**3GPP TSG-SA3 Meeting #116 *draft\_S3-242371-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, ZTE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2024-05-13 |
|  |  | | | |  | |  | | |  |
| ***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 behaviour of the AMF upon receiving the UDM notification to initiate primary authentication is not clear with respect to the AMF responses to the UDM. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Calrfication that the AMF can send either an acknowledgement or a single failure case (re-authention not allowed) to the UDM. The UDM action is also clarified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.5.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

#### 6.1.5.2 Security mechanisms

The UDM may initiate primary authentication based on procedures initiated by the UE (e.g. UE registration in 5GC) or towards the UE (e.g. SoR/UPU) or events from other NFs, considering the local policy into account as well.

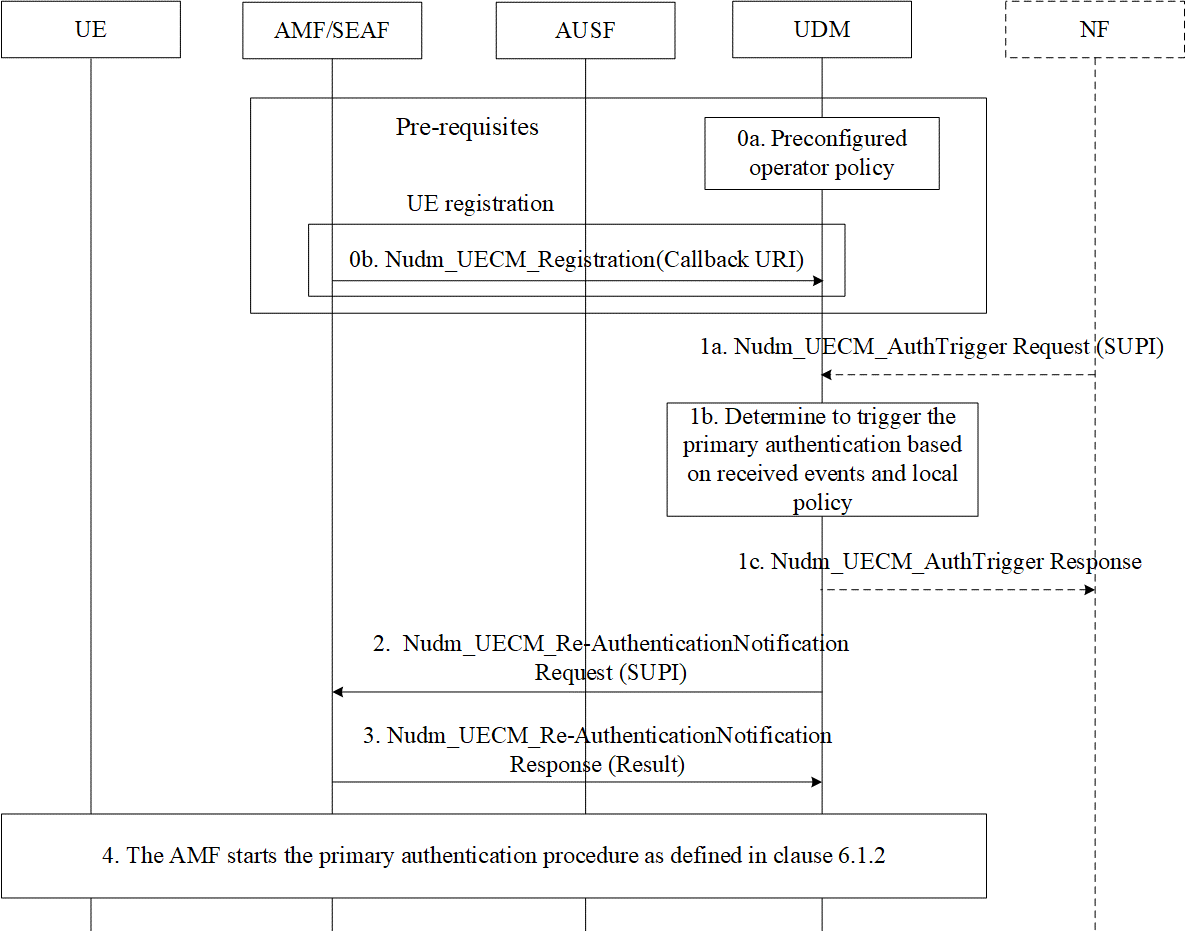


Figure 6.1.5.2-1 Home Network triggered primary authentication procedure

Step 0a and step 0b are the pre-requisites of the whole procedure.

