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

**E-Meeting, 12th – 20th May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.554** | **CR** | **0065** | **rev** | **3** | **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:*** | Resolving the EN related to possible changes to the 5G ProSe direct link security mode control procedure due to the security requirements of UE-to-network relay | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson, InterDigital | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2022-04-29 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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 can be 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 following EN:  Editor's note: Any possible changes to the 5G ProSe direct link security mode control procedure due to the security requirements of 5G ProSe layer-2 UE-to-network relay and 5G ProSe layer-3 UE-to-network relay are FFS and waiting for SA3 conclusion.  can now be resolved, where the requirements for the control plane security solution and the user security plane solution for UE-to-network relay have been clarified by SA3 in TS 33.503.  The main changes in the 5G ProSe direct link security mode control procedure to support the security requirements for the control plane security solution and the user security plane solution are:  1- The initiating UE doesn't derive a new KNRP by itself, but instead it receives the KNRP from either the PKMF (user plan solution) or the AMF (control plane solution).  2- The initiating UE doesn't generate Nonce\_2 by itself, but instead it receives the that value from either the PKMF (user plan solution) or the AMF (control plane solution).  3- The target UE calculates the KNRP upon getting the PROSE DIRECT LINK SECURITY MODE COMMAND message and using the Nonce\_2 included in it (where in the non-relay cases, the KNRP is calculated before this step).  4- Also keys names need to be adapted for different solutions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Resolving the EN that is related to possible changes to the 5G ProSe direct link security mode control procedure due to the security requirements of UE-to-network relay  Reflecting the changes mentioned above in the 5G ProSe direct link security mode control procedure | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | EN is not resolved, and the existing 5G ProSe direct link security mode control procedure can't be used for the UE-to-network relay cases. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.2.10.1, 7.2.10.2, 7.2.10.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | **Changes in Rev 2:**  This CR was already agreed in CT1#135-e, but the following issues were found after an offline check and they are fixed in this revision:  (1) There is a typo that needs a correction as following (highlighted in YELLOW):  *1) derive KNRP-sess from KNRP, KNRP freshness parameter ~~1~~2 and KNRP freshness parameter 1 received in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.503 [34]; and*  (2) The following statement that was added in clause 7.2.10.2 for Relay case is not needed and shall be removed:  *has either identified an existing KNRP based on the KNRP ID included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message*  because the initiating UE has to always initiate the key request procedures with the network to receive new KNR\_ProSe or KNRP, according to the control plane or user plane security solutions respectively.  (3) In clause 7.2.10.3, the text referring to NRPIK and NRPEK shall be extended to refer to Krelay-int and Krelay-enc as well. | | | | | | | | |

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

#### 7.2.10.1 General

The 5G ProSe direct link security mode control procedure is used to establish security between two UEs during a 5G ProSe direct link establishment procedure or a 5G ProSe direct link re-keying procedure. Security is not established if the UE PC5 signalling integrity protection is not activated. After successful completion of the 5G ProSe direct link security mode control procedure, the selected security algorithms and keys are used to integrity protect and cipher all PC5 signalling messages exchanged over this 5G ProSe direct link between the UEs and the security context can be used to protect all PC5 user plane data exchanged over this 5G ProSe direct link between the UEs. The UE sending the PROSE DIRECT LINK SECURITY MODE COMMAND message is called the "initiating UE" and the other UE is called the "target UE".

\*\*\*\*\* 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) in case of the direct communication is not between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, 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;

ii) in case of the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE with the security procedure over user plane being used, has received a new KNRP according to the security procedure over user plane as specified in 3GPP TS 33.503 [34];

iii) in case of the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE with the security procedure over control plane being used, has received a new KNR\_ProSe according to the security procedure over control plane as specified in 3GPP TS 33.503 [34]; or

iv) 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.

