**3GPP TSG-SA3 Meeting #115 *S3-240960***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **43.020** | **CR** | **0088** | **rev** |  | **Current version:** | **11.5.0** |  |
|  | | | | | | | | |
| *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:*** | Explicit requirement on initial INPUT value for the GPRS-A5 ciphering algorithm | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI8 | | | | |  | ***Date:*** | | | 2024-03-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-11 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to GSMA CVD 2023-0079, the GSMA CVD Panel of Experts recommends that clause D.4.6 includes an additional statement that the "…initial INPUT value determined by the network must be randomly generated for every new GPRS session and after the encryption key is changed".  This is needed in order to align this specification with the stage 3 specification TS 44.064, clause 8.9.2 which already includes such requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | A clarifying requirement is added in Annex D.4.6 to reflect the GSMA CVD PoE recommendation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Implementations which are based on stage 2 specifications are vulnerable to security attacks. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex D.4.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

## D.4.6 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide. Synchronisation is guaranteed by driving Algorithm GPRS-A5 by an explicit variable INPUT per established LLC and direction.

These initial INPUT values shall not be identical for the different LLC link. The initial INPUT value shall be determined by the network and shall be randomly generated for every new GPRS session and after the encryption key is changed. It may be identical for uplink and downlink value because the direction is given to the ciphering algorithm as described in 3GPP TS 41.061 and illustrated on the figure D.4.2. In a given direction, the INPUT value shall be unique for each frame.

The calculation of the INPUT value is described in GSM. The use of the INPUT value is described in 3GPP TS 41.061 and illustrated on the figure D.4.2.

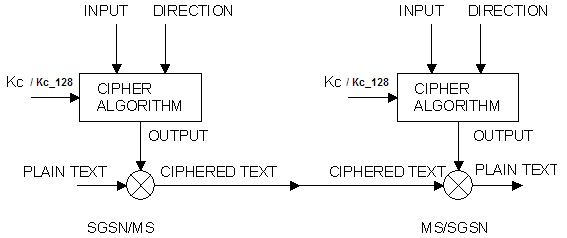


Figure D.4.2: Use of the INPUT parameter

\*\*\* END CHANGES \*\*\*