**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *S3-231926***

**Electronic meeting, Online, 17 - 21 April 2023** (revision of S3-yyxxxx)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **draftCR** | **rev** | - | **Current version:** | **18.0.0** |  |
|  | | | | | | | | |
| *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:*** | Living CR of the HONTRA procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | HN\_Auth | | | | |  | ***Date:*** | | | 2023-02-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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:*** | | This contribtion proposes the necessary requirements for the support and usage of a new home triggered primary authentication procedure that is under the control of the home network. The background is that while the in the 5G System, the home network is in general more involved than in previous generations in the primary authentication procedure, it is still the case that only the visisted network that can directly trigger a new fresh run of the primary authentication. Since the first release of the 5G system several use cases have been identified that would benefit from a home triggered procedure and hence this contribution provides the necessary changes to support such mechanism. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | A new procedure describing the usage and the message flow of a home network triggered primary authentication procedure as well as the definition of the related new services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No support for a home network triggered primary authenticationliving doc. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.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:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This draftCR's revision history:*** | | SA3#110: S3-231477, S3-231478  SA3#110Adhoc: | | | | | | | | |

\*\*\* BEGIN of 1st CHANGE \*\*\*

### 6.1.X Home network triggered primary authentication procedure

#### 6.1.X.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.

Editor’s Note: It needs to be stated in this clause that the support of HONTRA in 5GC is optional.

#### 6.1.X.2 Security mechanisms

The UDM may initiate primary authentication based onprocedures 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.x.2-1 Home Network triggered primary authentication procedure**

0a.[optional] 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 UDM shall create an implicit subscription for the serving AMF for the UDM to later notify the AMF for potential re-authentication.

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 is FFS, whether it is needed that a consumer NF (e.g. AUSF) triggers the UDM 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 considers based on certain factors to request the UDM for primary authentication using the UDM services as described in clause 14.

Editor’s Note: The factor the AAnF considers to request UDM for primary authentication is FFS, as AAnF request(s) should not lead to signalling overload as well as the AF key expiry/refresh issue should be handled.

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.

If there are different AMFs registered in the UDM for different access, and the procedure defined in 6.1X is supported, the UDM shall select one AMF to perform the reauthentication.

Editor’s Note: The selection of AMF is FFS, for example, whether 3GPP access type or selecting AMF based on CM state available in Access and mobility data.

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 authenticationpolicy, 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 PLMN 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 notification message to the AMF/SEAF with the UE’s SUPI.

Editor’s Note: The name of notification message between AMF and UDM is FFS.

3. After receiving the notification message from the UDM, the AMF/SEAF shall decide whether run the primary authentication procedure based on its own local authentication policy, and the UE state (e.g. if the UE is under handover, a similar way as some steps in Network Triggered Service Request (TS 23.502 [8], clause 4.2.3.3) can be reused, or if the UE is already under authentication by the AMF before receiving the authentication notification from the UDM). 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.

Editor’s Note: Whether the AMF marks the UE as pending authentication or not is FFS.

Editor's Note: The response message parameters and the semantics of the different cases (success, failure) are FFS.

Upon receiving a failure from the AMF, the UDM may check if another AMF is available over the other access. If available, the UDM may select another AMF and send an authentication request

Editor’s Note: If UDM has to send authentication requests to 2 AMFs, then how can it ensure double authentication is not performed? Therefore, upon receiving the successful authentication from one AMF, sending a cancellation authentication may be required. These aspects are FFS

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 \*\*\*