When:

a) the direct communication is not between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, if a new KNRP has been derived by the initiating UE; or

b) the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, if a new KNRP or KNR\_ProSe has been received by the initiating UE according to the security procedure over user plane or the security procedure over control plane, respectively, as specified in 3GPP TS 33.503 [34];

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

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

2) 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]; and

3) 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],

b) 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 as specified in 3GPP TS 33.503 [34] is used:

1) derive Krelay-sess from KNR\_ProSe, Nonce\_2 and Nonce\_1 received in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.503 [34]; and

2) derive the NR PC5 encryption key Krelay-enc and the NR PC5 integrity key Krelay-int from Krelay-sess and the selected security algorithms as specified in 3GPP TS 33.503 [34]; or

c) 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 as specified in 3GPP TS 33.503 [34] is used:

1) derive KNRP-sess from KNRP, KNRP freshness parameter 2 and KNRP freshness parameter 1 received in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.503 [34]; and

2) 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 33.503 [34]; 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 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 1: 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 or received at the initiating UE;

3) shall include a Nonce\_2 IE set to:

i) the 128-bit nonce value generated by the initiating UE when the direct communication is not between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE;

ii) the KNRP freshness parameter 2 value received by the initiating UE when the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE with the security procedure over user plane as specified in 3GPP TS 33.503 [34] being used; or

iii) the Nonce\_2 value received by the initiating UE when the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE with the security procedure over control plane as specified in 3GPP TS 33.503 [34] being used;

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 (or Krelay-int when applicable), NRPEK (or Krelay-enc when applicable) 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 2: 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 \*\*\*\*\*

#### 7.2.10.3 5G ProSe direct link security mode control procedure accepted by the target UE

Upon receipt of a PROSE DIRECT LINK SECURITY MODE COMMAND message, if a new assigned initiating UE's layer-2 ID is included and if the 5G ProSe direct link authentication procedure has not been executed, the target UE shall replace the original initiating UE's layer-2 ID with the new assigned initiating UE's layer-2 ID for 5G ProSe direct communication. The target UE shall check the selected security algorithms IE included in the PROSE DIRECT LINK SECURITY MODE COMMAND message. If "null integrity algorithm" is included in the selected security algorithms IE, the security of this 5G ProSe direct link is not activated. If "null ciphering algorithm" and an integrity algorithm other than "null integrity algorithm" are included in the selected algorithms IE, the signalling ciphering protection is not activated. If the target UE's 5G ProSe direct signalling integrity protection policy is set to "Signalling integrity protection required", the target UE shall check the selected security algorithms IE in the PROSE DIRECT LINK SECURITY MODE COMMAND message does not include the null integrity protection algorithm. If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall:

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

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

2) derive NRPIK from KNRP-sess and the selected integrity algorithm as specified in 3GPP TS 33.536 [37]; and

3) if the KNRP-sess is derived and the selected ciphering protection algorithm is not the null ciphering protection algorithm, then the target UE shall derive NRPEK from KNRP-sess and the selected ciphering algorithm as specified in 3GPP TS 33.536 [37]; or

b) if the direct communication is between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE:

1) if the security procedure over control plane as specified in 3GPP TS 33.503 [34] is used, derive Krelay-sess according to the security procedure over control plane, and derive Krelay-int from Krelay-sess and the selected integrity algorithm as specified in 3GPP TS 33.503 [34]. If the Krelay-sess is derived and the selected ciphering protection algorithm is not the null ciphering protection algorithm, then the target UE shall derive Krelay-enc from Krelay-sess and the selected ciphering algorithm as specified in 3GPP TS 33.503 [34]; or

2) if security procedure over user plane as specified in 3GPP TS 33.503 [34] is used, derive KNRP-sess according to the security procedure over user plane, and derive NRPIK from KNRP-sess and the selected integrity algorithm as specified in 3GPP TS 33.503 [34]. If the KNRP-sess is derived and the selected ciphering protection algorithm is not the null ciphering protection algorithm, then the target UE shall derive NRPEK from KNRP-sess and the selected ciphering algorithm as specified in 3GPP TS 33.503 [34].

