**3GPP TSG-SA3 Meeting #108-e *Draft\_S3-222007-r1***

**e-meeting, 22 - 26 Aug 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1454** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  |
| *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 | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | control on NSSAA procedures for multi registrations in two PLMNs |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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 canbe 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:*** | Multiple simultaneous Network Slice Specific Authentication and Authorization (NSSAA) may get triggered by AMFs of different PLMNs because of following reasons:• UE may initiate a registration to an AMF of the second network, which may trigger a NSSAA on a S-NSSAI, before NSSAA of the S-NSSAI triggered in the first network has completed. If this happens the EAP layer in the UE will not be able to handle parallel EAP authentication with the same EAP server and EAP id. • From the network side, the AAA-S which is authenticating the UE for the network slice in the NSSAA procedure, may initiate reauthentication and reauthorization of the UE, technically anytime after the authentication for any reason. If this happens the NSSAAF may trigger either or both AMFs to initiate new NSSAA procedure(s). This may lead to race conditions in the UE involving AMFs in two networks.  |
|  |  |
| ***Summary of change:*** | Clarify behavior of UE and NSSAAF in NSSAA procedure for multi-registration scenario, especially in multi PLMNs case. |
|  |  |
| ***Consequences if not approved:*** | NSSAA may be failed in multi-registration scenario as the EAP layer in the UE is not able to handle parallel EAP authentication with the same EAP server and EAP id. |
|  |  |
| ***Clauses affected:*** | 16.2, 16.3, 16.4 |
|  |  |
|  | **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 the 1st change ##################

## 16.2 Authorization for network slice access

This clause specifies the relationship between primary authentication (as described in Clause 6.1) and authorization for network slice access (as described in TS 23.502 [8]) for a UE. Authorization from a home/serving PLMN is required for a UE to gain access to a network slice, identified by an S-NSSAI. An authorized S-NSSAI (i.e. allowed S-NSSAI) shall be granted to a UE only after the UE has completed successfully primary authentication. At the end of the primary authentication, the AMF and UE may receive a list of allowed S-NSSAI, which the UE is authorized to access.

For certain S-NSSAIs, additional Network Slice Specific Authentication and Authorization (NSSAA) is required. This clause in addition specifies the pre-requisite for an NSSAA procedure that is described in clause 16.3, with reference to the following figure 16.2-1.



Figure 16.2-1: Relationship between primary authentication and NSSAA

1. UE sends a Registration Request with a list of S-NSSAIs. UE shall not include those S-NSSAIs for which NSSAA procedures are ongoing, regardless of access types in one or more PLMNs (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2). If the UE is performing registration over one access and intends to perform registration over the other access in the different PLMN, the UE shall check the mapped S-NSSAIs of the pending NSSAI for the second PLMN.

2. For an initial Registration Request, the AMF/SEAF shall invoke Primary authentication as described in clause 6.1.2 of the present document. For a subsequent Registration Request, the Primary authentication may be skipped if the UE has already been authenticated and the AMF has valid security context.

3. AMF shall determine whether NSSAA is required for each of S-NSSAIs, based on information stored locally or from UDM. For example, the NSSAA for an S-NSSAI may be omitted

1) if it is not required based on the subscription information,

2) if UE has previously performed NSSAA successfully, regardless of access type and the result is still valid, or

3) NSSAA for UE is ongoing

4. AMF sends the Registration Accept message to the UE (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2, step 21). Optionally UE sends a Registration Complete.

5. The EAP based NSSAA procedure for each S-NSSAI if required, as determined in step 3, is executed in this step.

6. Based on the results of step 5, AMF sends UE Configuration Update to update the requested S-NSSAI status based on the NSSAA results.

The procedure for step 5, i.e., the NSSAA procedure is specified in clause 16.3.

################### end of the change ##################

################### start the 2nd change ##################

## 16.3 Network slice specific authentication and authorization

This clause specifies the optional-to-use NSSAA between a UE and an AAA server (AAA-S) which may be owned by an external 3rd party enterprise. NSSAA uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication.

The EAP framework specified in RFC 3748 [27] shall be used for NSSAA between the UE and the AAA server. The SEAF/AMF shall perform the role of the EAP Authenticator and communicates with the AAA-S via the NSSAAF. The NSSAAF undertakes any AAA protocol interworking with the AAA-S. Multiple EAP methods are possible for NSSAA. If the AAA-S belongs to a third party the NSSAAF contacts the AAA-S via a AAA-P. The NSSAAF and the AAA-P may be co-located.

To protect privacy of the EAP ID used for the EAP based NSSAA, a privacy-protection capable EAP method is recommended, if privacy protection is required.

The steps involved in NSSAA are described below.



Figure 16.3-1: NSSAA procedure

1. For S-NSSAIs that are requiring NSSAA, based on change of subscription information, or triggered by the AAA-S, the AMF may trigger the start of the NSSAA procedure.

 If NSSAA is triggered as a result of Registration procedure, the AMF may determine, based on UE Context in the AMF, that for some or all S-NSSAI(s) subject to NSSAA, the UE has already been authenticated following a Registration procedure on a first access. Depending on NSSAA result (e.g. success/failure) from the previous Registration, the AMF may decide, based on Network policies, to skip NSSAA for these S-NSSAIs during the Registration on a second access.

