**3GPP TSG-SA3 Meeting #108-e *Draft\_S3-222006-r1***

**e-meeting, 22 - 26 Aug 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** |  **1453** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  |
| *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:***  | Add restriction for multi registrations in two PLMNs |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***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 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:*** | When UE registers to network via both 3GPP and non-3GPP (e.g. UE registered to 3GPP network PLMN-1 with AMF-1 first, then UE registers to non-3GPP network PLMN-2 with AMF-2 later), two different security contexts and states are maintained. However, UDM and USIM still maintain the single SQN set for 5G AKA based authentication. If there's no sequence control or restriction on the UE, UDM may receive two registration requests from the same UE in parellel, that results in two AKA challenges(means SQN value in UDM incremented twice( e.g. SQN#1 for 3GPP registration, and SQN#2 for non-3GPP registration) and AV generated twice). In some race condition, UE may receive the AKA challenge (e.g. SQN#2) via non-3GPP connection first, and pass it to USIM. That will cause AKA challenge failure for 3GPP registration when UE pass SQN#1 to USIM for 3GPP access challenge verification, because the SQN#1 is less than SQN#2 which already stored in the USIM. Triggering sync failure procedure from USIM to network may solve the issue finally, but it takes time and resource. |
|  |  |
| ***Summary of change:*** | Update rules related to parallel NAS connections to control sequence also for multi-registration in different PLMNs. |
|  |  |
| ***Consequences if not approved:*** | Primary authentication of one of two parallel registrations of an UE in different PLMNs may be failed in some race conditions.  |
|  |  |
| ***Clauses affected:*** | 6.9.5.2 |
|  |  |
|  | **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 the 1st change ##################

#### 6.9.5.2 Rules related to parallel NAS connections

Concurrent runs of security procedures in parallel over two different NAS connections when terminated in the same or different AMF(s) can lead to race conditions and mismatches between the security contexts in the network and the UE. In order to avoid such mismatches, the following rules shall be followed:

1. The SEAF/AMF shall not initiate a primary authentication or NAS SMC procedure in case a primary authentication or a NAS SMC procedure is ongoing on a parallel NAS connection. Authentication procedures followed by a NAS SMC procedures taking the new 5G security context into use, shall be performed on one NAS signalling connection at a time.

NOTE: This rule is only applied on the case that two different NAS connections terminated in the same AMF.

2. When the AMF has sent a NAS Security Mode Command to a UE in order to take a new KAMF into use and receives a context transfer request message for the UE from another AMF, the AMF shall wait for the completion of the NAS SMC procedure (e.g. receiving NAS Security Mode Complete) before transferring the context.

NOTE: This rule is only applied on the case that two different NAS connections terminated in the same AMF.

3. The UE shall not initiate a NAS registration over a second NAS connection to an AMF of the same or different network(s) before primary authentication on the first NAS connection is complete.

################### end of the change ##################