**3GPP TSG-SA3 Meeting #101e *S3-203074-r1***

**e-meeting, 9 – 20 November 2020** Revision of S3-20xxxx

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DRAFT** | **rev** | **1** | **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 |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | IMS SCAS: adding threats related to IMS signalling transport |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_IMS |  | ***Date:*** | 2020.10.22 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | 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:*** | If the protection implemented for the IMS signalling over Gm interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the IMS signalling data may be degraded and fail to fulfil the required security. The threats to IMS signalling transport needs to be added. |
|  |  |
| ***Summary of change:*** | Adding threats related to IMS signalling transport |
|  |  |
| ***Consequences if not approved:*** | No reference of threats related to IMS signalling transport. |
|  |  |
| ***Clauses affected:*** | New Annex X. |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## X.Y.Z Threats related to IMS signalling transport

***-*** *Threat name:*  No protection or weak protection for IMS signalling data.

***-*** *Threat Category:* Tampering,Information Disclosure.

***-*** *Threat Description:*

 If the protection implemented for the IMS signalling over Gm interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the IMS signalling data may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* IMS signalling data.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*