**3GPP TSG-CT WG1 Meeting #136-eC1-22xxxx**

**E-Meeting, 12th – 20th May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.554** | **CR** | **0096** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | Applicability of Key establishment information container IE to the security of the UE-to-network relay |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, OPPO |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-05-03 |
|  |  |  |  |  |
| ***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:*** | The Key establishment information container IE is used for authenticating the UE with the peer UE, and also for deriving the KNRP, as described for the 5G ProSe direct link authentication procedure and the 5G ProSe direct link security mode control procedure in TS 24.554, for the non-relaying case.However, that IE is not applicable for the security of the 5G ProSe UE-to-network relay, because the security of the 5G ProSe UE-to-network relay follow either the control plane solution or the user plane solution described in TS 33.503, where both solutions don't require the Key establishment information container IE.Hence it is needed to clarify that, the Key establishment information container IE is not applicable for UE-to-network relay, and is applicable only in the non-relay cases. |
|  |  |
| ***Summary of change:*** | Specifying in the relevant clauses that, the Key establishment information container IE is not applicable for UE-to-network relay, and is applicable only in the non-relay cases.Note: No change is done in the clauses of the 5G ProSe direct link authentication procedure because it is already stated there that the whole 5G ProSe direct link authentication procedure is not applicable for UE-to-network relay case. |
|  |  |
| ***Consequences if not approved:*** | Wrong specification which specifies that, Key establishment information container IE is used for any case (relay or non-relay) which is not correct. |
|  |  |
| ***Clauses affected:*** | 7.2.2.2, 7.2.10.2, 7.2.11.2, 10.3.1.3, 10.3.13.4, 10.3.16.2 |
|  |  |
|  | **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 remote UE and the 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 remote UE and the 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 a Nonce\_1 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";

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 the most significant 8 bits (MSB) 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 layer-3 remote UE and 5G ProSe layer-3 UE-to-network relay UE, the Signalling integrity protection policy shall be set to "Signalling integrity protection required";

j) shall include the Relay service code IE set to the relay service code of the target relay UE 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

h) 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 layer-3 remote UE and the 5G ProSe layer-3 UE-to-network relay UE; and

2) the security for 5G ProSe layer-3 relay use the security procedure over control plane as specified in 3GPP TS 33.503 [34].

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 initiating UE's layer-2 ID for unicast communication and:

a) the destination layer-2 ID used for unicast initial signalling; or

b) the destination layer-2 ID set to the source layer-2 ID of the selected 5G ProSe UE-to-network relay UE during the 5G ProSe UE-to-network relay discovery procedure as defined in clause 8.2.1;

and start timer T5080.

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 3: 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 \*\*\*\*\*

#### 7.2.10.2 5G ProSe direct link security mode control procedure initiation by the initiating UE

The initiating UE shall meet the following pre-conditions before initiating the 5G ProSe direct link security mode control procedure:

a) the target UE has initiated a 5G ProSe direct link establishment procedure toward the initiating UE by sending a PROSE DIRECT LINK ESTABLISHMENT REQUEST message and:

1) the PROSE DIRECT LINK ESTABLISHMENT REQUEST message:

i) includes a target user info IE which includes the application layer ID of the initiating UE; or

ii) does not include a target user info IE and the initiating UE is interested in the ProSe service identified by the ProSe identifier in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; and

2) the initiating UE:

i) has either identified an existing KNRP based on the KNRP ID included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or derived a new KNRP; or

ii) has decided not to activate security protection based on its UE 5G ProSe direct signalling security policy and the target UE's 5G ProSe direct signalling security policy; or

b) the target UE has initiated a 5G ProSe direct link re-keying procedure toward the initiating UE by sending a PROSE DIRECT LINK REKEYING REQUEST message and:

1) if the target UE has included a Re-authentication indication in the PROSE DIRECT LINK REKEYING REQUEST message, the initiating UE has derived a new KNRP.

If a new KNRP has been derived by the initiating UE, the initiating UE shall generate the 2 MSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the initiating UE.

The initiating UE shall select security algorithms in accordance with its UE 5G ProSe direct signalling security policy and the target UE's 5G ProSe direct signalling security policy. If the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure, the initiating UE shall not select the null integrity protection algorithm if the initiating UE or the target UE's 5G ProSe direct signalling integrity protection policy is set to "Signalling integrity protection required". If the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link re-keying procedure, the initiating UE:

a) shall not select the null integrity protection algorithm if the integrity protection algorithm currently in use for the 5G ProSe direct link is different from the null integrity protection algorithm;

b) shall not select the null ciphering protection algorithm if the ciphering protection algorithm currently in use for the 5G ProSe direct link is different from the null ciphering protection algorithm;

c) shall select the null integrity protection algorithm if the integrity protection algorithm currently in use is the null integrity protection algorithm; and

d) shall select the null ciphering protection algorithm if the ciphering protection algorithm currently in use is the null ciphering protection algorithm.