 If the NSSAA procedure corresponds to a re-authentication and re-authorization procedure triggered as a result of AAA Server-triggered UE re-authentication and re-authorization for one or more S-NSSAIs, as described in clause 16.4, or triggered by the AMF based on operator policy or a subscription change and if S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization are included in the Allowed NSSAI for each Access Type, the AMF selects an Access Type to be used to perform the NSSAA procedure based on network policies.

2. The AMF may request the UE User ID for EAP authentication (EAP ID) for the S-NSSAI in a NAS MM Transport message including the S-NSSAI.

3. The UE provides the EAP ID for the S-NSSAI alongside the S-NSSAI in an NAS MM Transport message towards the AMF.

4. The AMF sends the EAP ID to the NSSAAF which provides interface with the AAA, in an Nnssaaf\_NSSAA\_Authenticate Request (EAP ID Response, GPSI, S-NSSAI).

5. If the AAA-P is present (e.g. because the AAA-S belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF forwards the EAP ID Response message to the AAA-P, otherwise the NSSAAF forwards the message directly to the AAA-S. NSSAAF routes to the AAA-S based on the S-NSSAI. The NSSAAF/AAA-P forwards the EAP Identity message to the AAA-S together with S-NSSAI and GPSI. The AAA-S stores the GPSI to create an association with the EAP ID in the EAP ID response message so the AAA-S can later use it to revoke authorisation or to trigger reauthentication. The AAA-S uses the EAP-ID and S-NSSAI to identify for which UE and slice authorisation is requested.

NOTE 1: If the NSSAAF detects that there is an ongoing NSSAA for the same GPSI and S-NSSAI, the NSSAAF sends Nnssaaf\_NSSAA\_Authenticate Response (Failure, S-NSSAI, GPSI) to the AMF with failure cause to indicate ongoing authentication.

NOTE 2: If the AAA-S belongs to the 3rd party, the NSSAAF optionally maps the S-NSSAI to External Network Slice Information (ENSI), and forwards the EAP Identity message to the AAA-S together with ENSI and GPSI. In this case, the AAA-S uses the EAP-ID and ENSI to identify the UE for which slice authorisation is requested.

6 -11. EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

12. EAP authentication completes. An EAP-Success/Failure message is delivered to the NSSAAF/AAA-P along with GPSI and S-NSSAI/ENSI.

13. The NSSAAF sends the Nnssaaf\_NSSAA\_Authenticate Response (EAP-Success/Failure, S-NSSAI, GPSI) to the AMF.

14. The AMF transmits a NAS MM Transport message (EAP-Success/Failure) to the UE.

15. Based on the result of Slice specific authentication (EAP-Success/Failure), if a new Allowed NSSAI or new Rejected NSSAIs needs to be delivered to the UE, or if the AMF re-allocation is required, the AMF initiates the UE Configuration Update procedure, for each Access Type, as described in clause 4.2.4.2 of TS 23.502 [8].

If the NSSAA procedure can not be completed (e.g. due to server error or UE becoming unreachable), the AMF sets the status of the corresponding S-NSSAI subject to Network Slice-Specific Authentication and Authorization in the UE context as defined in TS 29.526 [96], so that an NSSAA is executed next time the UE requests to register with the S-NSSAI.

################### end of the change ##################

################### start the 3rd change ##################

## 16.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure



Figure 16.4-1: AAA Server initiated Network Slice-Specific Re-authentication and Re-authorization procedure

0. The UE is registered in 5GC via an AMF. The AMF ID is stored in the UDM.

1. The AAA-S requests the re-authentication and re-authorization for the Network Slice specified by the S-NSSAI/ENSI in the Re-Auth Request message, for the UE identified by the GPSI in this message. This message is sent to an AAA-P, if the AAA-P is used (e.g. the AAA Server belongs to a third party), otherwise it may be sent directly to the NSSAAF. If an AAA-P is present, the AAA-P relays the Reauthentication Request to the NSSAAF.

2. The NSSAAF checks whether the AAA-S is authorized to request the re-authentication and re-authorization by checking the local configuration of AAA-S address per S-NSSAI. If success,the NSSAAF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE.

3. The NSSAAF provides an acknowledgement to the AAA protocol Re-Auth Request message. If the AMF is not registered in UDM the procedure is stopped here.

4. If the AMF is registered in UDM, the NSSAAF requests the relevant AMF to re-authenticate/re-authorize the S-NSSAI for the UE using the Nnssaaf\_NSSAA\_Re-authenticationNotification service operation. The AMF is implicitly subscribed to receive Nnssaaf\_NSSAA\_Re-authenticationNotification service operations. The NSSAAF may discover the Callback URI for the Nnssaaf\_NSSAA\_Re-authenticationNotification service operation exposed by the AMF via the NRF.

The AMF acknowledges the notification of Re-authentication request.

NOTE: If NSSAAF receives two different AMF addresses from the UDM, the NSSAAF notifies one AMF first, then may notify the other AMF after completed the first re-authentication.

5. If the UE is registered with the S-NSSAI in the Mapping Of Allowed NSSAI, the AMF triggers the NSSAA procedure defined in clause 16.3 for the UE identified by the GPSI and the Network Slice identified by the S-NSSAI received from the NSSAAF.

If the UE is registered but the S-NSSAI is not in the Mapping Of Allowed NSSAI, the AMF removes any status of the corresponding S-NSSAI subject to Network Slice-Specific Authentication and Authorization in the UE context it may have kept, so that an NSSAA is executed next time the UE requests to register with the S-NSSAI.

################### end of the change ##################