**3GPP TSG-SA WG3 Meeting #98-E *S3-200180***

**Online, 2nd-6th March 2020**

|  |
| --- |
| *CR-Form-v11.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** | **0688** | **rev** | **-** | **Current version:** | **15.10** |  |
|  |
| *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 | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Security of RRC UE capability transfer procedure in EPS |
|  |  |
| ***Source to WG:*** | Intel |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI15 |  | ***Date:*** | 2020-03-02 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-15 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | This is an implementation of the LS reply on Handling of UE radio network capabilities in 4G and 5G, i.e., [S3-192271](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_95Bis_Sapporo/docs/S3-192271.zip). A CR was proposed in SA3-96 for LTE connecting to EPS , however it was decided to not pursue the CR as some CIOT UE without AS security will not be able to protect the UE capability.  |
|  |  |
| ***Summary of change:*** | A new clause 7.4.X(RRC UE capability transfer for UE with AS security).  |
|  |  |
| ***Consequences if not approved:*** | Tampering of UE capability information is possible and furthermore UE using CIOT CP optimization does not have AS security establishment. As a result, the existing solutions for normal UEs to protect the UE capability transfer does not prevent tampering of UE capability transfer using MITM attack.  |
|  |  |
| ***Clauses affected:*** | 7.4.X (new) |
|  |  |
|  | **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:*** |  |

\*\*\* START OF CHANGES \*\*\*

7.4.X RRC UE capability transfer procedure

The network should activate AS security (i.e., perform a successful AS SMC procedure) before running the RRC UE capability transfer procedure.

With the exception of unauthenticated emergency calls and the UEs using Control plane CIoT optimization, if the network had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, then the network shall not store them locally for later use and shall not send them to other network entities. In that case, the network shall re-run the RRC UE capability transfer procedure after a successful AS SMC procedure.

For the UEs using Control plane CIoT optimization, MME should not store the UE radio capability for a long period.\*\*\* END OF CHANGES \*\*\*