**3GPP TSG-WG SA2 Meeting #139E e-meeting  *S2-20xxxxx***

**Elbonia, June 1 – 5, 2020 (Phase-1) (revision of S2-200xxxx)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.502** | **CR** | **YYYY** | **rev** | **-**  | **Current version:** | **16.4.0** |  |
|  |
| *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:***  | Replacing AUSF by NSSAAF to support NSSAA  |
|  |  |
| ***Source to WG:*** | ZTE, Ericsson, Nokia, Nokia Shanghai Bell. |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNS |  | ***Date:*** | 2020-05-10 |
|  |  |  |  |  |
| ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | After thorough analysis, SA3 has decided on the security requirement to fully isolate the following two SBA Authentication service types, * primary authentication services towards UDM currently supported by AUSF
* NSSAA services involving interactions with a AAA-S

As a result, the NSSAA SBI services used by the AMF shall be hosted by a new NF, i.e. NSSAA Function (NSSAAF), to provide the NSSAA related services. From a specification point of view, this will require the definition of a new NF within the SBA architecture. From AMF point of view, this requires that AMF selects the new NF in the HPLMN when an NSSAA service is invoked. |
|  |  |
| ***Summary of change:*** | Introducing the new NSSAAF into Rel-17 network architecture and adding/updating the corresponding clauses for this new NF. |
|  |  |
| ***Consequences if not approved:*** | Fail to align the stage-2 architecture and solutions with stage-3 for Rel-16 to support network slice specific authentication. |
|  |  |
| ***Clauses affected:*** | 4.2.9, 4.2.9.1, 4.2.9.2, 4.2.9.3, 4.2.9.4, 5.2.10, 5.2.10.1, 5.2.10.5, 5.2.10.5.1, 5.2.10.5.2, 5.2.10.5.3 |
|  |  |
|  | **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:*** |  |

\* \* \* \* First change \* \* \* \*

### 4.2.9 Network Slice-Specific Authentication and Authorization procedure

#### 4.2.9.1 General

The Network Slice-Specific Authentication and Authorization procedure is triggered for an S-NSSAI requiring Network Slice-Specific Authentication and Authorization with an AAA Server (AAA-S) which may be hosted by the H-PLMN operator or by a third party which has a business relationship with the H-PLMN, using the EAP framework as described in TS 33.501 [15]. An AAA Proxy (AAA-P) in the HPLMN may be involved e.g. if the AAA Server belongs to a third party.

This procedure is triggered by the AMF during a Registration procedure when some Network Slices require Slice-Specific Authentication and Authorization, when AMF determines that Network Slice-Specific Authentication and Authorization is requires for an S-NSSAI in the current Allowed NSSAI (e.g. subscription change), or when the AAA Server that authenticated the Network Slice triggers a re-authentication.

The AMF performs the role of the EAP Authenticator and communicates with the AAA-S via the Network Slice Specific Authentication and Authorization Function, NSSAAF. The NSSAAF undertakes any AAA protocol interworking with the AAA protocol supported by the AAA-S.

#### 4.2.9.2 Network Slice-Specific Authentication and Authorization



Figure 4.2.9.2-1: Network Slice-Specific Authentication and Authorization procedure

1. For S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization, based on change of subscription information, or triggered by the AAA-S, the AMF may trigger the start of the Network Slice Specific Authentication and Authorization procedure.

 If Network Slice Specific Authentication and Authorization 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 Network Slice Specific Authentication and Authorization, the UE has already been authenticated following a Registration procedure on a first access. Depending on Network Slice Specific Authentication and Authorization result (e.g. success/failure) from the previous Registration, the AMF may decide, based on Network policies, to skip Network Slice Specific Authentication and Authorization for these S-NSSAIs during the Registration on a second access.

 If the Network Slice Specific Authentication and Authorization 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 4.2.9.2, 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 Network Slice Specific Authentication and Authorization procedure based on network policies.

2. The AMF may send an EAP Identity Request for the S-NSSAI in a NAS MM Transport message including the S-NSSAI. This is the S-NSSAI of the H-PLMN, not the locally mapped S-NSSAI value.

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

4. The AMF sends the EAP Identity Response to the NSSAAF in a Nnssaaf\_NSSAA\_Authenticate Request (EAP Identity Response, AAA-S address, 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. The NSSAAF uses towards the AAA-P or the AAA-S an AAA protocol message of the same protocol supported by the AAA-S.

6. The AAA-P forwards the EAP Identity message to the AAA-S addressable by the AAA-S address together with S-NSSAI and GPSI. The AAA-S stores the GPSI to create an association with the EAP Identity in the EAP ID response message, so the AAA-S can later use it to revoke authorization or to trigger reauthentication.

7-14. EAP-messages are exchanged with the UE. One or more than one iteration of these steps may occur.

15. EAP authentication completes. The AAA-S stores the S-NSSAI for which the authorisation has been granted, so it may decide to trigger reauthentication and reauthorization based on its local policies. An EAP-Success/Failure message is delivered to the AAA-P (or if the AAA-P is not present, directly to the NSSAAF) with GPSI and S-NSSAI.

16. If the AAA-P is used, the AAA-P sends an AAA Protocol message including (EAP-Success/Failure, S-NSSAI, GPSI) to the NSSAAF.

