**3GPP TSG-SA3 Meeting #104-e *S3-213012-r2***

**e-meeting,** **16 – 26 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33501** | **CR** | **1199** | **rev** | **2** | **Current version:** | **16.7.1** |  |
|  |
| *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:***  | Recovering NSSAI and ENSI mapping (Rel-16) |
|  |  |
| ***Source to WG:*** | S3 |
| ***Source to TSG:*** | Samsung |
|  |  |
| ***Work item code:*** | eNS |  | ***Date:*** | 2021-07-10 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-16 |
|  | *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:*** | It was agreed that if AAA-S belongs to third party then S-NSSAI may not be exposed. Hence, NSSAAF will internally map the S-NSSAI to ENSI and share the ENSI with AAA-S. Stage 3 specification has mentioned that Slice specific context is implementation dependent and may be kept for configured time. If this mapping data at NSSAAF is not found while reauthentication, re-authorization or revocation is triggered from AAA-S, then NSSAAF won’t be able to retrieve the NSSAI from ENSI and the procedure will fail. |
|  |  |
| ***Summary of change:*** | It is proposed that: 1. NSSAAF stores the mapping of ENSI and S-NSSAI locally and fetches it during re-authentication and revocation.
2. NSSAAF also stores the mapping information (S-NSSAI abd ENSI) in UDM. During reauthentication, re-authorization and revocation procedure, when NSSAAF does not find the mapping info, it requests UDM to fetch the mapping info. After it fetches from UDM this mapping is again stored at locally so that for future operation it will not request the UDM again.
 |
|  |  |
| ***Consequences if not approved:*** | If the NSSAAF won’t be able to retrieve the NSSAI from ENSI, then re-authentication, re-authorization and revocation procedures will fail. |
|  |  |
| ***Clauses affected:*** | 16.3; 16.4; 16.5 |
|  |  |
|  | **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 the changes \*\*\*\*\*\*\*\*\*\*

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 4.2.9.2 of TS 23.502 [8], 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 : If the AAA-S belongs to the 3rd party, the NSSAAF optionally maps the S-NSSAI to External Network Slice Inforamtion (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. The NSSAAF stores the mapping information locally and in UDM.

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].

\*\*\*\*\*\*\*\*\*\* Next 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 by verifying 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, ENSI) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE. If NSSAAF does not find the mapping information (S-NSSAI and ENSI) then it fetches from UDM.

3. 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.

4. 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.

\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*

16.5 AAA Server triggered Slice-Specific Authorization Revocation

****

**Figure 16.5-1: AAA Server-initiated Network Slice-Specific Authorization Revocation procedure**

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

1. The slice specific AAA-S requests the revocation of authorization for the Network Slice identified by the GPSI in the AAA Protocol Revoke Authorization Request message. This message is sent to NSSAAF instance interfacing with AAA-S or AAA-P if it is used.

The AAA-P, if present, relays the request to the NSSAAF.

2. The NSSAAF checks whether the AAA-S is authorized to request the revocation by verifying 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, ENSI) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE. If NSSAAF does not find the mapping information (S-NSSAI and ENSI) then it fetches from UDM.3. The NSSAAF request the relevant AMF to revoke the S-NSSAI authorization for the UE using the Nnssaaf\_NSSAA\_RevocationNotification service operation.

The AMF is implicitly subscribed to receive Nnssaaf\_NSSAA\_RevocationNotification service operations. The NSSAAF may discover the Callback URI for the Nnssaaf\_NSSAA\_RevocationNotification service operation exposed by the AMF via the NRF. The AMF acknowledges the Notification of Revocation request.

4. The NSSAAF sends an acknowledgement to the the AAA-S/AAA-P with AAA Protocol Revoke Authorization Response message.

5. The AMF sends the UE Configuration Update message to revoke the S-NSSAI from the current Allowed NSSAI, for any Access Type for which NSSAA had been successfully run on this S-NSSAI. The AMF provides a new Allowed NSSAI to the UE by removing the S-NSSAI for which authorization has been revoked. The AMF provides new rejected NSSAIs to the UE including the S-NSSAI for which authorization has been revoked. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and a Default NSSAI exists that requires no NSSAA or for which a NSSAA did not previously fail over this access, then the AMF may provide a new Allowed NSSAI to the UE containing the Default NSSAI. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

\*\*\*\*\*\*\*\*\*\* End of changes \*\*\*\*\*\*\*\*\*\*