**3GPP TSG-CT WG1 Meeting CT1#137-eC1-224617**

**E-Meeting, 18th - 26th August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.554** | **CR** | **0124** | **rev** | **-** | **Current version:** | **17.1.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Security protection on establishment request message for relay |
|  |  |
| ***Source to WG:*** | OPPO |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-7-7 |
|  |  |  |  |  |
| ***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 canbe 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:*** | As defined in TS 33.503, for U2N relay case, the PROSE DIRECT LINK ESTABLISHMENT REQUEST message should be integrity protected and the RSC and PRUK ID in this message should be ciphered by using the security parameters applied to the discovery message.In AS layers, the PC5 SRB 0 is used to carry the PROSE DIRECT LINK ESTABLISHMENT REQUEST message without security functionality in the PDCP layer, as same as the eV2X.**Observation 1: the security protection on the PROSE DIRECT LINK ESTABLISHMENT REQUEST message cannot be done at PDCP layer.**Actually, the discovery messages face the same situation, i.e. the security protection is done at ProSe layer and cannot be done at PDCP layer.So, the security protection on the PROSE DIRECT LINK ESTABLISHMENT REQUEST message should be done also at ProSe layer.**Proposal 1: the security protection on the PROSE DIRECT LINK ESTABLISHMENT REQUEST message is performed at ProSe layer.**Otherwise, SRB 1, same with SMC, is used to send PROSE DIRECT LINK ESTABLISHMENT REQUEST message then many RAN2 impacts can be expected. A LS to RAN2 is also needed to make them change their spec although R17 has been frozen.Although, right now, there is the following requirement in 24.554:*If the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, then the UE shall apply the DUIK, DUSK, or DUCK with the associated encrypted bitmask used for UE-to-network relay discovery along with the UTC-based counter for security protection of the relay service code and the 5G PRUK ID, if available, (see clause 6.3.5.2 of 3GPP TS 33.503 [34]) and the UE shall use the security protected relay service code or the security protected 5G PRUK ID for creating a PROSE DIRECT LINK ESTABLISHMENT REQUEST message.*The MIC IE is missing in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message.**Proposal 2: the MIC IE should be added to the PROSE DIRECT LINK ESTABLISHMENT REQUEST message.**To satisfy the cipher protection of these 2 IEs, if we think about the intial NAS message which includes the non-cleartext IEs without ciphering the whole initial NAS message, the non-cleartext IEs are put into the NAS message container and this NAS message container is ciphered.The similar mechamism should also applied to the PROSE DIRECT LINK ESTABLISHMENT REQUEST message.Note that if the SUCI is used as the UE identity, there is no need to cipher the SUCI based on TS 33.503.**Proposal 3: the RSC and PRUK ID are put into a ciphered container.** |
|  |  |
| ***Summary of change:*** | Add MIC IE and put the RSC and 5G PRUK ID into a ciphered container in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message. |
|  |  |
| ***Consequences if not approved:*** | Not align with stage 2 requirement. |
|  |  |
| ***Clauses affected:*** | 7.2.2.2, 7.2.2.3, 10.3.1.1, 10.3.1.7, 10.3.1.10, 10.3.1.a(new), 11.3.y(new), 11.3.z(new) |
|  |  |
|  | **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 \*\*\*\*\*

#### 7.2.2.2 5G ProSe direct link establishment procedure initiation by initiating UE

The initiating UE shall meet the following pre-conditions before initiating this procedure:

a) a request from upper layers to transmit the packet for ProSe application over PC5;

b) the communication mode is unicast mode (e.g., pre-configured as specified in clause 5.2.4 or indicated by upper layers);

c) the link layer identifier for the initiating UE (i.e., layer-2 ID used for unicast communication) is available (e.g., pre-configured or self-assigned) and is not being used by other existing 5G ProSe direct links within the initiating UE;

d) the link layer identifier for the destination UE (i.e., the unicast layer-2 ID of the target UE or the broadcast layer-2 ID) is available to the initiating UE (e.g., pre-configured, obtained as specified in clause 5.2 or known via prior ProSe direct communication);

NOTE 1: In the case where different ProSe applications are mapped to distinct default destination layer-2 IDs, when the initiating UE intends to establish a single unicast link that can be used for more than one ProSe identifiers, the UE can select any of the default destination layer-2 ID for unicast initial signalling.

