**3GPP TSG-SA3 Meeting #111 *draft\_*S3-233xxx-r1**

**Berlin, Germany, 22 -26 May 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1670** | **rev** | 1 | **Current version:** | **18.1.0** |  |
|  | | | | | | | | |
| *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 |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Introducing Home Trigger primrary authentication procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon,Nokia, Nokia Shanghai Bell, Qualcomm Incorporated, Samsung, Lenovo, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | HN\_Auth | | | | |  | ***Date:*** | | | 2023-05-20 |
|  |  | | | |  | |  | | |  |
| ***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 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 authentication feature | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.x (new) ; 6.14.2.1 ; 6.15.2.1 ; 8.1 ; 14.2.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: S3-232211,S3-232123, S3-232168, S3-232169,S3-232110  S3-232193  SA3#111: S3-233287, S3-233224, S3-233216, S3-233223, S3-233217, S-233218. | | | | | | | | |

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

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

#### 6.1.X.1 General

The support of Home Network triggered authentication is optional for the HN and the SN. If both the networks (HN and SN) support Home Network triggered primary authentication, the following clauses apply.

#### 6.1.X.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.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.

1. 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.

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 send Nudm\_UECM\_AuthTrigger request to the UDM for primary authentication using the UDM services as described in clause 14.2.X.

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.

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. 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 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 a 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 in the UE context.

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. If the UE attaches to a new AMF (e.g., in a mobility scenario), then the new AMF may retrieve the UE Context from the previous AMF, determine that authentication is pending for the UE, and perform reauthentication. 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. While the authentication is pending, whether the UDM selects another AMF after receiving an acknowledgement is FFS. Requirement of authentication cancelation is also to be rechecked.

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 1st CHANGE \*\*\*

**\*\***\*\* START OF 2nd CHANGES \*\*\***\***

6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case where the UE registers with VPLMN AMF is described below in figure 6.14.2.1-1:

****

**Figure 6.14.2.1-1: Procedure for providing list of preferred PLMN/access technology combinations** **during registration in VPLMN**

1) The UE initiates registration by sending Registration Request message to the VPLMN AMF.

2-3) The VPLMN AMF executes the registration procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]. As part of the registration procedure, the VPLMN AMF executes primary authentication of the UE and then initiates the NAS SMC procedure, after the authentication is successful.

4-5) The VPLMN AMF invokes the Nudm\_UECM\_Registration message to the UDM and registers access with the UDM as per step 14a in sub-clause 4.2.2.2.2 of 3GPP TS 23.502[8].

6) The VPLMN AMF invokes Nudm\_SDM\_Get service operation message to the UDM to get amongst other information the Access and Mobility Subscription data for the UE (see step 14b in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]).

7) The UDM decides to send the Steering of Roaming Information, and obtains a list of preferred PLMN/access technology combinations and optional additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator), or a secured packet list as described in TS 23.122 [53].

NOTE 1: Additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator) can only be added when the AMF supports SoR transparent container.

If the UDM determines that the UE is configured to not expect to receive Steering of Roaming Information at initial registration and if the UDM determines that no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed, then the UDM may not piggyback Steering of Roaming Information at all in the Nudm\_SDM\_Get response and hence the following steps are omitted.

8-9) The UDM shall invoke Nausf\_SoRProtection service operation message to the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the HPLMN decides that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf\_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-IUE, as specified in sub-clause 14.1.3 of this document.

NOTE 2: At reception of Nausf\_SoRProtection\_Protect request from the UDM, if the SoR header is not included in the request, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and list of preferred PLMN/access technology combinations or secured packet (if provided); otherwise, if the SoR header is contained in the request, the AUSF uses the received SoR header in the calculation of SoR-MAC-IAUSF..

The details of the CounterSoR are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SoR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the received Steering of Roaming Information is not tampered with or removed by the VPLMN. The expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering of Roaming Information.

10) The UDM responds to the Nudm\_SDM\_Get service operation to the VPLMN AMF, which shall include the SoR transparent container as specified in clause 6.1.6.3.2 of TS 29.503 [93] if the VPLMN AMF support SoR transparent container, or shall include individual IEs comprising the ACK Indication, the list of preferred PLMN/access technology combinations or secured packet (if provided), SoR-MAC-IAUSF and CounterSoR within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-IUE.

11) If the SoR transparent container is received from the UDM, the VPLMN AMF shall include the received SoR transparent container in the Registration Accept message and send it to the UE. If the individual IEs are received from the UDM, the VPLMN AMF shall construct the SOR header based on the ACK Indication and the list of preferred PLMN/access technology combinations or secured packet (if provided) received from the UDM and include it in the SOR transparent container as specified in clause 9.11.3.51 of TS 24.501 [35]. The vPLMN shall also include SoR-MAC-IAUSFand CounterSoR(both also received from the UDM) in the constructed SoR transparent container, and convey the constructed SoR transparent container to the UE in the Registration Accept message.

12) On receiving the Registration Accept message with the SoR transparent container from the AMF the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the SoR transparent container, including the CounterSoR and the SoR header, and verifies whether it matches the SoR-MAC-IAUSF value received in the Registration Accept message. Based on the SoR-MAC-IAUSF verification outcome, the behaviour of the UE is specified in TS 23.122 [53].

13) If the UDM has requested an acknowledgement from the UE and the UE verified that the SoR transparent container received in step 12 has been provided by the HPLMN, then the UE shall send the Registration Complete message to the serving AMF. The UE shall generate the SoR-MAC-IUE as specified in Annex A.18 and includes the generated SoR-MAC-IUE in a SOR transparent container in the Registration Complete message.

