**3GPP TSG-CT WG1 Meeting #126-eC1-206043**

**Electronic meeting, 15-23 October 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.587** | **CR** | **0126** | **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:***  | Add triggers to re-keying procedure |
|  |  |
| ***Source to WG:*** | OPPO |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eV2XARC |  | ***Date:*** | 2020-9-9 |
|  |  |  |  |  |
| ***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 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-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:*** | In TS 33.536, there is the following cases that UE should trigger re-keying procedure:- This shall be done before the counter for a PDCP bearer repeats with the current keys.- The UE initiating the establishment of a user plane bearer shall select an LCID whose associated value of Bearer for input to the security algorithms (see clauses 5.3.3.1.5.2 and 5.3.3.1.5.3) has not been used with the current keys, NRPEK and NRPIK. If this is not possible the UE shall initiate a re-keying (see clause 5.3.3.1.4.4) before establishing the user plane bearer.However, the corresponding triggers are missing in 24.587. |
|  |  |
| ***Summary of change:*** | Add the missing triggers to re-keying procedure. |
|  |  |
| ***Consequences if not approved:*** | Stage 2 requirement for triggering re-keying procedure is missing. |
|  |  |
| ***Clauses affected:*** | 6.1.2.10.2 |
|  |  |
|  | **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 of change \*\*\*\*\*

##### 6.1.2.10.2 PC5 unicast link re-keying procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the PC5 unicast link re-keying procedure:

a) there is a PC5 unicast link between the initiating UE and the target UE; and

1) if the session key KNRP-sess used to protect PC5 unicast link needs to be refreshed and neither timer T5bbb nor T5008 are running;

2) if the UE wants to refresh KNRP and neither timer T5007 nor T5008 are running; or

3) if the lower layers inform that the PC5 unicast link re-keying procedure is needed.

In order to initiate the PC5 unicast link re-keying procedure, the initiating UE shall create a DIRECT LINK REKEYING REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container IE if 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 PC5 unicast 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 PC5 unicast link;

d) shall include the 8 MSBs of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] 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 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 T5008. The UE shall not send a new DIRECT LINK REKEYING REQUEST message to the same target UE while timer T5008 is running.

NOTE 2: In order to ensure successful PC5 unicast link re-keying, T5008 should be set to a value larger than the sum of T5006 and T5007.



Figure 6.1.2.10.2: PC5 unicast link re-keying procedure

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