e) the initiating UE is either authorised for 5G ProSe direct communication over PC5 in NR-PC5 in the serving PLMN, has a valid authorization for 5G ProSe direct communication over PC5 in NR-PC5 when not served by NG-RAN, or is authorized to use a 5G ProSe UE-to-network relay UE. The UE considers that it is not served by NG-RAN if the following conditions are met:

1) not served by NG-RAN for ProSe direct communication over PC5;

2) in limited service state as specified in 3GPP TS 23.122 [14], if the reason for the UE being in limited service state is one of the following;

i) the UE is unable to find a suitable cell in the selected PLMN as specified in 3GPP TS 38.304 [15];

ii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #11 "PLMN not allowed" as specified in 3GPP TS 24.501 [11]; or

iii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #7 "5GS services not allowed" as specified in 3GPP TS 24.501 [11]; or

3) in limited service state as specified in 3GPP TS 23.122 [14] for reasons other than i), ii) or iii) above and located in a geographical area for which the UE is provisioned with "non-operator managed" radio parameters as specified in clause 5.2;

f) there is no existing 5G ProSe direct link for the pair of peer application layer IDs, or there is an existing 5G ProSe direct link for the pair of peer application layer IDs and:

1) the network layer protocol of the existing 5G ProSe direct link is not identical to the network layer protocol required by the upper layer in the initiating UE for this ProSe application;

2) the security policy (either signalling security policy or user plane security policy) corresponding to the ProSe identifier is not compatible with the security policy of the existing 5G ProSe direct link; or

3) in case of the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, the existing 5G ProSe direct link for the peer UE is established with a different RSC or without an RSC;

g) the number of established 5G ProSe direct links is less than the implementation-specific maximum number of established 5G ProSe direct links allowed in the UE at a time; and

h) timer T5088 is not associated with the link layer identifier for the destination UE or timer T5088 associated with the link layer identifier for the destination UE has already expired or stopped.

After receiving the service data or request from the upper layers, the initiating UE shall derive the PC5 QoS parameters and assign the PQFI(s) for the PC5 QoS flows(s) to be established as specified in clause 7.2.7.

In order to initiate the 5G ProSe direct link establishment procedure, the initiating UE shall create a PROSE DIRECT LINK ESTABLISHMENT REQUEST message. The initiating UE:

a) shall include the source user info set to the initiating UE's application layer ID received from upper layers;

b) shall include the ProSe identifier(s) received from upper layer if the 5G ProSe direct link establishment procedure is not for 5G ProSe direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE;

c) shall include the target user info set to the target UE's application layer ID if received from upper layers, or to the identity of the 5G ProSe UE-to-network relay UE obtained during the 5G ProSe UE-to-network relay discovery procedure, or if the destination layer-2 ID is the unicast layer-2 ID of target UE;

d) if the 5G ProSe direct link is not for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE:

1) shall include the key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred" and may include the key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection not needed";

NOTE 2: The key establishment information container is provided by upper layers.

e) shall include:

1) a Nonce\_1, if the direct communication is not between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, or if the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the security procedure over control plane is used as specified in 3GPP TS 33.503 [34]; or

2) a KNRP freshness parameter 1, if the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the security procedure over user plane is used as specified in 3GPP TS 33.503 [34];

 set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this 5G ProSe direct link if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred";

NOTE 3: The Nonce\_1 IE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message is used to hold the value of Nonce\_1 or KNRP freshness parameter 1.

f) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the security establishment of this 5G ProSe direct link;

g) shall include theMSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.503 [34] if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred";

h) may include a KNRP ID if the initiating UE has an existing KNRP for the target UE;

i) shall include its UE PC5 unicast signalling security policy. In the case where the different ProSe applications are mapped to the different PC5 unicast signalling security policies, when the initiating UE intends to establish a single unicast link that can be used for more than one ProSe application, each of the signalling security polices of those ProSe applications shall be compatible, e.g., "Signalling integrity protection not needed" and "Signalling integrity protection required" are not compatible. In case the 5G ProSe direct link establishment procedure is for direct communication between 5G ProSe remote UE and 5G ProSe UE-to-network relay UE, the Signalling integrity protection policy shall be set to "Signalling integrity protection required";

j) shall include the MIC IE set to the calculated MIC value as specified in clause 6.3.5.3 of 3GPP TS 33.503 [34] if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the UE has the DUIK;

k) shall include the UTC-based counter LSB set to the four least significant bits of the UTC-based counter if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE;

l) shall include the Ciphered IE container IE whose value part is security protected by using the DUSK or DUCK with the associated encrypted bitmask used for 5G ProSe UE-to-network relay discovery along with the UTC-based counter for security protection of the relay service code and the 5G PRUK ID, if available, (see clause 6.3.5.2 of 3GPP TS 33.503 [34]) if the the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the Ciphered IE container IE includes:

