**3GPP TSG-SA3 Meeting #99e *S3-201443***

**e-meeting, 11 -15 May 2020** Revision of S3-201392

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** | **0695** | **rev** | 2 | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Security Aspects of DNS and ICMP |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | UPIP\_SEC |  | ***Date:*** | 2020-05-20 |
|  |  |  |  |  |
| ***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:*** | In EPS, UP IP is not supported on the Uu interface. Lack of support for UP IP may allow an attacker to modify the user plane data over the air undetected, leading to a security vulnerability that may be exploited when DNS or ICMP messages are carried over the user plane. |
|  |  |
| ***Summary of change:*** | Addition of Annex Y that refers to Annex X (Security Aspects of DNS and ICMP) of TS 33.501 so that DNS and ICMP messages can be protected in EPS. |
|  |  |
| ***Consequences if not approved:*** | DNS and ICMP messages remain vulnerable in EPS. |
|  |  |
| ***Clauses affected:*** |  Annex Y (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:*** | Approval of this CR is dependent on the approval of CR#0841 to TS 33.501 in S3-201442 |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annex Y (informative):
Security Aspects of DNS and ICMP

# X.1 General

The security measures specified in Annex X of TS 33.501 [43] can be used to protect the DNS and ICMP messages that are carried over the user plane.

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