**3GPP TSG-SA3 Meeting #98e *S3-200191***

**e-meeting, 2-6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **0032** | **rev** | **1** | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Updating the clause of "Key Reuse" for the gNB | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Telecom Italia, NTT DoCoMo | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2020-02-21 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The threat of key reuse for the gNB in TR 33.926 clause D.2.2.7 was decribed without indicating the conditions under which the threat can be exploited. Explicitly stating the conditions is necessary for differentiating the test cases in TS 33.511 clause 4.2.2.1.13 covering different purposes. Hence it is proposed to update the threat with all possible conditions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added the threat conditions in Annex D.2.2.7 for completeness. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The threat description for the test cases in TS 33.511 clause 4.2.2.1.13 is not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | D.2.2.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### D.2.2.7 Key Reuse

*- Threat name:* Key Reuse.

*- Threat Category*: Information Disclosure.

*- Threat Description*: If AS keys are not refreshed by the gNB when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KgNB, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions:

- when the PDCP COUNT wraps around and is reused with the same Radio Bearer (RB) identity and with the same KgNB, e.g. due to the transfer of large volumes of data.

- when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around.

*- Threatened Asset*: User plane data, Mobility Management data.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*