1) the relay service code of the target relay UE; or

2) the PRUK ID of the initiating UE if:

i) the initiating UE have a valid PRUK; and

ii) the security for 5G ProSe UE-to-network relay uses the security procedure over user plane as specified in 3GPP TS 33.503 [34]; and

l) shall include the UE identity IE set to the SUCI of the initiating UE if:

1) the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE; and

2) the security for 5G ProSe UE-to-network relay uses the security procedure over control plane as specified in 3GPP TS 33.503 [34], or, the security for 5G ProSe UE-to-network relay uses the security procedure over user plane and the initiating UE does not have a valid PRUK as specified in 3GPP TS 33.503 [34]; and

n) shall include the HPLMN ID of the initiating UE, if the PRUK ID of the initiating UE does not contain the HPLMN ID of the initiating UE or the routing information to the 5G PKMF of the initiating UE.

Editor's note: It is FFS how the UE determines whether the security for 5G ProSe layer-3 relay uses the security procedure over control plane or the security procedure over user plane as specified in 3GPP TS 33.503 [34].

After the PROSE DIRECT LINK ESTABLISHMENT REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the source layer-2 ID and destination layer-2 ID as follows:

a) if the 5G ProSe direct communication is in a consequence of 5G ProSe direct discovery as defined in clause 6.2.14, clause 6.2.15, and clause 8.2.1:

 self-assign a source layer-2 ID, and the destination layer-2 ID set to the source layer-2 ID in the received PROSE PC5 DISCOVERY message for discovery procedure; or

b) otherwise:

 self-assign a source layer-2 ID, and the destination layer-2 ID set to the destination layer-2 ID used for unicast initial signalling as specified in clause 5.2.4,

NOTE 4: The UE implementation ensures that any value of the self-assigned source layer-2 ID in a) and b) is different from any other self-assigned source layer-2 ID(s) in use for 5G ProSe direct discovery as specified in clause 6.2.14, clause 6.2.15 and clause 8.2.1, and is different from any other provisioned destination layer-2 ID(s) as specified in clause 5.2.

NOTE 5: It is possible for the initiating UE to reuse the initiating UE's layer-2 ID used in previous 5G ProSe direct link with the same peer UE.

and start timer T5080.

NOTE 6: A default PC5 DRX configuration is used for transmitting this message as specified in 3GPP TS 38.300 [21].

The UE shall not send a new PROSE DIRECT LINK ESTABLISHMENT REQUEST message to the same target UE identified by the same application layer ID while timer T5080 is running. If the target user info IE is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message (i.e., ProSe application oriented 5G ProSe direct link establishment procedure), the initiating UE shall handle multiple PROSE DIRECT LINK ESTABLISHMENT ACCEPT messages, if any, received from different target UEs for the establishment of multiple 5G ProSe direct links before the expiry of timer T5080.

NOTE 7: In order to ensure successful 5G ProSe direct link establishment, T5080 should be set to a value larger than the sum of T5089 and T5092.



Figure 7.2.2.2.1: UE oriented 5G ProSe direct link establishment procedure



Figure 7.2.2.2.2: ProSe service oriented 5G ProSe direct link establishment procedure

\*\*\*\*\* Next change \*\*\*\*\*

#### 7.2.2.3 5G ProSe direct link establishment procedure accepted by the target UE

Upon receipt of a PROSE DIRECT LINK ESTABLISHMENT REQUEST message, if the target UE accepts this request, the target UE shall uniquely assign a PC5 link identifier, create a 5G ProSe direct link context.

If the PROSE DIRECT LINK ESTABLISHMENT REQUEST message is for 5G ProSe direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, the target UE decrypts the encrypted the Ciphered IE container IE including the relay service code and 5G PRUK ID, if received, using the DUIK, DUSK, or DUCK with the associated encrypted bitmask used for 5G ProSe UE-to-network relay discovery and verifies if the relay service code matches with the one that the target UE has sent during 5G ProSe UE-to-network relay discovery procedure.

If the 5G ProSe direct link establishment procedure is not for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, the target UE may initiate 5G ProSe direct link authentication procedure as specified in clause 7.2.12 and shall initiate 5G ProSe direct link security mode control procedure as specified in clause 7.2.10.

If the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, the target UE shall proceed with either the security procedure over control plane or the security procedure over user plane as specified in 3GPP TS 33.503 [34].