Then the initiating UE shall:

a) generate a 128-bit Nonce\_2 value;

b) derive KNRP-sess from KNRP, Nonce\_2 and Nonce\_1 received in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.536 [37];

c) derive the NR PC5 encryption key NRPEK and the NR PC5 integrity key NRPIK from KNRP-sess and the selected security algorithms as specified in 3GPP TS 33.536 [37], and

d) create a PROSE DIRECT LINK SECURITY MODE COMMAND message. In this message, the initiating UE:

1) shall include the key establishment information container IE 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 and a new KNRP has been derived at the initiating UE and the authentication method used to generate KNRP requires sending information to complete the 5G ProSe direct link authentication procedure;

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

2) shall include the MSB of KNRP ID IE if a new KNRP has been derived at the initiating UE;

3) shall include a Nonce\_2 IE 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 selected integrity protection algorithm is not the null integrity protection algorithm;

4) shall include the selected security algorithms;

5) shall include the UE security capabilities received from the target UE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or PROSE DIRECT LINK REKEYING REQUEST message;

6) shall include the UE 5G ProSe direct signalling security policy received from the target UE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; and

7) shall include the LSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [37] if the selected integrity protection algorithm is not the null integrity protection algorithm.

If the security protection of this 5G ProSe direct link is activated, the initiating UE shall form the KNRP-sess ID from the MSB of KNRP-sess ID received in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or PROSE DIRECT LINK REKEYING REQUEST message and the LSB of KNRP-sess ID included in the PROSE DIRECT LINK SECURITY MODE COMMAND message. The initiating UE shall use the KNRP-sess ID to identify the new security context.

After the PROSE DIRECT LINK SECURITY MODE COMMAND message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for 5G ProSe direct communication and the target UE's layer-2 ID for 5G ProSe direct communication, NRPIK, NRPEK if applicable, KNRP-sess ID, the selected security algorithm as specified in TS 33.536 [37]; an indication of activation of the 5G ProSe direct signalling security protection for the 5G ProSe direct link with the new security context, if applicable, and start timer T5089. The initiating UE shall not send a new PROSE DIRECT LINK SECURITY MODE COMMAND message to the same target UE while timer T5089 is running.

NOTE: The PROSE DIRECT LINK SECURITY MODE COMMAND message is integrity protected (and not ciphered) at the lower layer using the new security context.

If the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link re-keying procedure, the initiating UE shall provide to the lower layers an indication of activation of the 5G ProSe direct user plane security protection for the 5G ProSe direct link with the new security context, if applicable, along with the initiating UE's layer-2 ID for 5G ProSe direct communication and the target UE's layer-2 ID for 5G ProSe direct communication.



Figure 7.2.10.2.1: 5G ProSe direct link security mode control procedure

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

#### 7.2.11.2 5G ProSe direct link re-keying procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the 5G ProSe direct link re-keying procedure:

a) there is a 5G ProSe direct link between the initiating UE and the target UE; and

1) if the session key KNRP-sess used to protect 5G ProSe direct link needs to be refreshed and neither timer T5089 nor T5091 are running;

2) if the UE wants to refresh KNRP and neither timer T5089 nor T5091 are running; or

3) if the lower layers indicate that a 5G ProSe direct link re-keying procedure needs to be performed.

In order to initiate the 5G ProSe direct link re-keying procedure, the initiating UE shall create a PROSE DIRECT LINK REKEYING REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container IE 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 and the null integrity protection algorithm is not in use;

NOTE 1: The key establishment information container is provided by upper layers.

b) shall include a Nonce\_1 IE set to the 128-bit nonce value generated by the initiating UE for the purpose of session key refresh over this 5G ProSe direct link if the null integrity protection algorithm is not in use;

c) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the re-keying of this 5G ProSe direct link;

d) shall include the MSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.503 [34] if the null integrity protection algorithm is not in use; and

e) may include a Re-authentication indication if the initiating UE wants to derive a new KNRP.

After the PROSE DIRECT LINK REKEYING REQUEST message is generated, the initiating 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 start timer T5091. The UE shall not send a new PROSE DIRECT LINK REKEYING REQUEST message to the same target UE while timer T5091 is running.

NOTE 2: In order to ensure successful 5G ProSe direct link re-keying, T5091 should be set to a value larger than the sum of T5092 and T5089.



Figure 7.2.11.2.1: 5G ProSe direct link re-keying procedure

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

#### 10.3.1.3 Key establishment information container

The UE shall include this IE if the UE PC5 unicast signalling security policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred", and 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.

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

#### 10.3.13.4 Key establishment information container

The UE shall include this IE if the UE has derived a new KNRP and the authentication method used to generate KNRP requires sending information to complete the authentication procedure, and 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.

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

#### 10.3.16.2 Key establishment information container

The UE shall include this IE if the null integrity protection algorithm is not in use, and 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.

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