**3GPP TSG-SA3 Meeting #101e *S3-203059***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | DRFATCR | **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:***  | Threats related to security enforcement configuration for TSC services |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS\_5G |  | ***Date:*** | 2020.10.26 |
|  |  |  |  |  |
| ***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:*** | As defined in TS 33.501 clause L.3, the UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane.If the UP security enforcement information is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE, may be tampered or intercepted by the attacker. Hence, new test on this feature is required. |
|  |  |
| ***Summary of change:*** | Adding threats related to incorrect security enforcement configuration |
|  |  |
| ***Consequences if not approved:*** | No reference of threats related to incorrect security enforcement configuration. |
|  |  |
| ***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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### E.2.2.X Incorrect security enforcement configuration

* *Threat name:* Incorrect security enforcement configuration
* *Threat Reference*: Tampering data, Information Disclosure
* *Threat Description*: In case where the UDM is configured to set and provide the User Security Policy to the SMF for TSC service, if the UP security policy is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE in the user plane may be removed, tampered or intercepted by an attacker.
* *Threatened Asset*: User Subscription Data

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