6.1.3.3.1.
* In step 13 and 14, “should” is changed to “shall” as these steps are mandatory procedure if the Match Report is sent to the 5G DDNMF in the HPLMN of the monitoring UE based on the conditions in step 11.
* In step 15, “check result” is changed to “MIC check result” for clarification.

In clause 6.1.3.2 Restricted discovery,

* Clause 6.1.3.2.1 General is added based on the descriptions in TS 33.303[3].
* In step 9 of both Model A and Model B, “shall” is included as it is mandatory when the 5G DDNMF configures to perform Match Report for MIC checking.
* In step 13 in Model A and step 16 in Model B, the condition for sending Match Report is added.
* In NOTE 4, “This ensures that the impersonation of the discoveree UE is not feasible when the discoverer UEs make use of match reports” is deleted as it is not needed in the technical specification.

In addition, the clause 6.1.3.2.3 (Protection of the discovery messages over the PC5 interface) is added to indicate that the protection of the discovery messages follows TS 33.303 [3] clause 6.1.3.4.3.

# 4 Detailed proposal

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

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

## 6.1 Security for 5G ProSe Discovery

Editor’s Notes: This clause contains the description of the security for open 5G ProSe Direct Discovery and restricted 5G ProSe Direct Discovery and 5G ProSe UE-to-Network Relay Discovery.

### 6.1.1 General

### 6.1.2 Security requirements

### 6.1.3 Security procedures

#### 6.1.3.1 Open discovery

The open discovery security procedure is described as follows:



**Figure 6.1.3.1-1: Open discovery security procedure**

1. The announcing UE sends a Discovery Request message containing the ProSe Application ID to the 5G DDNMF in its HPLMN in order to be allowed to announce a code on its serving PLMN (either VPLMN or HPLMN).
2. If the announcing UE wants to send announcements in the VPLMN, it needs to be authorised from the VPLMN 5G DDNMF. The 5G DDNMF in the HPLMN requests authorization from the VPLMN 5G DDNMF by sending Announce Auth.() message.
3. VPLMN 5G DDNMF responds with an Announce Auth. Ack () message, if authorization is granted. There are no changes to these messages for the purpose of protecting the transmitted code for open discovery. If the Announcing UE is not roaming, these steps do not take place.
4. The 5G DDNMF in HPLMN of the announcing UE returns the ProSe App Code that the announcing UE can announce and a Discovery Key associated with it. The 5G DDNMF stores the Discovery Key with the ProSe App Code. In addition, the 5G DDNMF provides the UE with a CURRENT\_TIME parameter, which contains the current UTC-based time at the 5G DDNMF, a MAX\_OFFSET parameter, and a Validity Timer. The UE sets a clock which is used for ProSe authentication (i.e. ProSe clock) to the value of CURRENT\_TIME and the UE stores the MAX\_OFFSET parameter, overwriting any previous values. The announcing UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB9, NITZ, NTP, GPS, via Ub interface (in GBA) (depending on which is available).

NOTE 1: The UE may use unprotected time to obtain the UTC-based counter associated with a discovery slot. This means that the discovery message could be successfully replayed if a UE is fooled into using a time different to the current time. The MAX\_OFFSET parameter is used to limit the ability of an attacker to successfully replay discovery messages or obtain correctly MICed discovery message for later use. This is achieved by using MAX\_OFFSET as a maximum difference between the UTC-based counter associated with the discovery slot and the ProSe clock held by the UE.

NOTE 2: A discovery slot is the time at which an announcing UE sends the announcement.

1. The UE starts announcing, if the difference between UTC-based counter provided by the system associated with the discovery slot and the UE’s ProSe clock is not greater than the MAX\_OFFSET and if the Validity Timer has not expired. For each discovery slot it uses to announce, the announcing UE calculates a 32-bit Message Integrity Check (MIC) to include with the ProSe App Code in the discovery message. Four least significant bits of UTC-based counter are transmitted along with the discovery message. The MIC is calculated as described in clause A.2 of TS 33.303 [x] using the Discovery Key and the UTC-based counter associated with the discovery slot.
2. The Monitoring UE sends a Discovery Request message containing the ProSe Application ID to the 5G DDNMF in its HPLMN in order to get the Discovery Filters that it wants to listen for.
3. The 5G DDNMF in the HPLMN of the monitoring UE sends Monitor Req. message to the 5G DDNMF in the HPLMN of the announcing UE.
4. The 5G DDNMF in the HPLMN of the announcing UE sends Monitor Resp. message to the 5G DDNMF in the HPLMN of the monitoring UE. 5G DDNMF
5. The 5G DDNMF returns the Discovery Filter containing either the ProSe App Code(s), the ProSe App Mask(s) or both along with the CURRENT\_TIME and the MAX\_OFFSET parameters. The UE sets its ProSe clock to CURRENT\_TIME and stores the MAX\_OFFSET parameter, overwriting any previous values. The monitoring UE obtains a value for a UTC-based counter associated with a discovery slot based on UTC time. The counter is set to a value of UTC time in a granularity of seconds. The UE may obtain UTC time from any sources available, e.g. the RAN via SIB9, NITZ, NTP, GPS (depending on which is available).
6. The Monitoring UE listens for a discovery message that satisfies its Discovery Filter, if the difference between UTC-based counter associated with that discovery slot and UE’s ProSe clock is not greater than the MAX\_OFFSET of the monitoring UE's ProSe clock.
7. On hearing such a discovery message, and if the UE has either not checked the MIC for the discovered ProSe App Code previously or has checked a MIC for the ProSe App Code and the associated Match Report refresh timer (see steps 14 and 15 for details of this timer) has expired, or as required based on the procedure specified in TS 23.304 [2], 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 App Code and MIC.5G DDNMF If a Match Report is not required, the Monitoring UE shall locally process the discovery message and the rest of the procedure is not performed.
8. The 5G DDNMF in the HPLMN of the monitoring UE passes the discovery message parameters including the ProSe App Code and MIC and associated counter parameter to the 5G DDNMF in the HPLMN of the announcing UE in the Match Report message.
9. The 5G DDNMF in the HPLMN of the announcing UE shall check the MIC is valid. The relevant Discovery Key is found using the ProSe App Code.
10. The 5G DDNMF in the HPLMN of the announcing UE shall acknowledge a successful check of the MIC to the 5G DDNMF in the HPLMN of the monitoring UE in the Match Report Ack message. The 5G DDNMF in the HPLMN of the announcing UE include a Match Report refresh timer in the Match Report Ack message. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe App Code.
11. The 5G DDNMF in the HPLMN of the monitoring UE acknowledges the MIC check result to the monitoring UE. The 5G DDNMF returns the parameter ProSe Application ID to the UE. 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 may optionally modify the received Match Report refresh timer based on local policy and then include the Match Report refresh timer in the message to the Monitoring UE.

