**3GPP TSG-SA3 Meeting #101e *S3-203076***

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

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

|  |
| --- |
|  |
| ***Title:***  | IMS SCAS: adding threats related to Resynchronization failure |
|  |  |
| ***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:*** | The threats related to Resynchronization failure needs to be added. In the synchronization failure scenario, after receiving the CM4 message from HSS, the UE may not be able to access to the network if no new authentication procedures is triggered by the S-CSCF. This can result in waste of system resources and deny a legitimate user access to the system. |
|  |  |
| ***Summary of change:*** | Adding threats related to Resynchronization failure |
|  |  |
| ***Consequences if not approved:*** | No reference of threats related to Resynchronization failure. |
|  |  |
| ***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 No resynchronization

* *Threat name:* No resynchronization
* *Threat Reference*: Denial of Service
* *Threat Description*: In the synchronization failure scenario, after receiving the CM4 message from HSS, the UE may not be able to access to the network if no new authentication procedure is triggered by the S-CSCF, i.e. the UE is given no opportunity to resynchronize with the network. This can result in waste of system resources and deny a legitimate user access to the system.
* *Threatened Asset*: Sufficient Processing Capacity

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