**3GPP TSG-SA3 Meeting #105-e *S3-214232-r1***

**e-meeting, 08 - 19 November 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **01** | **CR** | **1243** | **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:*** | Network initiated Primary Authentication | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung, NEC | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-10-11 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | 7 |
|  | *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:*** | | Authentication of UE generates a key KAUSF that is shared between UE and home network. In 5G, KAUSF is a long term key, as UEs may be attached to a network for extended times without refreshing the KAUSF. In such scenarios, the home network doesn't have a mechanism to trigger re-authentication for the UE to refresh KAUSF.  During SA3#104-e meeting an LS (S3-213170) was sent to CT4 asking clarification on whether there is any mechanism already specified for re-authentication in CT4 specification. Excerpt from CT4 reply LS (C4-215437) are as follows:   |  | | --- | | 1) Whether it is possible for the UDM to send the application error *(REAUTHENTICATION\_REQUIRED)* to the AMF without a request from the AMF.  [CT4] No, this error cannot be sent without a request from the AMF.  2) Whether CT4 has already specified any procedure that allows the home network (particularly UDM and/or AUSF) to trigger re-authentication procedure.  [CT4] CT4 defines UDM triggered AMF de-registration procedure which can cause de-registration and re-registration of the UE, so that UDM can insist for re-authentication during re-registration. Though this procedure is not intended for triggering re-authentication, as it results in service impact. |   Based on the reply LS from CT4, it is necessary to have a requirement/procedure in SA3 to trigger re-authentication explicitly without having any service impact by maintaining the UE contexts. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This CR proposes, to trigger the re-authentication procedure by the UDM, based on request from an internal NF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UE may go into out-of-service, if there is a need for new KAUSF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.8.1, 6.1.X (new), 6.14.2.3, 6.15.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 of Changes \*\*\*

### 5.8.1 Generic requirements

The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected.

NOTE 1: Security mechanisms for protection of subscription credentials in ARPF are left to implementation.

NOTE 2: Security mechanisms for storage of subscription credentials in the UDR and for the transfer of authentication subscription data (as specified in 3GPP TS 29.505 [70]) between UDR and ARPF are left to implementation.

The UDM shall initiate re-authentication of the UE, if an internal NF request to initiate re-authentication to refresh the UE specific home key (KAUSF).

\*\*\* Next Change \*\*\*

### 6.1.X Initiation of re-authentication

A new primary re-authentication may require for certain events at the network, resulting in refresh of the latest home key KAUSF. In such scenarios, an internal Network Function shall request the UDM to trigger the re-authentication procedure.

Upon receiving the re-authentication request which may include SUPI or error message that indicates need for re-authentication from an internal Network Function, the UDM shall check whether the primary re-authentication for the UE to be initiated or request to be rejected, based on the operator policy. Operator policy includes the details of the wait period for the new request, after the last successful authentication. If the operator policy allows, then the UDM shall request the AMF currently serving the UE to initiate the primary authentication for the UE. Upon receiving the request which includes SUPI from the UDM, the AMF(SEAF) shall initiate the primary authentication as described in clause 6.1.2 of this document, resulting in generation of fresh key material in the UE and in the network as described in clause 6.2 of this document, if the primary authentication is performed successfully.

Editor’s Note: Exact message names and the AUSF service details are to be update, once CT WGs specified the stage 3 details.

\*\*\* Next 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 newly derived KAUSF is stored (see clause 6.2.2.2). The UE shall store the SoR counter. If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterSoR shall be stored in the USIM. Otherwise, CounterSoR shall be stored in the non-volatile memory of the ME

To generate the SoR-MAC-IAUSF, the AUSF shall use the 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 newly derived KAUSF is stored (see clause 6.2.2.1). 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. 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.

Upon receiving the error code “COUNTER\_WRAP” in Nausf\_SoRProtection Response from the AUSF, when the CounterSoR associated with the KAUSF of the UE is about to wrap around in the AUSF, then the UDM shall request the serving AMF to initiate the re-authentication procedure as specified in clause 6.1.X of this document. After successful completion of the primary re-authentication, the UDM invokes Nausf\_SoRProtection service again.

\*\*\* 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 newly derived KAUSF is stored (see clause 6.2.2.2). The UE shall store the UPU counter . If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterUPU shall be stored in the USIM. Otherwise, CounterUPU shall be stored in the non-volatile memory of the ME.

To generate the UPU-MAC-IAUSF, the AUSF shall use the 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 newly derived KAUSF is stored (see clause 6.2.2.1). 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. 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.

Upon receiving the error code “COUNTER\_WRAP” in Nausf\_UPUProtection Response from the AUSF, when the CounterUPU associated with the KAUSF of the UE is about to wrap around in the AUSF, then the UDM shall request the serving AMF to initiate the re-authentication procedure as specified in clause 6.1.X of this document. After successful completion of the primary re-authentication, the UDM invokes Nausf\_UPUProtection service again.

\*\*\* End of Changes \*\*\*