**3GPP TSG-SA3 Meeting #106-e *S3-220061***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | 1 | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Align GUTI allocation to best practices of unpredictable identifier generation. | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Deutsche Telekom AG, T-Mobile US | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-02-03 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | Current requirement on GUTI allocation ensures only the confidentiality of subscriber identities, but subscribers may not be safe from privacy leakage.  Recent studies have shown that the absence of a more detailed standard guideline for GUTI allocation has resulted in the problem of an easily predictable allocation logic. By that the GUTI allocation becomes predictable in certain scenarios, what brings an attacker, who could predict the GUTI of a victim, in the position to track that subscriber - what violates subscriber privacy eventually.  Thus, from subscriber's privacy point of view it is important that each new GUTI is a new random, unpredictable value that does not allow correlation with previously used GUTIs or any other temporary subscriber identity. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Align GUTI allocation to best practices of unpredictable identifier generation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | An attacker can track a subscriber over the radio if the new GUTI can be correlated with the previously used GUTI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.1 Mechanism for user identity confidentiality | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGINNING OF CHANGES \*\*\*

## 7.1 Mechanism for user identity confidentiality

The MME shall allocate a GUTI to a UE in order to support the subscriber identity confidentiality. The GUTI is defined in TS 23.003 [3].

S-TMSI, the shortened form of the GUTI, is used to support the subscriber identity confidentiality with more efficient radio signalling procedures (e.g. paging and Service Request).

A new GUTI shall be sent to the UE only after a successful activation of NAS security.

From subscriber's privacy point of view, a new GUTI shall be a new random, unpredictable value that does not allow correlation with previously used GUTIs or any other temporary subscriber identity.

GUTI generation should be following the best practices of unpredictable identifier generation and frequent reallocation.

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