#### 6.1.3.2 Restricted discovery

##### 6.1.3.2.1 General

The security for both models of restricted discovery is similar to that of open 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 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 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[x], 5G Prose introduced a new feature:

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

##### 6.1.3.2.2 Security flows

###### 6.1.3.2.2.1 Model A restricted discovery

The security procedure for Model A restricted discovery is described as follows:



**Figure 6.1.3.2.2.1-1: Model A restricted discovery security procedure**

Steps 1-4 refer to an Announcing UE.

1. Announcing UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to get the ProSe Code to announce and to get the associated security material.
2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server.
3. If the Announcing UE is roaming, the 5G DDNMFs in the HPLMN and VPLMN of the Announcing UE exchange Announce Auth.
4. The 5G DDNMF in the HPLMN of the Announcing UE returns the ProSe 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 Code and are stored with the ProSe 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 may include the PC5 security policies in the Discovery Response message.

NOTE: 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

1. The Monitoring UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to be allowed to monitor for one or more Restricted ProSe Application User IDs.
2. 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.
3. 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.
4. The 5G DDNMF in the HPLMN of the Monitoring UE may exchange authorization messages with the ProSe Application Server.
5. 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 Code, the corresponding Code-Receiving Security Parameters and an optional Discovery User Integrity Key (DUIK). 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 Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters).

The 5G DDNMF in the HPLMN of the Announcing UE may send the PC5 security policies to the 5G DDNMF in the HPLMN of the Monitoring UE.

NOTE 1: There are two configurations possible for integrity checking, namely, MIC checked by the 5G DDNMF, and MIC checked at the UE side. Which of the configuration is used is decided by the 5G DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

1. 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. 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 and Code-Receiving Security Parameters.

If the 5G DDNMF in the HPLMN of the Monitoring UE receives the PC5 security policies 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.

1. 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.
2. 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 2: 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.

1. If the UE has either not had the 5G DDNMF check the MIC for the discovered ProSe Code previously or the 5G DDNMF has checked a MIC for the ProSe 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 Code and MIC. The 5G DDNMF checks the MIC.
2. The 5G DDNMF in the HPLMN of the Monitoring UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Monitoring UE is authorised to discover the Announcing UE.
3. 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 Code.
4. 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 Model B restricted discovery

The security procedure for Model B restricted discovery is described as follows:



**Figure 6.1.3.2.2.2-1: Model B restricted discovery security procedure**

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.
2. The 5G DDNMF may check for the announce authorization with the ProSe Application Server depending on 5G DDNMF configuration.
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.
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) and their Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT\_TIME and MAX\_OFFSET parameters. 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 may include the PC5 security policies in the Discovery Response message.

NOTE: 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

1. The Discoverer UE sends a Discovery Request message containing the RPAUID to the 5G DDNMF in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application User IDs.
2. 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.
3. 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.
4. The 5G DDNMF in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.
5. 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, and an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code. 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 to the 5G DDNMF in the HPLMN of the Discoverer UE.

NOTE 1: There are two configurations possible for integrity checking, namely, MIC checked by the 5G DDNMF, and MIC checked at the UE side; this is decided by the 5G DDNMF that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

1. 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.
2. 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 and the Code-Sending Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters. 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.

If the 5G DDNMF in the HPLMN of the Discoverer UE receives the PC5 security policies 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.

1. 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.
2. 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 2: Match Reports are not used for the MIC checking of ProSe Query Codes.

1. 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.
2. 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 3: 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 4: 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.

1. 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.
2. The 5G DDNMF in the HPLMN of the Discoverer UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Discoverer UE is authorised to discover the Discoveree UE.
3. 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.
4. 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.

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

There are three types of security that are used to protect the restricted 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 [x].

Editor’s Note: it is for ffs whether security algorithms and/or process in clause 6.1.3.4.3 TS 33.303 can be applied without modification given the potentially different size of the discovery message in 5G ProSe.

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