**3GPP TSG-SA3 Meeting #106-e S3-220326**

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

**Source: Qualcomm Incorporated**

**Title: CR to ProSe TS – Update on the discovery protection mechanisms in Direct Discovery**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***This contribution proposes the texts for discovery message protection mechanisms 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

Based on the discussion on protection mechanisms for discovery messages in S3-220325, this contribution proposes to update the TS 33.503 [1] as in Section 4.

# 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 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 [4], 5G Prose introduced a new feature:

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

- Ciphering algorithms for message-specific confidentiality are configured at the UE during the Discovery Request procedure. The chosen ciphering algorithm is signalled during discovery.

**\*\*\*\*\* END OF 1st CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 2nd CHANGES \*\*\*\*\***

##### 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. 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.

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 shall include the chosen PC5 ciphering algorithms in the Discovery Response message.

 In addition, the 5G DDNMF in the HPLMN of the Announcing UE may include the PC5 security policies in the Discovery Response message.

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 Monitoring UE.

5. The Monitoring UE sends a Discovery Request message containing the RPAUID and 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.

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.

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.

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

9. 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, an optional Discovery User Integrity Key (DUIK), and a chosen PC5 ciphering algorithms. 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 2: 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.

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 algorithms. 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 algorithms.

 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.

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 including the chosen PC5 ciphering algorithm used to protect 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 using the signalled PC5 ciphering algorithm. 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.

**\*\*\*\*\* END OF 2nd CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 3rd CHANGES \*\*\*\*\***

###### 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. 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.

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), 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 algorithms in the Discovery Response message.

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

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 the 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.

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.

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.

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

9. 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 algorithms. 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 2: 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.

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.

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 algorithms. 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 algorithms.

 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.

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 including the chosen PC5 ciphering algorithm used to protect 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 using the signalled PC5 ciphering algorithm.

NOTE 3: 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 using the signalled PC5 ciphering algorithm in Step 12. 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 using the signalled PC5 ciphering algorithm in Step 12. 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 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.

NOTE 5: 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.

**\*\*\*\*\* END OF 3rd CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 4th CHANGES \*\*\*\*\***

##### 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 [4]. The protection mechanisms specified in TS 33.303 are reused with the following changes:

* Message-specific confidentiality mechanisms as specified in A.yy in the current specification.
* In A.5 of TS 33.303, the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the discovery message to be scrambled and set to Min (the length of discovery message – 16, 256).
* The time-hash-bitsequence is obtained as specified in A.zz in the current specification.
* In clause 6.1.3.4.3.2 of TS 33.303, MIC is set to a 32-bit random string if DUIK was not provisioned.

**\*\*\*\*\* END OF 4th CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 5th CHANGES \*\*\*\*\***

# A.yy Message-specific confidentiality mechanisms for discovery

Message-specific confidentiality protection is provided by ProSe layer between ProSe UEs.

The use and mode of operation of the 128-NEA algorithms are specified in Annex D in TS 33.501 [3].

The input parameters to the 128-NEA algorithms as described in Annex D in TS 33.501 are:

* KEY : 128 least significant bits of the output of the DUCK. KDF (DUCK, UTC-based counter, MIC)
* COUNT : UTC-based counter
* BEARER : 0x00
* DIRECTION : 0x00
* LENGTH : the length of the discovery message – length of Message Type, UTC based counter LSB and MIC.

KEY is set to as such to generate message-specific keystream as in TS 33.303 [4].

The output keystream of the ciphering algorithm (output\_keystream) is then masked with the Encrytped\_bits\_mask to produce the final keystream for the message-specific confidentiality protection (KEYSTREAM):

* KEYSTREAM = output\_keystream AND (Encrypted\_bits\_mask || 0xFF..FF) where the length of Encrypted\_bits\_mask is set to Min (the length of discovery message – 48 , 224).

The KEYSTREAM is XORed with the discovery message for message-specific confidentiality protection.

**\*\*\*\*\* END OF 5th CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 6th CHANGES \*\*\*\*\***

# A.zz Calculation of scrambling bits for discovery

When calculating the time-hash-bitsequence for discovery, the following parameters shall be used to form the input S to the KDF that is specified in Annex B of TS 33.220 [5]:

- FC = 0x4C

- P0 = UTC-based counter for scrambling associated with the discovery slot – see subclause 6.1.3.2.3.5.

- L0 = length of above (i.e. 0x00 0x04).

- P1 = message fragment index.

- L1 = length of the above (i.e., 0x00 0x02).

The input key shall be the 256-bit DUSK.

The time-hash-bitsequence is obtained as

a. time-hash-bitsequence = “”

b. For i = 0 to FLOOR((L+LMIC)/32)):

time-hash-bitsequence = time-hash-bitsequence || KDF (DUSK, UTC-based counter, i)

c. time-hash-bitsequence = time-hash-bitsequence || LSB(KDF (DUSK, UTC-based counter, FLOOR((L+LMIC)/32)) + 1), 8\*(L + LMIC - 32\* FLOOR((L+ LMIC)/32)) )

Where L is the length of the discovery message; LMIC is the length of the MIC, e.g., 4 bytes; || indicates concatenation; LSB(x,b) returns the b least significant bits of x; FLOOR(x) returns the largest integer less than or equal to x; and KDF() refers to a key derivation.

**\*\*\*\*\* END OF 6th CHANGES \*\*\*\*\***