**3GPP TSG-SA3 Meeting #99 *S3-201296***

**e-meeting, 11 -15 May 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **845** | **Rev** | **-** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | To mitigate the GSMA referenced potential attacks on the sensitive UP traffic (like DNS, ICMP), a UP IP activated dedicated PDU session is established. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | To separate and protect sensitive traffic (like DNS, ICMP) in a dedicated PDU sessions that support UP IP. The network provides configuration to establish the dedicated PDU session using the URSP. The network configuration can be based on the device capability or based on the UP IP security policy. Based on the URSP, the UE establish the application specific PDU session(s) and additionally a dedicated PDU session. Using the IP Packet Filter Set, the application packets are routed via the appropriate PDU sessions. If the application data is DNS (example, identified using Port number and/or destination IP address) or ICMP message (example, identified using protocol field), then the packets are routed via the UP IP activated dedicated PDU session. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Possibility of manipulation of encrypted sensitive UP traffic. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.6.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\*\*\*\*\*\*\*\*\*\*\***

### 6.6.X UP integrity protection for UP Signalling messages

Based on the serving network policy, a special DNN may be configured in the UE. The UE uses the special DNN, to establish a dedicated PDU session, which shall be used for the protection of the UP Signalling messages (for example, DNS, ICMP protocol messages). The special DNN configuration information is delivered in the URSP from the PCF via AMF to the UE using the UE Configuration Update procedure as defiend in TS 23.502 [8] or preconfigured within the UE Local Configuration.

The UE uses the URSP rules or the UE Local Configuration to determine details for establishing the PDU sessions, when the application triggers the PDU session establishment, as defined in TS 23.501 [2]. If the special DNN matches the application traffic descriptor, then the UE shall initiate the PDU session establishment procedure to establish the dedicated PDU session in addition to the application specific PDU session(s). The UP security policy provided by the SMF shall activate the UP integrity protection for the dedicated PDU session. After successful establishment of the PDU sessions, the dedicated PDU session shall be used to exchange the UP signalling messages (for example, DNS, ICMP protocol messages) with integrity protection.

**\*\*\*\*\*\*\*\*\*\*\*\*End of Change\*\*\*\*\*\*\*\*\*\*\***