**3GPP TSG-SA3 Meeting #101e *S3-203069***

**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 5G LAN services | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2020.10.26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel17 |
|  | *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 can be 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 K.3, to reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy.  If the UP security policy within a specific 5G Lan group is not the same, the data may be leaked from the unprotected air interface. Especially, for the case that one security policy is “required’, while the other security policy is “not needed”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding threats related to security policy misalignment on the 5G LAN services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No reference of threats related to security policy misalignment on the 5G LAN services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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 UP security policy configuration for 5G LAN service

* *Threat name:* Incorrect UP security policy configuration for 5G LAN service
* *Threat Reference*: Tampering data, Information Disclosure
* *Threat Description*: It is assumed that two UEs are belonging to one 5G LAN group. In case where the UDM is configured to set and provide User Plane Security policy to the SMF, if the UP security policies set for all the UEs belonging to a specific 5G LAN service are not consistent, e.g. the UP security policy1 for the UE1 is set to "required", and the UP security policy2 for the UE2 is set to "not needed", the 5G LAN service data transferred from gNB to UE2 may be removed, tampered or intercepted by the attacker, even if the service data transferred to the UE1 is protected. That means, the 5G LAN service data will be in the risk of being attacked with the lowest security level set in the the UP security policy.
* *Threatened Asset*: User Subscription Data

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