**3GPP TSG-CT WG1 Meeting #133e-bisC1-220253**

**E-meeting, 17-21 January 2022**

**Source: Qualcomm**

**Title: Correction on security material encoding of discovery message**

**Spec: 3GPP TS 24.554**

**Agenda item: 17.2.18**

**Document for: Agreement**

**1. Reason for Change**

ProSe PC5 discovery message includes MIC and UTC-based counter LSB for security protection. These values should be placed in the last part of the message for security processing purpose. Several discovery messages in TS 24.554 are not aligned with it. In addition, optional value also needs to be security protected, so it should be encoded as ‘conditional’ value, and Composition parameters indicates the presence of conditional value.

**2. Proposal**

It is proposed to change direct discovery message encoding to make alignement in terms of place of MIC and UTC-based counter LSB. Optional value is changed to be encoded as conditional value with composition parameter.

Please note that Metadata parameter is under the ongoing SA3 disucssion how to apply security protection. It can be aligned once SA3 makes decision.

Please note that this pCR is based on TS 24.554 version 1.0.0.

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

### 10.2.1 Message definition

This message is sent by the UE over the PC5 interface for open 5G ProSe direct discovery and restricted 5G ProSe direct discovery. See table 10.2.1.1, table 10.2.1.2, table 10.2.1.3, table 10.2.1.4, table 10.2.1.5, table 10.2.1.6, table 10.2.1.7, table 10.2.1.8, table 10.2.1.9, table 10.2.1.10 and table 10.2.1.11.

Message type: PROSE PC5 DISCOVERY

Significance: dual

Direction: UE to peer UE

Editor's note: The IEs related to security are FFS and depend on SA3 requirements.

Editor's note: The condition of the optional IEs is FFS.

Table 10.2.1.1: PROSE PC5 DISCOVERY message content for open 5G ProSe direct discovery announcement

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | ProSe application code | ProSe application code11.2.2 | M | V | 23 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| xx | Metadata | Metadata11.2.x | O | TLV | x |
| NOTE: The discovery type is set to "Open discovery" and the content type is set to "Announcement". |

Table 10.2.1.2: PROSE PC5 DISCOVERY message content for restricted 5G ProSe direct discovery announcement

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | ProSe restricted code | ProSe restricted code11.2.3 | M | V | 23 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| xx | Metadata | Metadata11.2.x | O | TLV | x |
| NOTE: The discovery type is set to "Restricted discovery" and the content type is set to "Announcement". |

Table 10.2.1.3: PROSE PC5 DISCOVERY message content for restricted 5G ProSe direct discovery solicitation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | ProSe query code | ProSe restricted code11.2.3 | M | V | 23 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| xx | Metadata | Metadata11.2.x | O | TLV | x |
| NOTE: The discovery type is set to "Restricted discovery" and the content type is set to "Solicitation". |

Table 10.2.1.4: PROSE PC5 DISCOVERY message content for restricted 5G ProSe direct discovery response

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | ProSe response code | ProSe restricted code11.2.3 | M | V | 23 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| xx | Metadata | Metadata11.2.x | O | TLV | x |
| NOTE: The discovery type is set to "Restricted discovery" and the content type is set to "response". |

Table 10.2.1.5: PROSE PC5 DISCOVERY message for group member discovery announcement

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Application layer group ID | Application layer group ID11.2.6 | M | LV | 2-257 |
|  | Announcer info | User info ID11.2.7 | M | V | 6 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| NOTE: The discovery type is set to "Restricted discovery", the content type is set to "Group member discovery announcement/group member discovery response" and the discovery model is set to "Model A". |

Table 10.2.1.6: PROSE PC5 DISCOVERY message for group member discovery solicitation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE 1) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Application layer group ID | Application layer group ID11.2.6 | M | LV | 2-257 |
|  | Discoverer info | User info ID11.2.7 | M | V | 6 |
|  | GMDS composition | GMDS composition11.2.8 | M | V | 1 |
|  | Target user info | Target user info11.2.9 | C(NOTE 2) | V | 6 |
|  | Target group info | Target group info11.2.10 | C(NOTE 2) | V | 3 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| NOTE 1: The discovery type is set to "Restricted discovery", the content type is set to "Group member discovery solicitation" and the discovery model is set to "Model B".NOTE 2: Presence of the target user info and of target group info is indicated by the GMDS composition. |

Table 10.2.1.7: PROSE PC5 DISCOVERY message for group member discovery response

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Application layer group ID | Application layer group ID11.2.6 | M | LV | 2-257 |
|  | Discoveree info | User info ID11.2.7 | M | V | 6 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | Binary11.2.5 | M | V | 1 |
| NOTE: The discovery type is set to "Restricted discovery", the content type is set to "Group member discovery announcement/group member discovery response" and the discovery model is set to "Model B". |

Table 10.2.1.8: PROSE PC5 DISCOVERY message for UE-to-network relay discovery announcement

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE 1) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Announcer info | User info ID11.2.7 | M | V | 6 |
|  | Relay service code (NOTE 2) | Relay service code11.2.11 | M | V | 3 |
|  |  |  |  |  |  |
|  | Status indicator | Status indicator11.2.12 | M | V | 1 |
|  | U2NRDA Composition | U2NRDA Composition11.2.y | M | V | 1 |
| yy | NCGI | NCGI11.2.15(NOTE 3) | C | V | 8 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | UTC-based counter LSB 11.2.14 | M | V | 1 |
|  |  |  |  |  |  |
| NOTE 1: The discovery type is set to "Restricted discovery", the content type is set to "UE-to-network relay discovery announcement/UE-to-network relay discovery response" and the discovery model is set to "Model A".NOTE 2: If the announcing UE works as a 5G ProSe Layer-3 UE-to-network relay UE, the S-NSSAI associated with the relay service code belongs to the allowed NSSAI of the UE.NOTE 3: Presence of the NCGI is indicated by the U2NRDA Composition. |

