**3GPP TSG-CT WG1 Meeting #127-eC1-207247**

**Electronic meeting, 13-20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0157** | **rev** | **1** | **Current version:** | **16.2.1** |  |
|  | | | | | | | | |
| *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:*** | IP address information in security mode control procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-10-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | PC5 unicast link security mode control procedure is triggerred by PC5 unicast link establishment and PC5 unicast link re-keying procedures to negotiate new PC5 unicast link security context between initiating UE and target UE. If PC5 unicast link security mode control procedure is triggerred by PC5 unicast link re-keying procedures, the IP address information such as IP address configuration and Link local IPv6 address should not be included in DIRECT LINK SECURITY MODE COMPLETE message. Because these informations have been transmitted during the PC5 unicast link establishment procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | IP address configuration and Link local IPv6 address should be included in DIRECT LINK SECURITY MODE COMPLETE message only if the PC5 unicast link security mode control procedure is triggerred by PC5 unicast link establishment procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Missing the restriction about the IP address configuration and Link local IPv6 address IEs in DIRECT LINK SECURITY MODE COMPLETE message | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.7.3, 7.3.14.2, 7.3.14.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

##### 6.1.2.7.3 PC5 unicast link security mode control procedure accepted by the target UE

Upon receipt of a DIRECT LINK SECURITY MODE COMMAND message, the target UE shall first check the selected security algorithms IE included in the DIRECT LINK SECURITY MODE COMMAND message. If "null integrity algorithm" is included in the selected security algorithms IE, the security of this PC5 unicast 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 PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required", the target UE shall check the selected security algorithms IE in the DIRECT LINK SECURITY MODE COMMAND message does not include the null integrity protection algorithm. If the an integrity algorithm other than "null integrity algorithm" is included in the selected security algorithms IE.If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall:

a) derive KNRP-sess from KNRP, Nonce\_1 and Nonce\_2 received in the DIRECT LINK SECURITY MODE COMMAND message as specified in 3GPP TS 33.536 [20]; and

b) derive NRPIK from KNRP-sess and the selected integrity algorithm as specified in 3GPP TS 33.536 [20].

If the KNRP-sess is derived and the selected ciphering protection algorithm is not the null integrityciphering protection algorithm, then the target UE shall derive NRPEK from KNRP-sess and the selected ciphering algorithm as specified in 3GPP TS 33.536 [20].

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

a) checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message only include the null integrity protection algorithm if the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection not needed" or "signalling integrity protection notor preferred"; and

b) checking the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK, 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 DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

d) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure,

1) checking that the received UE PC5 unicast signalling security policy has not been altered compared to the values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message; and

2) checking that the 8 LSBs of KNRP-sess ID included in the 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 DIRECT LINK ESTABLISHMENT REQUEST message; and

e) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure and the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm, checking that the selected security algorithms in the 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 DIRECT LINK ESTABLISHMENT REQUEST message, the target UE included a Re-authentication indication in the DIRECT LINK REKEYING REQUEST message or the initiating UE has chosen to derive a new KNRP, the target UE shall derive KNRP as specified in 3GPP TS 33.536 [20]. The target UE shall choose the 16 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 MSBs of KNRP ID and its chosen LSBs of KNRP ID and shall store the complete KNRP ID with KNRP.

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

a) shall include the PQFI and the corresponding PC5 QoS parameters;

b) if IP communication is used and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast 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) "IPv6 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 "IPv6 address allocation not supported" and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [6];

d) if a new KNRP was derived, shall include the 16 LSBs of KNRP ID; and

e) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, shall include its UE PC5 unicast user plane security policy for this PC5 unicast link. In the case where the different V2X services are mapped to the different PC5 unicast user plane security policies, when more than one V2X service identifier is included in the DIRECT LINK ESTABLISHMENT REQUEST message, each of the user plane security polices of those V2X 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 8 MSBs of KNRP-sess ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNRP-sess ID received in the DIRECT LINK SECURITY MODE COMMAND message.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall integrity protect the DIRECT LINK SECURITY MODE COMPLETE message with the new security context. If the selected ciphering protection algorithm is not the null ciphering protection algorithm, the target UE shall cipher the DIRECT LINK SECURITY MODE COMPLETE message with the new security context.

After the 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 unicast communication and the initiating UE's layer-2 ID for unicast communication, NRPIK, NRPEK if applicable, KNRP-sess ID, and the selected security algorithm as specified in TS 33.536 [20].

\*\*\*\*\* Second change \*\*\*\*\*

#### 7.3.14.2 IP address configuration

The UE shall include this IE if IP communication is used and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure.

\*\*\*\*\* Third change \*\*\*\*\*

#### 7.3.14.3 Link local IPv6 address

The UE shall include this IE if IP communication is used, the IP address configuration is set to "IPv6 address allocation not supported" and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure.

\*\*\*\*\* End change \*\*\*\*\*