**3GPP TSG-SA3 Meeting #110 Adhoc-e *draft\_*S3-232026-r1**

**Electronic Meeting, 17 - 21 April 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **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:*** | HONTRA Clarifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | HN\_Auth | | | | |  | ***Date:*** | | | 2023-04-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | The Living CR for the HONTRA Procedure is agreed in S3-230977 during SA3#110 Meeting. The HONTRA procedure has some Editor’s Notes on ‘type of interactions between AMF and UDM’ and ‘step details, trigger to UDM etc.,’. Further NOTE 1 mentions an example which states that, ‘if the PLMN does not support the SoR/UPU feature, then a policy to initiate HONTRA upon SoR/UPU counter wrap around will not be required.’. The observation here is that, if the PLMN does not support the SoR/UPU feature, first there will not be any SoR/UPU wrap around can happen. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This contribution provides clarifications on ‘interaction between AMF and UDM’ and ‘steps details’ to resolve the related Editor’s Note. Further this contribution corrects the NOTE 1. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The HONTRA procedure will remain incomplete and incorrect. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.X, 6.14.2.3, 6.15.2.2, 14.2.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*

## 6.1X Home network triggered primary authentication procedure

### 6.1X.1 General

In case the HN and the SN support the services defined in clause 14.2.x, then the UDM is able to trigger a primary authentication procedure as described in the following clause.

Editor's Note: The impact of HONTRA on the security related service operations in clause 14 is FFS. The above statement wil be updated when the service operations are agreed.

### 6.1X.2 Security mechanisms

The UDM may initiate primary authentication based on events from other NFs, considering local policy into account as well.



**Figure 6.1.x.2-1 Home Network triggered primary authentication procedure**

0a.The UDM if supports HONTRA feature, it shall be pre-configured with an operator policy in order to determine when to trigger a primary (re-)authentication procedure as part of the operator authentication policy.

A prerequisite for the initiation of Home Network Triggered Primary Authentication is that the UDM already has the information about the AMF serving the UE. Otherwise, the UDM cannot contact any AMF in later steps.

Editor’s Note: Whether a new UDM service is needed for the UDM to initiate authentication for a UE’s SUPI to request AMF is FFS.

The UDM decides itself based on events (e.g., SoR/UPU or if AAnF requests) or authentication policy and performs home network triggers primary authentication as described in the following steps. The AAnF can consider the authentication policy available it’s side for the AKMA and related AF key lifetime setting. If an AF key expiry happens and still if there is no successful primary authentication that resulted in new AKMA key, then the AAnF can consider to request the UDM based on clause 14.2.6.1. Based on a received event and the local operator authentication policy, if there is no ongoing primary authentication for the UE, and if the UDM determines to trigger the primary authentication, the UDM determines the serving AMF/SEAF of the target UE.

Editor’s Note: The handling of multiple AMFs registered to the UDM is FFS.

NOTE 1: The reasons for the UDM determining that the UE needs to be authenticated can be different. For example, the UDM can determine to initiate a primary authentication when the AMF registers the UE upon the Registration procedure during the mobility from EPC or when SoR/UPU counters are about to wrap around, or when required based on authentication policy. The UDM behaviour is determined by the operator primary authentication policy which takes into account the support of certain features in the PLMN and if a time information is set by the operator to trigger a primary (re-)authentication. For example, if the PLMN does not support the SoR/UPU feature, then a SoR/UPU counter wrap around will not happen and so HONTRA initiation will not be required for such case.

2. The UDM sends an authentication request message to the AMF/SEAF with the UE’s SUPI.

3. After receiving the authentication message from the UDM, the AMF/SEAF shall decide whether run the primary authentication procedure based on its own local authentication policy. If the AMF/SEAF cannot run a primary authentication as described in steps 4, the AMF/SEAF sends the authentication response message to the UDM with an acknowledgement which includes failure cause, else it is set as success in case the AMF/SEAF can run a primary authentication.

Editor’s Note: The serving network has its own authentication policy. Moreover, it is possible that the UE cannot be reached. Therefore, it is FFS whether it can start a primary authentication right away after receiving the authentication message from the UDM.

4. The AMF/SEAF starts the primary authentication procedure as defined in clause 6.2.1 of the present document.

The UDM may execute other procedures (e.g., SoR/UPU) depending on the reason that motivated the UDM triggered (re-)authentication procedure in step 1.

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

\*\*\*Start of Change 2\*\*\*

#### 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.

\*\*\*End of Change 2\*\*\*

\*\*\*Start of Change 3\*\*\*

#### 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.

\*\*\*End of Change 3\*\*\*

\*\*\*Start of Change 4\*\*\*

### 14.2.6 Nudm\_UEAuthentication\_ Trigger service operation

The following table illustrates the authentication related services for home network triggered primary (re)authentication initiation that UDM provides.

Table 14.2.6-1: NF services for authentication trigger provided by UDM

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nudm\_UEAuthentication\_ Trigger | authentication | Request/Response | a NF |

**Service operation name:** Nudm\_UEAuthentication\_ Trigger.

**Description:** This service operation allows the NFto request UDM to trigger a primary (re-)authentication as described in Clause 6.1.5.

**Input, Required:** SUPI, Cause .

**Input, Optional:** None.

**Output, Required:** ACK Indication.

**Output, Optional:** None.

\*\*\*End of Change 4\*\*\*