**3GPP TSG-SA3 Meeting #100e *S3-20XXXX***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **Draft CR** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Threat analysis on state transition from inactive state to connected state |
|  |  |
| ***Source to WG:*** | Huawei;Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS\_5G |  | ***Date:*** | 17-08-2020 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | R-17 |
|  | *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)* |
|  |  |
| ***Reason for change:*** | When state transition from inactive state to the connected state, if the gNB does not reactivate the UP security based on UP activation status, the UP activation status between the gNB and the UE will be different. This will cause the misalignment on UP activation status. |
|  |  |
| ***Summary of change:*** | Add a new threat analysis to 33.926 |
|  |  |
| ***Consequences if not approved:*** | The threat cannot be well identified and the test on it cannot find its threat reference. |
|  |  |
| ***Clauses affected:*** | D.2.2.X(new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  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.X State translation from inactive state to connected state

*- Threat name:* State transition from inactive state to connected state

*- Threat Category*: Denial of Service.

*- Threat Description*: When state transits from inactive state to the connected state, if the gNB does not reactivate/activate the UP security based on UP activation status included in the UE 5G AS security context, the UP activation status between the gNB and the UE may be different. This will cause the misalignment on UP activation status, and result in the UE has to reconnect to the Network again which wastes resource both at UE and gNB.

*- Threatened Asset*: Sufficient Processing Capability.

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