Table 10.2.1.9: PROSE PC5 DISCOVERY message for UE-to-network relay discovery solicitation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Discoverer info | User info ID11.2.7 | M | V | 6 |
|  | Relay service code | Relay service code11.2.11 | M | V | 3 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | UTC-based counter LSB 11.2.14 | M | V | 1 |
| NOTE: The discovery type is set to "Restricted discovery", the content type is set to "UE-to-network relay discovery solicitation" and the discovery model is set to "Model B". |

Table 10.2.1.10: PROSE PC5 DISCOVERY message for UE-to-network relay discovery response

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE 1) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Discoveree info | User info ID11.2.7 | M | V | 6 |
|  | Relay service code (NOTE 2) | Relay service code11.2.11 | M | V | 3 |
|  |  |  |  |  |  |
|  | Status indicator | Status indicator11.2.12 | M | V | 1 |
|  | U2NRDR Composition | U2NRDR Composition11.2.z | M | V | 1 |
| yy | NCGI | NCGI11.2.15(NOTE 3) | C | V | 8 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | UTC-based counter LSB 11.2.14 | M | V | 1 |
|  |  |  |  |  |  |
| NOTE 1: The discovery type is set to "Restricted discovery", the content type is set to "UE-to-network relay discovery announcement/UE-to-network relay discovery response" and the discovery model is set to "Model B".NOTE 2: If the discoveree UE works as a 5G ProSe Layer-3 UE-to-network relay UE, the S-NSSAI associated with the relay service code belongs to the allowed NSSAI of the UE.NOTE 3: Presence of the NCGI is indicated by the U2NRDR Composition. |

Table 10.2.1.11: PROSE PC5 DISCOVERY message for relay discovery additional information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | ProSe direct discovery PC5 message type (NOTE) | ProSe direct discovery PC5 message type11.2.1 | M | V | 1 |
|  | Relay service code | Relay service code11.2.11 | M | V | 3 |
|  | Announcer info | User info ID11.2.7 | M | V | 1 |
|  | RDAI Composition | RDAI Composition11.2.aa | M | V | 1 |
| yy | NCGI | NCGI11.2.15(NOTE 2) | C | V | 8 |
| xx | Relay TAI | TAI11.2.13(NOTE 2) | C | V | 3 |
|  | MIC | MIC11.2.4 | M | V | 4 |
|  | UTC-based counter LSB | UTC-based counter LSB 11.2.14 | M | V | 1 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| NOTE 1: The discovery type is set to "Restricted discovery", the content type is set to "Relay discovery additional information" and the discovery model is set to "Model A".NOTE 2: Presence of the NCGI and Relay TAI is indicated by the RDAI Composition. |

\*\*\* second change \*\*\*

### 11.2.y U2NRDA Composition

This parameter is used to indicate the content of the PC5\_DISCOVERY message for UE-to-network relay discovery announcement.

This parameter is coded as shown in figure 11.2.y.1 and table 11.2.y.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NCGII | Spare | octet 1 |

Figure 11.2.y.1: U2NRDA Composition parameter

Table 11.2.y.1: U2NRDA Composition parameter

|  |
| --- |
| NCGI indication (NCGII) (octet 1) |
| Bit |
| 8 |  |  |  |  |
| 0 |  |  |  | NCGI is not included |
| 1 |  |  |  | NCGI is included |
|  |
| Bits 1 to 7 of octet 1 are spare and shall be coded as zero. |

\*\*\* third change \*\*\*

### 11.2.z U2NRDR Composition

This parameter is used to indicate the content of the PC5\_DISCOVERY message for UE-to-network relay discovery response.

This parameter is coded as shown in figure 11.2.z.1 and table 11.2.z.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NCGII | Spare | octet 1 |

Figure 11.2.z.1: U2NRDR Composition parameter

Table 11.2.z.1: U2NRDR Composition parameter

|  |
| --- |
| NCGI indication (NCGII) (octet 1) |
| Bit |
| 8 |  |  |  |  |
| 0 |  |  |  | NCGI is not included |
| 1 |  |  |  | NCGI is included |
|  |
| Bits 1 to 7 of octet 1 are spare and shall be coded as zero. |

\*\*\* last change \*\*\*

### 11.2.aa RDAI Composition

This parameter is used to indicate the content of the PC5\_DISCOVERY message for relay discovery additional information.

This parameter is coded as shown in figure 11.2.aa.1 and table 11.2.aa.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NCGII | RTAII | Spare | octet 1 |

Figure 11.2.aa.1: RDAI Composition IE parameter

Table 11.2.aa.1: RDAI Composition parameter

|  |
| --- |
| NCGI indication (NCGII) (octet 1) |
| Bit |
| 8 |  |  |  |  |
| 0 |  |  |  | NCGI is not included |
| 1 |  |  |  | NCGI is included |
|  |
| Relay TAI indication (RTAII) (octet 1) |
| Bit |
| 7 |  |  |  |  |
| 0 |  |  |  | Relay TAI is not included |
| 1 |  |  |  | Relay TAI is included |
| Bits 1 to 6 of octet 1 are spare and shall be coded as zero. |