|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **3GPP TSG-SA WG3 Meeting #99e S3-201116****e-meeting, 11 – 15 May 2020**

|  |
| --- |
| *CR-Form-v11.4* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | DraftCR | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  |
| *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:***  | (D)DoS mitigation in PNiNPNs |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | Vertical\_LAN\_SEC |  | ***Date:*** | 2020.05.11 |
|  |  |  |  |  |
| ***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:*** | (D)DoS attack issue not yet addressed in new Annex on NPN.  |
|  |  |
| ***Summary of change:*** | Based on TR 33.819 conclusion, rejecting invalid UEs before primary athentication is selected for (D)DoS attack mitigation.  |
|  |  |
| ***Consequences if not approved:*** | (D)DoS attack issue is not addressed in the normative work. |
|  |  |
| ***Clauses affected:*** | Annex I.X (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:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE

## I.X (D)DoS mitigation in PNiNPNs

AMF shall verify whether UE access is allowed by Mobility Restrictions according to the subscription data received from UDM. After a verification failure, the AMF shall send a rejection message with an appropriate cause to the UDM. The rejection cause indicates that the UE is rejected because of CAG not allowed. The UDM shall store the received rejection message from AMF and keeps tracks of the number of rejections along with UE’s SUPI. The UDM monitors the rejection, and based on the repeated rejection notifications from the AMF, can mark the UE as malicious. When a new authentication request with an additional CAG access indication for the UE arrives, the UDM can reject the UE immediately after the SUCI de-concealment and skip the primary authentication procedure.

NOTE 1: It is up to the operator’s policy to set the number of rejections UDM can tolerate before marking UE as malicious.

NOTE 2: It is up to the operator’s policy to define when to unmark a UE.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE