**3GPP TSG-SA3 Meeting #108e *S3-222102***

**e-meeting, 22 - 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DRAFT CR** | **rev** | **-** | **Current version:** | **17.4.0** |  |
|  |
| *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 |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Threat related to Local UP IP configuration |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The eNB is expected to be locally configured with UP integrity protection policy as specified in clause 7.3.3 of TS 33.401. In case it is not, then the UP IP feature will not be enabled even if the UE supports the UP IP. |
|  |  |
| ***Summary of change:*** | Update the threat to TR 33.926. |
|  |  |
| ***Consequences if not approved:*** | Incomplete security assurance work for the UP IP feature |
|  |  |
| ***Clauses affected:*** | New |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\* Begin 1st change\*\*\*\*\*\*\*\*\*

##### C.2.2.xLocal user plane integrity protection configuration

***-*** *Threat name:* Local user plane integrity protection configuration

***-*** *Threat Category:* Tampering data

***-*** *Threat Description:* When an eNB supports user plane integrity protection, and if the eNB is not preconfigured with a user plane integrity protection policy, and if the UE supports user plane integrity protection, then the protection might be disabled exposing the user plane data to tampering attacks when the MME does not send a user plane integrity protection policy to the eNB.

***-*** *Threatened Asset:* user plane data.

\*\*\*\*\*\*\*\*\* End of change\*\*\*\*\*\*\*\*\*