**3GPP TSG-SA3 Meeting #98e *S3-200500***

**e-meeting, 2 – 6 March 2020** was S3-200117

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** |  | **rev** |  | **Current version:** | 16.0.0 |  |
|  |
| *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 | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Draft CR for network slice specific authentication procedures’ |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson, Huawei, HiSilicon, InterDigital, |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNS-SEC |  | ***Date:*** | 25/11/2019 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | R16 |
|  | *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:*** | Addition of security procedures for network slices. |
|  |  |
| ***Summary of change:*** | SA3#98e: No new content added or changed.SA3#97:S3-194536, S3-194537, S3-194538, S3-194539, S3-194540 merged. Content for clauses x.2, x.3, x.4 tentatively agreed. Text for Nausf\_NSSAA services tentatively agreed. All clauses may need further correction and enhancement.SA3#96 ad-hoc: A new subclause for network slice security opened. |
|  |  |
| ***Consequences if not approved:*** | Security procedures for network slices are not supported. |
|  |  |
| ***Clauses affected:*** | New clause? |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **n** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **n** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **n** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# x Security procedures for network slices

### x.x.1 General

This clause specifies the security procedures for network slices.

### x.x.2 Authorization for network slice access

Editor’s Note: The text in this clause needs to be revised to capture the following three ordered points;

firstly that a successful primary authentication to gain access to the network is a pre-requisite for authorisation for a slice,

secondly the authorisation information for the UE for accessing a slice is downloaded from the UDM to the AMF and

finally the downloaded authorisation for a slice indicates whether a slice authentication is required in addition to the primary authentication.

This clause specifies the relationship between primary authentication (as described in Clause 6.1) and authorization for network slice access (as described in TS23.502 [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 NSSAA procedure that will be described in section x.x.3, with reference to the following figure x.x.2-1.



Figure x.x.2-1: Relationship between primary authentication and slice-specific authentication and authorization

1. UE sends a Registration Request with a list of S-NSSAIs. UE shall not include those S-NSSAIs for which SSAA is ongoing, regardless of access type (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2).
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 slice-specific authentication and authorization is required for each of S-NSSAI, based on information stored locally or from UDM. For example, the network slice-specific authentication for an S-NSSAI may be omitted

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

2)if UE has previously performed network slice-specific authentication successfully, regardless of access type and the result is still valid, or

3)network slice-specific authentication for UE is ongoing

1. AMF sends UE the Registration Accept message and 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.
2. EAP based slice-specific authentication and authorization 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 slice-specific authentication results.

The procedure for step 5, i.e., the slice-specific authentication and authorizaiton procedure is specified in clause x.x.3.

### x.x.3 Network Slice specific authentication

This clause specifies the optional-to-use Network slice-specific authentication and authorization between a UE and an AAA server (AAA-S). Network slice-specific authentication and authorization 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 Network slice-specific authentication and authorization 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 AUSF. The AUSF undertakes any AAA protocol interworking with the AAA protocol supported by the AAA-S. Multiple EAP methods are possible.

To protect privacy of the EAP ID used for the EAP based Network Slice Specific Authentication and Authoriztation, a privacy-protection capable EAP method is recommended, if privacy protection is required.

The steps involved in network slice specific authentication and authorization are described below.

****

**Figure X-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 request the UE User ID for EAP authentication (EAP ID) 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 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 AUSF in a Nausf\_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 AUSF forwards the EAP ID Response message to the AAA-P, otherwise the AUSF forwards the message directly to the AAA-S. The AUSF uses towards the AAA-P or the AAA-S an AAA protocol message of the same protocol supported by the AAA-S. AUSF knows which AAA-S to use for each S-NSSAI (e.g. based on local configuration).

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 authorisation or to trigger reauthentication. The AAA-S uses the S-NSSAI to identify for which S-NSSAI authorisation is requested. The AAA-S stores the S-NSSAIs for which the authorisation has been provided so it may decide to trigger reauthentication and reauthorization and/or revocation based on its local policies.

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

15. EAP authentication completes. An EAP-Success/Failure message is delivered to the AAA-P (or if the AAA-P is not present, directly to the AUSF) with GPSI and S-NSSAI.

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

17. The AUSF sends the Nausf\_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.

19. 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. If the Network Slice-Specific Authentication and Authorization fails for all S-NSSAIs in the Allowed NSSAI, the AMF shall execute the Network-initiated Deregistration procedure 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

Editor’s Note: This call flow needs further alignment with SA2

Editor’s Note: The msg name EAP ID in the flow needs alignment for clarity.

