**3GPP TSG-SA3 Meeting #100e *S3-201942r3***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.536** | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Clarification on the unicast privacy procedures | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 06-08-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | Clarify that the link identifier update procedure procedure and Layer-2 link release procedure can be used to provide privacy but the privacy is only achieved if a non-NULL confidentiality algorithm is selected for the connection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Make it clear the achieving privacy with these procedures relies on the selection of non-NULL confidentilaity algorithm | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Lack of clarity on whether privacy is achieved. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.3.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 CHANGES \*\*\*\***

5.3.3.2.1 General

The link identifier update procedure given in TS 23.287 [2] is used to provide privacy for the identities in the unicast link. This procedure only provides privacy if a non-NULL confidentiality algorithm is selected, as this means the messages in this procedure are sent confidentiality protected (i.e. using a non-NULL confidentiality algorithm) and hence the new identities agreed by the UEs are only known to the involved UEs. A three-way message exchange procedure is required with this procedure since both UEs need to change their identifiers during the same procedure and to allow these new values to be acknowledged before them being used. This procedure is used to preserve the privacy for the identities that are seen in the clear for an ongoing unicast connection.

NOTE: From a security point of view, it is assumed that the link identifier update procedure is used with a protected connection.

A separate privacy threat that allows to link two subsequent connections is caused by either the same KNRP ID or same partial KNRP ID value being sent in the Direct Communication Request message for subsequent connections. The Layer-2 link release procedure given in TS 23.287 [2] can be used to provide privacy for the KNRP ID. To provide privacy using the link release procedure, the messages in the Layer-2 link release procedure are always sent after security has been established for the connection and hence when a non-NULL confidentiality algorithm is selected the new KNRP ID agreed by the UEs is only known to the involved UEs. Privacy is preserved only when the non-NULL confidentiality algorithm is selected.

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