0a. The UDM may be pre-configured with an operator authentication policy in order to determine when to trigger a primary authentication procedure.

0b. The UE registers to the network. As part of the registration, the serving AMF registers the UE with the UDM via the Nudm\_UECM\_Registration as per TS 23.502 [8], clause 4.2.2.2.2. The AMF shall provide a callback URI within the AMF registration for the UDM to create an implicit subscription to later notify the AMF for potential home network triggered re-authentication using the Nudm\_UECM\_Re-AuthenticationNotification service operation as in step 2.

1a-c. The UDM decides itself based on events (e.g., SoR/UPU or NF requests such as AAnF requests as defined in TS 33.535 [91]) or authentication policy and performs home network triggered primary authentication as described in the following steps. The NF such as the AAnF considers based on operator's local authentication policy described in TS 33.535 [91] to send Nudm\_UECM\_AuthTrigger request to the UDM for primary authentication using the UDM services as described in clause 14.2.6. The NF may send a Nudm\_UECM\_AuthTrigger Request message to the UDM with the SUPI of the target UE. The UDM may acknowledge the request with an Nudm\_UECM\_AuthTrigger Response to the NF.

NOTE A: For the NF (e.g., AAnF) request event, the UDM can decide not to proceed with triggering the primary authentication based on the UDM’s local authentication policy. In case of AAnF being the NF, as AAnF sets the AF key expiry based on operator’s local authentication policy, no frequent AF key expiry can happen and there is no risk of signalling overload. 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.

If there are different AMFs registered in the UDM for different access, the UDM shall select one AMF to perform the re-authentication. The criteria for selecting the AMF are dependent of the local UDM authentication policy.

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, or based on the request from AAnF. The UDM behaviour is determined by operator policy which takes into account the support of certain features in the PLMN. For example, if the HPLMN does not support the SoR/UPU feature, then SoR/UPU counter wrap around will not happen, and primary authentication will not be required for this case.

2. The UDM sends a Nudm\_UECM\_Re-AuthenticationNotification message to the AMF/SEAF with the UE’s SUPI.

3. After receiving the Nudm\_UECM\_Re-AuthenticationNotification message from the UDM, the AMF/SEAF shall decide whether to run the primary authentication procedure based on its own local authentication policy, and the UE state.

NOTE X: Examples of UE state is when the UE is under handover, or if the UE is already under authentication by the AMF before receiving the authentication notification from the UDM.

If the AMF/SEAF determines that it cannot run a primary authentication as described in step 4 due to local policy, the AMF/SEAF sends the authentication response message to the UDM with a re-authentication not allowed failure cause else it acknowledges the request.

If the AMF/SEAF acknowledged the request but the AMF/SEAF is not able to initiate the primary authentication towards the UE (e.g. if UE is not reachable), the AMF/SEAF shall set the authentication pending flag.

Upon receiving a failure from the AMF, the UDM may check if another AMF is available over the other access or wait for a subsequent registration from another AMF to . retry Step 2.

When UE re-attaches to the same AMF or becomes reachable, the AMF checks the authentication pending flag and performs the reauthentication if needed. Once UE reauthentication is done, the AMF resets the authentication pending flag.

NOTE 2: In the case that the UE attaches to a new AMF, the new AMF will register to the UDM using the Nudm\_UECM\_Registration message. In this case, the UDM can determine again on whether to trigger the primary authentication as described in 1b.

NOTE Y: The AMF will respond either with an acknowledgement message or a failure message. The acknowledgement message is to tell the UDM that the AMF is currently handling or will initiate the primary authentication. The failure response message is used to tell the UDM that the AMF will not initiate the primary authentication based on the request.

4. The AMF/SEAF starts the primary authentication procedure as defined in clause 6.1.2 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 CHANGES \*\*\*