**3GPP TSG-SA3 Meeting #100e *S3-202034-r1***

**e-meeting, 17 -28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **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:*** | Handling of counter wrap around in UDM | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2020-08-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | It is specified in 6.14.2.3 that AUSF shall suspend SoR protection service if the CounterSOR associated with the KAUSF of the UE is about to wrap around and can only be resumed when a fresh KAUSF is generated for the UE. But how this suspending state of AUSF for the SoR protection service for the UE is synchronized to UDM and when UDM could resume the SoR information list update procedure as defined in 6.14.2.2 is not specified.  It is also specified in 6.15.2.2 that AUSF shall suspend UE Parameters Update protection service if the CounterUPU associated with the KAUSF of the UE is about to wrap around and can only be resumed when a fresh KAUSF is generated for the UE. But how this suspending state of AUSF for the UE Parameters Update protection service for the UE is synchronized to UDM and when UDM could resume the UE Parameters Update procedure as defined in 6.15.2.1 is not specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is specified that the AUSF provides an error indication to the UDM when the CounterSOR or CounterUPU associated with the KAUSF of the UE is about to wrap around.  In this case, the UDM aborts the ongoing SoR or UPU procedure and suspends any subsequent SoR or UPU procedure for the UE until the reception of a new success authentication result confirmation for the UE (cf. step 1 of clause 6.1.4.1a-1). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | UDM and AUSF is not synchronized on the counter wrap around handling for the SoR protection service and UPU protection service, unnessary network traffic can’t be avoided:   * During AUSF’s suspending period of the SoR protection service for the UE, UDM continue to consume AUSF’s SoR protection service before KAUSF is refreshed which would be failed in vain. * During AUSF’s suspending period of the UPU protection service for the UE, UDM continue to consume AUSF’s UPU protection service before KAUSF is refreshed which would be failed in vain. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.14.2.3, 6.15.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.14.2.3 SoR Counter

The AUSF and the UE shall associate a 16-bit counter, CounterSoR, with the key KAUSF.

The UE shall initialize the CounterSoR to 0x00 0x00 when the KAUSF is derived.

To generate the SoR-MAC-IAUSF, the AUSF shall use a counter, called a CounterSoR. The CounterSoR shall be incremented by the AUSF for every new computation of the SoR-MAC-IAUSF. The CounterSoR is used as freshness input into SoR-MAC-IAUSF and SoR-MAC-IUE derivations as described in the Annex A.17 and Annex A.18 respectively, to mitigate the replay attack. The AUSF shall send the value of the CounterSoR (used to generate the SoR-MAC-IAUSF) along with the SoR-MAC-IAUSF to the UE. The UE shall only accept CounterSoR value that is greater than stored CounterSoR value. The UE shall store the received CounterSoR, onlyif the verification of the received SoR-MAC-IAUSF is successful. The UE shall use the stored CounterSoR received from the HPLMN, when deriving the SoR-MAC-IUE for the SoR acknowledgement.

The AUSF and the UE shall maintain the CounterSoR for lifetime of the KAUSF.

The AUSF that supports the control plane solution for steering of roaming shall initialize the CounterSoR to 0x00 0x01 when the KAUSF is derived. The AUSF shall set the CounterSoR to 0x00 0x02 after the first calculated SoR-MAC-IAUSF, and monotonically increment it for each additional calculated SoR-MAC-IAUSF. The SoR Counter value of 0x00 0x00 shall not be used to calculate the SoR-MAC-IAUSF and SoR-MAC-IUE.

The AUSF shall suspend the SoR protection service for the UE, if the CounterSoR associated with the KAUSF of the UE, is about to wrap around. In this case, the AUSF replies with the corresponding error indication to SoR protection requests from UDM. The UDM shall abort the ongoing procedure for the steering of UE in VPLMN for the UE and shall also suspend any subsequet procedures for the steering of UE in VPLMN for the UE It is left to implementation when the UDM resumes ny suspended procedures for the steering of UE in VPLMN for the UE.

When a fresh KAUSF is generated for the UE, the CounterSoR at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume the SoR protection service for the UE.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.15.2.2 UE Parameters Update Counter

The AUSF and the UE shall associate a 16-bit counter, CounterUPU, with the key KAUSF.

The UE shall initialize the CounterUPU to 0x00 0x00 when the KAUSF is derived.

To generate the UPU-MAC-IAUSF, the AUSF shall use a counter, called a CounterUPU. The CounterUPU shall be incremented by the AUSF for every new computation of the UPU-MAC-IAUSF. The CounterUPU is used as freshness input into UPU-MAC-IAUSF and UPU-MAC-IUE derivations as described in the Annex A.19 and Annex A.20 respectively, to mitigate the replay attack. The AUSF shall send the value of the CounterUPU (used to generate the UPU-MAC-IAUSF) along with the UPU-MAC-IAUSF to the UE. The UE shall only accept CounterUPU value that is greater than stored CounterUPU value. The UE shall update the stored CounterUPU with the received CounterUPU, onlyif the verification of the received UPU-MAC-IAUSF is successful. The UE shall use the CounterUPU received from the UDM, when deriving the UPU-MAC-IUE for the UE Parameters Upadate Data acknowledgement.

The AUSF and the UE shall maintain the CounterUPU for lifetime of the KAUSF.

The AUSF that supports the UE parameters update using control plane procedure shall initialize the CounterUPU to 0x00 0x01 when the KAUSF is derived. The AUSF shall set the CounterUPU to 0x00 0x02 after the first calculated UPU-MAC-IAUSF, and monotonically increment it for each additional calculated UPU-MAC-IAUSF. The UPU Counter value of 0x00 0x00 shall not be used to calculate the UPU-MAC-IAUSF and UPU-MAC-IUE.

The AUSF shall suspend the UE Parameters Update protection service for the UE, if the CounterUPU associated with the KAUSF of the UE, is about to wrap around. In this case, the AUSF replies with the corresponding error indication to UE Paratemers Update protection requests from UDM. The UDM shall abort any ongoing UE Parameters Update procedure for the UE and shall also suspend any subsequet UE Parameters Update procedures for the UE. It is left to implementation when the UDM resumes ny suspended UE Parameters Update procedures for the UE.

When a fresh KAUSF is generated for the UE, the CounterUPU at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume theUE Parameters Update protection service for the UE.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*