**3GPP TSG-SA3 Meeting #98e *draft\_S3-200384-r1***

**e-meeting, 2 – 6 March 2020 *merger of 160, 371 and 384***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.819** | **CR** | **0766** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  |
| *For* [***HELP***](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 | **x** | ME | **x** | Radio Access Network | **x** | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | UP security policy enforcement |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Interdigital, Ericsson??, Huawei??  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | VERTICAL\_LAN\_SEC |  | ***Date:*** | 6.3.2020 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** |  Rel-16 |
|  | *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:*** | Handling of UP security policy enforcement not addressed, taking over the conclusion of TR into normative clause. |
|  |  |
| ***Summary of change:*** | Adding a clause on UP security policy enforcement in line with conclusion. |
|  |  |
| ***Consequences if not approved:*** | UP security policy enforcement not handled for 5GLAN. |
|  |  |
| ***Clauses affected:*** | K.2, K.3 (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:*** | Note to MCC: please check on formatting of headlines |
|  |  |
| ***This CR's revision history:*** |  |

## \*\*\*\*\*\*\*\* START OF CHANGES

Annex K (normative):
Security for 5GLAN services

K.1 General

5GLAN services are described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [8].

K.2 Authentication and authorization

For authentication and authorization of a UE in 5GLAN communication, the secondary authentication procedures between UE and external data networks via the 5G Network as described in clause 11 shall apply.

K.3 Handling of UP security policy

During establishment of the PDU Session, secondary authentication may be performed in order to authenticate and authorize the UE for accessing the DNN associated with the 5G LAN group according to TS 23.501 [2]. After the UE is authenticated and data connection is set up, any protected data transported between the UE and NG-RAN is using the mechanisms for UP security as described in clause 6.6.

To reduce incremental complexity added by security, the same UP security policy for all 5G LAN group members may be provided by SMF to gNB with "Required" to be the preferred policy. I.e. for a 5G LAN group, when one or more of the PDU sessions have the UP security policy set to “Required”, all the PDU sessions belonging to that group would be set to "Required".

When generating the policy enforcement information, and to avoid the redundant double protection, the SMF may consider information by a DN-AAA about DN protection mechanisms already applied.

## \*\*\*\*\*\*\*\* END OF CHANGES