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

18. The AMF transmits a NAS MM Transport message (EAP-Success/Failure) to the UE. The AMF shall store the EAP result for each S-NSSAI for which the NSSAA procedure in steps 1-17 was executed.

19a. [Conditional] If a new Allowed NSSAI (i.e. including any new S-NSSAIs in a Requested NSSAI for which the NSSAA procedure succeeded and/or excluding any S-NSSAI(s) in the existing Allowed NSSAI for the UE for which the procedure has failed) and/or new Rejected S-NSSAIs (i.e. including any S-NSSAI(s) in the existing Allowed NSSAI for the UE for which the procedure has failed, or any new requested S-NSSAI(s) for which the NSSAA procedure failed) need 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.

19b. [Conditional] If the Network Slice-Specific Authentication and Authorization fails for all S-NSSAIs (if any) in the existing Allowed NSSAI for the UE and (if any) for all S-NSSAIs in the Requested NSSAI, the AMF shall execute the Network-initiated Deregistration procedure described in clause 4.2.2.3.3, or reject the UE Registration Request (if that was the trigger for this procedure), and it shall include in the explicit De-Registration Request or Registration Reject message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value. If the Network Slice-Specific Re-Authentication and Re-Authorization fails and there are PDU session(s) established that are associated with the S-NSSAI for which the NSSAA procedure failed, the AMF shall initiate the PDU Session Release procedure as specified in clause 4.3.4 to release the PDU sessions with the appropriate cause value.

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



Figure 4.2.9.3-1: AAA Server initiated Network Slice-Specific Re-authentication and Re-authorization procedure

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

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

3a-3b. NSSAAF gets AMF ID from UDM using Nudm\_UECM\_Get with the GPSI in the received AAA message.

4. The NSSAAF notifies Re-auth event to the AMF to re-authenticate/re-authorize the S-NSSAI for the UE using Nnssaaf\_NSSAA\_Notify with the GPSI and S-NSSAI in the received AAA message. The callback URI of the notification for the AMF is derived via NRF as specified in TS 29.501 [62].

5. The AMF triggers the Network Slice-Specific Authentication and Authorization procedure defined in clause 4.2.9.1.

#### 4.2.9.4 AAA Server triggered Slice-Specific Authorization Revocation



Figure 4.2.9.4-1: AAA Server-initiated Network Slice-Specific Authorization Revocation procedure

1. The AAA-S requests the revocation of authorization for the Network Slice specified by the S-NSSAI in the AAA protocol Revoke Auth Request message, for the UE identified by the GPSI in this message. This message is sent to AAA-P if it is used.

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

3a-3b. NSSAAF gets AMF ID from UDM using Nudm\_UECM\_Get with the GPSI in the received AAA message.

4. The NSSAAF notifies Revoke Auth event to the AMF to revoke the S-NSSAI authorization for the UE using Nnssaaf\_NSSAA\_Notify with the GPSI and S-NSSAI in the received AAA message. The callback URI of the notification for the AMF is derived via NRF as specified in TS 29.501 [62].

5. The AMF updates the UE configuration to revoke the S-NSSAI from the current Allowed NSSAI, for any Access Type for which Network Slice Specific Authentication and Authorization had been successfully run on this S-NSSAI. The UE Configuration Update may include a request to Register if the AMF needs to be re-allocated. 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 Network Slice Specific Authentication or for which a Network Slice Specific Authentication 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 Network Slice Specific Authentication failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in clause 4.2.2.3.3, 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. If there are PDU session(s) established that are associated with the revoked S-NSSAI, the AMF shall initiate the PDU Session Release procedure as specified in clause 4.3.4 to release the PDU sessions with the appropriate cause value.

\* \* \* \* Second change \* \* \* \*

### 5.2.10 AUSF Services

#### 5.2.10.1 General

The following table illustrates the AUSF Services.

Table 5.2.10.1-1: List of AUSF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | OperationSemantics | Example Consumer(s) |
| Nausf\_UEAuthentication | Authenticate | Request/Response | AMF |
| Nausf\_SoRProtection | Protect | Request/Response | UDM |
| Nausf\_UPUProtection | Protect | Request/Response | UDM |
|  |  |  |  |
|  |  |  |  |

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

#### 5.2.10.5 Void

\* \* \* \* Third change \* \* \* \*

### 5.2.x Nnssaaf\_NSSAA service

#### 5.2.x.1 General

The following table illustrates the NSSAAF Services.

Table 5.2.x-1: List of NSSAAF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | OperationSemantics | Example Consumer(s) |
| Nnssaaf\_NSSAA | Authenticate | Request/Response | AMF |
|  | Notify | Subscribe/Notify | AMF |

#### 5.2.x.2 Nnssaaf\_\_NSSAA service

##### 5.2.x.2.1 General

**Service Description:** the NSSAAF provides Network Slice- Specific Authentication and Authorization (NSSAA) service to the requester NF by relaying EAP messages towards a AAA-S or AAA-P and performing related protocol conversion as needed. It also provides notification to the current AMF where the UE is of the need to re-authenticate and re-authorize the UE or to revoke the UE authorization. The AMF to receive the notification is implicitly subscribed and it is found in the UDM by providing the UE GPSI.

##### 5.2.x.2.2 Nnssaaf\_\_NSSAA\_Authenticate service operation

See TS 33.501 [15].

##### 5.2.x.2.3 Nnssaaf\_NSSAA\_Notify service operation

See TS 33.501 [15].

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