**3GPP TSG-SA WG3 Meeting #104-eS3-212791r1**

**Electronic meeting, 16-27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1181** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  |
| *For* [***HELP***](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:***  | Addressing requirements to address the attack preventing NAS procedures to succeed |
|  |  |
| ***Source to WG:*** | Apple |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-08-16 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***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 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:*** | GSMA sent an LS (S3-211384/FASG Doc 92\_003) to SA3 and CT1 disclosing an attack (GSMA reference CVD-2021-0043) which allegedly impact the NAS protocol in the EPS and potentially in the 5GS.As mentioned in GSMA LS:  “The researchers claim that – in addition to Denial-of-Service (DoS) – the attack can cause essential security procedures to fail. As an example, the GUTI reallocation procedure may be prevented. The researchers claim this will lead to a prolonged usage of the same GUTI, allowing for prolonged tracking of a subscriber via the GUTI. They have observed this behavior in an opensource MME implementation. They also mention that preventing the NAS security mode procedure could prevent security key refresh.”The current specification TS 33.501 already defined the requirements to mandate the network to assign a new GUTI, However, there is no recovery procedure defined either on the UE or on the network side, if the GUTI assignment does not happen/keeps failing. This attack could be addressed by the simple enhancement in the network side, which is, whenever this abnormal case occur, network shall release the NAS connection, then UE will initiate the registration procedure.  |
|  |  |
| ***Summary of change:*** | Add the requirement that whenever this abnormal case occur, UE should initiate the registration procedure. |
|  |  |
| ***Consequences if not approved:*** | 5G-GUTI will not be udated and will be used for a prolonged time and it is allowing higher possibility to track the user.  |
|  |  |
| ***Clauses affected:*** | 6.12.3 |
|  |  |
|  | **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 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.12.3 Subscription temporary identifier

A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [19].

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the N1 NAS signalling connection is suspended.

Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM-IDLE mode with suspend indication in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the suspension of the N1 NAS signalling connection.

NOTE 1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above, for example after a Service Request message from the UE not triggered by the network.

NOTE 2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF.

~~When a new GUTI is relocated, if the GUTI Re-allocation is not resulting in a response from the UE (Registration Complete, UE Configuration Update complete), then AMF should release the NAS connection, and UE should initiate the registration procedure.~~

When UE is expecting a new 5G-GUTI, but failed to receive a new one, UE should initiate the registration procedure using the SUCI to get a new 5G-GUTI.

5G-TMSI generation should be following the best practices of unpredictable identifier generation.

A new I-RNTI shall be sent to a UE only after a successful activation of AS security.

On transition of UE to RRC INACTIVE state requested by gNB during RRC Resume procedure or RNAU procedure, the gNB shall assign a new I-RNTI to the UE.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*