**3GPP TSG-SA3 Meeting #100e *draft\_S3-201692\_r2***

**e-meeting, 17 -28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.536** | **CR** | **0006** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)****on using this form: comprehensive instructions can be found at  <http://www.3gpp.org/Change-Requests>.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update the clause 5.3.3.2.2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE Corporation | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-08-07 |
|  |  | | | |  | |  | | |  |
| ***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)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In the clause 5.3.3.2.2.1 and 5.3.3.2.2.2, link identifier update and Layer-2 link release procedure step 1, the MSB of KNRP-sess ID that UE\_1 choose to identify KNRP-sess should not be same with the former one, as well as the LSB of KNRP-sess ID in step 2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarification of MSB and LSB in clause 5.3.3.2.2.1 and 5.3.3.2.2.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | May cause some misunderstanding. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.3.2.2.1, 5.3.3.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

**\*\*\*\* START OF CHANGE 1 \*\*\*\***

##### 5.3.3.2.2 Procedures

5.3.3.2.2.1 Link identifier update

Figure 5.3.3.2.2-1 shows the flows for changing the identities of the UEs involved in PC5 unicast link. The figure only displays the security parameters (KNRP-sess ID)that are changed and the Layer-2 IDs but not the other parameters described in TS 23.287 [2].



Figure 5.3.3.2.2.1-1: Link identifier update procedure

The procedure proceeds with the following steps and provides additional handling on top of what is provided in TS 23.287 [2].

0. UE\_1 and UE\_2 are communicating via a unicast link and have established the security for the link.

1. UE\_1 decides to change its identifiers and sends a Link Identifier Update Request message to UE\_2 (see TS 23.287 [2]). In addition to the changed identifiers, UE\_1 shall include the new MSB of KNRP-sess ID in the Link Identifier Update Request message. These bits shall be chosen so that they uniquely identify KNRP-sess at UE\_1.The new MSB of KNRP-sess ID shall be selected randomly.

2. UE\_2 shall choose the new LSB of KNRP-sess ID so that they uniquely identify KNRP-sess at UE\_2. The new LSB of KNRP-sess ID shall be selected randomly. UE\_2 shall form the new KNRP-sess ID from the MSB received from UE\_1 and the LSB that UE\_2 chose. UE\_2 shall associate the new KNRP-sess ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new KNRP-sess ID when it uses the updated Layer-2 IDs. In addition to its updated identifiers, UE\_2 shall send the LSB of KNRP-sess ID to UE\_1 along with the received MSB of KNRP-sess ID and other identifiers received from UE\_1 in the Link Identifier Update Response message. UE\_1 shall check that the returned MSB of KNRP-sess ID is identical to the one sent in step 1.

3. UE\_1 shall form the new KNRP-sess ID from the LSB received from UE\_2 and the MSB chosen by UE\_1 (in step 1). UE\_1 shall associate the new KNRP-sess ID with the updated Layer-2 IDs (see TS 23.287 [2]) and shall use this new KNRP-sess ID when it uses the updated Layer-2 IDs. UE\_1 shall send the Link Identifier Update Ack message to UE\_2 including the LSB of KNRP-sess ID and other identifiers received from UE\_2. UE\_2 shall check that the returned LSB of KNRP-sess ID are identical to the one sent in step 2.

5.3.3.2.2.2 Layer-2 link release

Figure 5.3.3.2.2.2-2 shows the message flows for changing the KNRP ID of the UEs involved in PC5 unicast link to remediate the privacy threat for the KNRP ID. This message flow is based on the Layer-2 link release procedure provided in clause 6.3.3.3 of TS 23.287 [2]. The messages in the Layer-2 link release procedure are always sent protected and hence the new KNRP ID agreed by the UEs is only known to the involved UEs. The new KNRP ID is used on a subsequent unicast link establishment procedure (see clause 5.3.3.1.4.3).



Figure 5.3.3.2.2.2-2: Layer-2 link release procedure

0. UE\_1 and UE\_2 have a unicast link established as described in TS 23.287 [2].

1. UE\_1 sends a Disconnect Request message to UE\_2 in order to release the layer-2 link (see TS 23.287 [2]). UE\_1 shall include the new MSB of KNRP ID in the Disconnect Request message. These bits shall be chosen so that they uniquely identify KNRP at UE\_1.The new MSB of KNRP ID shall be selected randomly2. UE\_2 shall choose the new LSB of KNRP ID so that they uniquely identify KNRP at UE\_2.The new LSB of KNRP ID shall be selected randomly..UE\_2 shall form the new KNRP ID from the MSB received from UE\_1 and the LSB that UE\_2 chose. UE\_2 may use this new KNRP ID when it reconnects with UE\_1. UE\_2 shall send the LSB of KNRP ID to UE\_1 in the Disconnect Response message. Upon reception of the Disconnect Response message, UE\_1 shall form the new KNRP ID from the LSB received from UE\_2 and the MSB that was chosen by UE\_1 (in step 1). UE\_1 may use this new KNRP ID when it reconnects with UE\_2.

**\*\*\*\* END OF CHANGES \*\*\*\***