**3GPP TSG-SA3 Meeting #103-e *draft r1 S3-211473***

**e-meeting, 17 - 28 May 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **43.020** | **CR** | **0058** | **rev** | **1** | **Current version:** | **16.0.0** |  |
|  |
| *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 | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Removal of GEA2 due to security concerns |
|  |  |
| ***Source to WG:*** | Vodafone |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2021-05-08 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Several issues relating to GEA1 and GEA2 have recently come to light that mean these algorithms need to be depriciated. |
|  |  |
| ***Summary of change:*** | Update clause D.4.9 to prohibit the support for GEA2. |
|  |  |
| ***Consequences if not approved:*** | There is a potential security hole that could allow a threat actor to decrypt encrypted data. |
|  |  |
| ***Clauses affected:*** | D.4.9 |
|  |  |
|  | **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:*** | Similar CRs are available for releases 11 to 15.  |
|  |  |
| ***This CR's revision history:*** |  |

D.4.9 Support of GPRS-A5 Algorithms in MS

It is mandatory for GEA3 and non encrypted mode (i.e. GEA0) to be implemented in mobile stations. GEA4 may be implemented in the mobile stations. In particular, it is prohibited to implement GEA1 and GEA2 in mobile stations.

No other GPRS encryption algorithms shall be supported in mobile stations.