The target UE shall set the source layer-2 ID and the destination layer-2 ID as specified in clause 7.2.12 and clause 7.2.10, and store the corresponding source layer-2 ID for unicast communication and the destination layer-2 ID for unicast communication in the 5G ProSe direct link context.

If:

a) the target user info IE is included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message and this IE includes the target UE's application layer ID; or

b) the target user info IE is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message and the target UE is interested in the ProSe application(s) identified by the ProSe identifier IE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message;

then the target UE shall either:

a) identify an existing KNRP based on the KNRP ID included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; or

b) if KNRP ID is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message, the target UE does not have an existing KNRP for the KNRP ID included in PROSE DIRECT LINK ESTABLISHMENT REQUEST message or the target UE wishes to derive a new KNRP, derive a new KNRP. This may require performing one or more 5G ProSe direct link authentication procedures as specified in clause 7.2.12.

NOTE 1: How many times the 5G ProSe direct link authentication procedure needs to be performed to derive a new KNRP depends on the authentication method used.

After an existing KNRP was identified or a new KNRP was derived, the target UE shall initiate a 5G ProSe direct link security mode control procedure as specified in clause 7.2.10.

Upon successful completion of the 5G ProSe direct link security mode control procedure, in order to determine whether the PROSE DIRECT LINK ESTABLISHMENT REQUEST message can be accepted or not, in case of IP communication, the target UE checks whether there is at least one common IP address configuration option supported by both the initiating UE and the target UE.

Before sending the PROSE DIRECT LINK ESTABLISHMENT ACCEPT message to the 5G ProSe remote UE, the target UE acting as a 5G ProSe layer-3 UE-to-network relay UE shall inform the lower layer to initiate the UE requested PDU session establishment procedure as specified in 3GPP TS 24.501 [11] if:

1) the PDU session for relaying the service associated with the RSC has not been established yet; or

2) the PDU session for relaying the service associated with the RSC has been established but the PDU session type is Unstructured.

If the target UE accepts the 5G ProSe direct link establishment procedure, the target UE shall create a PROSE DIRECT LINK ESTABLISHMENT ACCEPT message. The target UE:

a) shall include the source user info set to the target UE's application layer ID received from upper layers;

b) shall include PQFI(s), the corresponding PC5 QoS parameters and optionally the ProSe identifier(s) that the target UE accepts, if the target UE is not acting as a 5G ProSe layer-2 UE-to-network relay UE;

c) may include the PC5 QoS rule(s) if the target UE is not acting as a 5G ProSe layer-2 UE-to-network relay UE;

d) shall include an IP address configuration IE set to one of the following values if IP communication is used and the target UE is not acting as a 5G ProSe layer-2 UE-to-network relay UE:

1) "DHCPv4 server" if only IPv4 address allocation mechanism is supported by the target UE, i.e., acting as a DHCPv4 server; or

2) "IPv6 router" if only IPv6 address allocation mechanism is supported by the target UE, i.e., acting as an IPv6 router; or

3) "DHCPv4 server & IPv6 Router" if both IPv4 and IPv6 address allocation mechanism are supported by the target UE; or

4) "address allocation not supported" if neither IPv4 nor IPv6 address allocation mechanism is supported by the target UE and the target UE is not acting as a 5G ProSe layer-3 UE-to-network relay UE;

NOTE 2: The UE doesn't include an IP address configuration IE nor a link local IPv6 address IE, if Ethernet or Unstructured data unit type is used for communication.

e) shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [16] if IP address configuration IE is set to "address allocation not supported", the received PROSE DIRECT LINK SECURITY MODE COMPLETE message included a link local IPv6 address IE and the target UE is neither acting as a 5G ProSe layer-2 UE-to-network relay UE nor acting as a 5G ProSe layer-3 relay UE; and

f) shall include the configuration of UE PC5 unicast user plane security protection based on the agreed user plane security policy, as specified in 3GPP TS 33.503 [34].

After the PROSE DIRECT LINK ESTABLISHMENT ACCEPT message is generated, the target UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication and shall start timer T5090 if at least one of ProSe identifiers for the 5G ProSe direct links satisfies the privacy requirements as specified in clause 5.2.4 and clause 5.2.5.

NOTE 3: Two UEs negotiate the PC5 DRX configuration in the AS layer, and the PC5 DRX parameter values are configured per pair of source and destination Layer-2 IDs in the AS layer, as specified in 3GPP TS 38.300 [21].