14) The AMF sends a Nudm\_SDM\_Info request message to the UDM. If a transparent container with the SoR-MAC-IUE was received in the Registration Complete message, then if the AMF supports SoR transparent container, the AMF shall include the received SoR transparent container in SoR transparent container in the Nudm\_SDM\_Info request message, otherwise, the AMF shall include the SoR-MAC-IUE  in the received SoR transparent container in the Nudm\_SDM\_Info request message.

15) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information in step 10, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 10.

If the UDM supports Home triggered authentication (see clause 6.1.X), the UDM based on its local policy may decide to trigger a primary authentication to refresh the SoR counter based on the value of counter received in step 9.

\*\*\* END of 2nd CHANGE \*\*\*

**\*\***\*\* START OF 3rd CHANGES \*\*\***\***

6.15.2.1 Procedure for UE Parameters Update

The UDM may decide to perform UE parameters update anytime after the UE has been successfully authenticated and registered to the 5G system. The security procedure for the UE parameters update is described below in figure 6.15.2.1-1:

****

**Figure 6.15.2.1-1: Procedure for UE Parameters Update**

1) The UDM decides to perform the UE Parameters Update (UPU) using the control plane procedure while the UE is registered to the 5G system. If the final consumer of any of the UE parameters to be updated (e.g., the updated Routing ID Data) is the USIM, the UDM shall protect these parameters using a secured packet mechanism (see 3GPP TS 31.115 [65]) to update the parameters stored on the USIM. The UDM shall then prepare the UE Parameters Update Data (UPU Data) by including the parameters protected by the secured packet, if any, as well as any UE parameters for which final consumer is the ME (see TS 24.501 [35]).

2-3) The UDM shall invoke Nausf\_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-IAUSF and CounterUPU as specified in sub-clause 14.1.4 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the UDM decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall set the corresponding indication in the UE Parameters Update Data (see TS 24.501 [35]) and include the ACK Indication in the Nausf\_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-IUE, as specified in sub-clause 14.1.4 of this document.

The details of the CounterUPU is specified in sub-clause 6.15.2.2 of this document. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-IUE allows the UDM to verify that the UE received the UE Parameters Update Data correctly.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which includes the UPU transparent container if the AMF supports UPU transparent container, or includes individual IEs comprising the UE Parameters Update Data, UPU-MAC-IAUSF, CounterUPU within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected UPU-XMAC-IUE.

5) Upon receiving the Nudm\_SDM\_Notification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the transparent container if received from the UDM in step 4. Otherwise, if the UDM provided individual IEs in step 4, then the AMF shall construct a UPU transparent container.

6) On receiving the DL NAS Transport message, the UE shall calculate the UPU-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.19) on the received UE Parameters Update Data and the CounterUPU and verify whether it matches the UPU-MAC-IAUSF value received within the UPU transparent container in the DL NAS Transport message. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is protected by secured packet (see 3GPP TS 31.115 [65]), the ME shall forward the secured packet to the USIM using procedures in 3GPP TS 31.111 [66]. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is not protected by secure packet, the ME shall update its stored parameters with the received parameters in UDM Updata Data.

7) If the UDM has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the UDM, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the UPU-MAC-IUE as specified in Annex A.20 and include the generated UPU-MAC-IUE in a transparent container in the UL NAS Transport message.

8) If a transparent container with the UPU-MAC-IUE was received in the UL NAS Transport message, the AMF shall send a Nudm\_SDM\_Info request message with the transparent container to the UDM.

9) If the UDM indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall compare the received UPU-MAC-IUE with the expected UPU-XMAC-IUE that the UDM stored temporarily in step 4.

If the UDM supports Home triggered authentication (see clause 6.1.X), the UDM based on its local policy may decide to trigger a primary authentication to refresh the UPU counter based on the value of counter received in step 3.

\*\*\* END of 3rd CHANGE \*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 4th CHANGES \*\*\*\*\*\*\*\*\*\*\*\*

## 8.1 General

As described in TS 23.501 [2], in order to interwork with EPC, the UE can operate in Single Registration or Dual Registration mode.

When operating in Dual Registration mode, the UE shall independently maintain and use two different security contexts, an EPS security context to interact with the Evolved Packet System and a 5G security context to interact with the 5G System. Therefore, during inter-system mobility, when the target system is EPS, the UE shall take into use the EPS security context and hence all the security mechanisms described in TS 33.401 [10] are applicable. In the other direction, i.e. when the target system is the 5GC, the UE shall take into use the 5G security context and hence all the security mechanisms described in the present document are applicable.

When operating in Single Registration mode, there are two cases depending on the support of the N26 interface between the AMF and the MME. In both cases the security mechanisms described in all the subsequent sub-clauses are applicable.

Upon registration during mobility from EPS to 5GS, the UDM may decide to trigger the procedure defined in clause 6.1.X based on the local operator authentication policy.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 4th CHANGES\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 5th CHANGES \*\*\*\*\*\*\*\*\*\*\*\*

### 14.2.X Nudm\_UECM\_AuthTrigger service operation

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

Table 14.2.X-1: NF services for authentication trigger provided by UDM

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nudm\_UECM\_AuthTrigger | Auth Trigger | Request/Response | AAnF |

**Service operation name:** Nudm\_UECM\_AuthTrigger.

**Description:** This service operation allows the NF to request UDM to trigger a primary (re-)authentication as described in Clause 6.1.X.

**Input, Required:** SUPI.

**Input, Optional:** None.

**Output, Required:** Success/Failure.

**Output, Optional:** None.

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