The target UE shall determine whether or not the PROSE DIRECT LINK SECURITY MODE COMMAND message can be accepted by:

a) checking that the selected security algorithms in the PROSE DIRECT LINK SECURITY MODE COMMAND message does not include the null integrity protection algorithm if the target UE's 5G ProSe direct signalling integrity protection policy is set to "Signalling integrity protection required";

b) asking the lower layers to check the integrity of the PROSE DIRECT LINK SECURITY MODE COMMAND message using NRPIK (or Krelay-int when applicable) and the selected integrity protection algorithm, if the selected integrity protection algorithm is not the null integrity protection algorithm;

c) checking that the received UE security capabilities have not been altered compared to the values that the target UE sent to the initiating UE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or PROSE DIRECT LINK REKEYING REQUEST message;

d) if the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure,

1) checking that the received UE 5G ProSe direct signalling security policy has not been altered compared to the values that the target UE sent to the initiating UE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; and

2) checking that the LSB of KNRP-sess ID included in the PROSE DIRECT LINK SECURITY MODE COMMAND message are not set to the same value as those received from another UE in response to the target UE's PROSE DIRECT LINK ESTABLISHMENT REQUEST message; and

e) if the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link re-keying procedure and the integrity protection algorithm currently in use for the 5G ProSe direct link is different from the null integrity protection algorithm, checking that the selected security algorithms in the PROSE DIRECT LINK SECURITY MODE COMMAND message do not include the null integrity protection algorithm.

If the target UE did not include a KNRP ID in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message, the target UE included a Re-authentication indication in the PROSE DIRECT LINK REKEYING REQUEST message or the initiating UE has chosen to derive:

a) a new KNRP if the direct communication is not between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE; the target UE shall derive KNRP as specified in 3GPP TS 33.536 [37];

b) a new KNRP, 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 as specified in 3GPP TS 33.503 [34] is used, the target UE shall derive KNRP as specified in 3GPP TS 33.536 [37]; or

c) a new KNR\_ProSe, 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 as specified in 3GPP TS 33.503 [34] is used, the target UE shall derive KNR\_ProSe as specified in 3GPP TS 33.536 [37]; and

the target UE shall choose the 2 LSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the target UE. The target UE shall form KNRP ID from the received MSB of KNRP ID and its chosen LSB of KNRP ID and shall store the complete KNRP ID with KNRP.

If the target UE accepts the PROSE DIRECT LINK SECURITY MODE COMMAND message, the target UE shall create a PROSE DIRECT LINK SECURITY MODE COMPLETE message. In this message, the target UE:

a) shall include the PQFI and the corresponding PC5 QoS parameters if the direct communication is not for 5G ProSe direct communication between the 5G ProSe layer-2 remote UE and the 5G ProSe layer-2 UE-to-network relay UE;

b) if IP communication is used and the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure, shall include an IP address configuration IE set to one of the following values:

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

2) "address allocation not supported" if IPv6 address allocation mechanism is not supported by the target UE;

c) if IP communication is used, the IP address configuration IE is set to "address allocation not supported" and the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure, shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [25];

d) if a new KNRP was derived, shall include the 2 LSBs of KNRP ID; and

e) if the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure, shall include its UE 5G ProSe direct user plane security policy for this 5G ProSe direct link. In the case where the different ProSe services are mapped to the different 5G ProSe direct user plane security policies, when more than one ProSe identifier is included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message, each of the user plane security polices of those ProSe services shall be compatible, e.g., "user plane integrity protection not needed" and "user plane integrity protection required" are not compatible.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall form the KNRP-sess ID from the MSB of KNRP-sess ID it had sent in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or PROSE DIRECT LINK REKEYING REQUEST message and the LSB of KNRP-sess ID received in the PROSE DIRECT LINK SECURITY MODE COMMAND message. The target UE shall use the KNRP-sess ID to identify the new security context.

After the PROSE DIRECT LINK SECURITY MODE COMPLETE message is generated, the target UE shall pass this message to the lower layers for transmission along with the target UE's layer-2 ID for 5G ProSe direct communication and the initiating UE's layer-2 ID for 5G ProSe direct communication, NRPIK (or Krelay-int when applicable), NRPEK (or Krelay-enc when applicable) if applicable, KNRP-sess ID, the selected security algorithm as specified in 3GPP TS 33.536 [37] , and 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.

NOTE: The PROSE DIRECT LINK SECURITY MODE COMPLETE message and further 5G ProSe direct signalling messages are integrity protected and ciphered (if applicable) 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 target 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.

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