After sending the PROSE DIRECT LINK ESTABLISHMENT ACCEPT message, the target UE shall provide the following information along with the layer-2 IDs to the lower layer, which enables the lower layer to handle the coming PC5 signalling or traffic data:

a) the PC5 link identifier self-assigned for this 5G ProSe direct link;

b) PQFI(s) and its corresponding PC5 QoS parameters, if available; and

c) an indication of activation of the PC5 unicast user plane security protection for the 5G ProSe direct link, if applicable.

If the target UE accepts the 5G ProSe direct link establishment request and the 5G ProSe direct link is established not for 5G ProSe direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, then the target UE may perform the PC5 QoS flow establishment over 5G ProSe direct link as specified in clause 7.2.7. If the 5G ProSe direct link is established for 5G ProSe direct communication between the 5G ProSe layer-3 remote UE and the 5G ProSe layer-3 UE-to-network relay UE, then the target UE may perform the PC5 QoS flow establishment over 5G ProSe direct link as specified in clause 8.2.6.

\*\*\*\*\* Next change \*\*\*\*\*

#### 10.3.1.1 Message definition

This message is sent by a UE to another peer UE to establish a direct link. See table 10.3.1.1.1.

Message type: PROSE DIRECT LINK ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to peer UE

Table 10.3.1.1.1: PROSE DIRECT LINK ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PROSE DIRECT LINK ESTABLISHMENT REQUEST message identity | ProSe PC5 signalling message type11.3.1 | M | V | 1 |
|  | Sequence number | Sequence number11.3.2 | M | V | 1 |
|  | Source user info | Application layer ID11.3.4 | M | LV | 2-256 |
|  | UE security capabilities | UE security capabilities11.3.11 | M | LV | 3-9 |
|  | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy11.3.12 | M | V | 1 |
| 7B | ProSe identifiers | ProSe identifier11.3.3 | O | TLV-E | 21-65538 |
| 74 | Key establishment information container | Key establishment information container11.3.9 | O | TLV-E | 4-65538 |
| 56 | Nonce\_1 | Nonce11.3.10 | O | TV | 17 |
| 5C | MSB of KNRP-sess ID | MSB of KNRP-sess ID11.3.13 | O | TV | 2 |
| 28 | Target user info | Application layer ID11.3.4 | O | TLV | 3-257 |
| 58 | KNRP ID | KNRP ID11.3.14 | O | TV | 5 |
|  |  |  |  |  |  |
| TBD | Ciphered IE container | Ciphered IE container11.3.z | O | TLV | 3-n |
| 7D | UE identity | 5GS mobile identity11.3.30 | O | TLV-E | 4-n |
|  |  |  |  |  |  |
| 2A | HPLMN ID | PLMN ID11.3.33 | O | TV | 2 |
| 2B | UTC-based counter LSB | UTC-based counter LSB11.2.11 | O | TV | 2 |
| TBD | MIC | MIC11.3.y | O | TV | 5 |

\*\*\*\*\* Next change \*\*\*\*\*

#### 10.3.1.7 Void

\*\*\*\*\* Next change \*\*\*\*\*

#### 10.3.1.10 Ciphered IE container

The UE shall include this IE if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the relay service code and/or the PRUK ID shall be ciphered.

\*\*\*\*\* Next change \*\*\*\*\*

#### 10.3.1.a MIC

The UE shall include this IE if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE and the UE has the DUIK.

\*\*\*\*\* Next change \*\*\*\*\*

### 11.3.y MIC

This parameter is used to carry the MIC value for integrity protection of the PROSE DIRECT LINK ESTABLISHMENT REQUEST message.

The MIC IE is a type 3 information element with a length of 5 octets.

### 11.3.z Ciphered IE container

This parameter is used to contain the ciphered relay service code and PRUK ID.

The Ciphered IE container IE is a type 4 information element with a minimum length of 3 octets.

The Ciphered IE container information element is coded as shown in figure 11.3.z.1 and table 11.3.z.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Ciphered IE container IEI | octet 1 |
| Length of Ciphered IE container IE | octet 2 |
| Relay service code | octet 3octet 5 |
| PRUK ID | octet 6\*octet n\* |

Figure 11.3.z.1: Ciphered IE container information element

Table 11.3.z.1: Ciphered IE container information element

|  |
| --- |
| Relay service code (octet 3 to 5)The relay service code field contains the 24-bit relay service code. |
| PRUK ID (octet 6 to n)The PRUK ID field is defined as the length and value part of Figure 11.3.32.1 and Table 11.3.32.1. |
|  |

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