Editor’s Note: It is ffs whether AUSF is involved in the call flow and whether S-NSSAIs can be sent to AAA-S.

x.x.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure

Editor’s Note: Further detail and alignment with SA2 callflows are FFS.

****

**Figure X.X.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 in the 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 may be sent directly to the AUSF.

2. The AAA-P, if present, relays the AAA Protocol Reauthentication Request to the AUSF.

3. The AUSF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the AUSF with the AMF ID of the AMF serving the UE.

4. The AUSF requests the relevant AMF to re-authenticate/re-authorize the S-NSSAI for the UE using the Nausf\_NSSAA\_Re-authenticationNotification service operation.

The AMF is implicitly subscribed to receive Nausf\_NSSAA\_Re-authenticationNotification service operations. The AUSF may discover the Callback URI for the Nausf\_NSSAA\_Re-authenticationNotification service operation exposed by the AMF via the NRF.

The AMF acknowledges the notification of Re-authentication request.

5. The AMF triggers the Network Slice-Specific Authentication and Authorization procedure defined in clause X.X.3 for the UE identified by the GPSI and the Network Slice identified by the S-NSSAI received from the AUSF.

X.X.5 AAA Server triggered Slice-Specific Authorization Revocation

Editor’s Note: Further detail and alignment with SA2 callflows are FFS.

****

**Figure 4.2.9.4-1: 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 AAA-S requests the revocation of authorization for the Network Slice specified by the S-NSSAI in the AAA Protocol Revoke Authorization 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 AUSF.

3. The AUSF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the AUSF with the AMF ID of the AMF serving the UE.

4. The AUSF request the relevant AMF to revoke the S-NSSAI authorization for the UE using the Nausf\_NSSAA\_RevocationNotification service operation.

The AMF is implicitly subscribed to receive Nausf\_NSSAA\_RevocationNotification service operations. The AUSF may discover the Callback URI for the Nausf\_NSSAA\_RevocationNotification service operation exposed by the AMF via the NRF.

The AMF acknowledges the Notification of Revocation request.

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 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 1st change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

14.1.1 General

Editor’s Note: This clause needs further alignment with SA2.

The AUSF provides UE authentication service to the requester NF by Nausf\_UEAuthentication for primary authentication and Nausf\_NSSAA for Network Slice Specific Authentication and Authorization. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. Clause 14.1.2 describes the Nausf\_UEAuthentication\_Authenticate service operation. Clause 14.1.X describes the service operations related to the Nausf\_NSSAA service. The services listed here are used in procedures that are described in clause 6 and clause Z of the present document.

Since AUSF is completely security-related, all service operations are described in the present document. TS 23.501 [2], clause 7.2.7, only lists the services and TS 23.502 [8], clause 5.2.10, provides the reference to the present document.

 \*\*\* End of 2nd Change \*\*\*

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

14.1.X Nausf\_NSSAA services

Editor’s Note: This clause needs further alignment with SA2.

The following table illustrates the security related services for Network Slice Specific Authentication and Authorisation that AUSF provides.

**Table 14.1.3-1: NF services for the NSSAA service provided by AUSF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name** | **Service Operations** | **Operation Semantics** | **Example Consumer(s)** |
| Nausf\_NSSAA | Authenticate | Request/Response | AMF |
| Re-AuthenticationNotification | Notify | AMF |
| RevocationNotification | Subscribe/Notify | AMF |

14.1.X.1 Nausf\_NSSAA\_Authenticate service operation

**Service operation name:** Nausf\_NSSAA\_Authenticate

**Description:** NF requester requires AUSF to relay Network Slice specific authentication messages towards the corresponding AAA-S handling the Network Slice specific authentication for the requested S-NSSAI.

**Input, Required:**

1. In the initial NSSAA requests: EAP ID Response, GPSI, S-NSSAI
2. In subsequent NSSAA requests: EAP message, GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** EAP message, GPSI, S-NSSAI

**Output, Optional:** None

14.1.X.2 Nausf\_NSSAA\_Re-AuthenticationNotification service operation

**Service operation name:** Nausf\_NSSAA\_Re-AuthenticationNotification

**Description:** AUSFnotifies the NF consumer to trigger a Network Slice specific reauthentication procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nausf\_NSSAA\_Re-authenticationNotification service operations.

**Input, Required:** GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

14.1.X.3 Nausf\_NSSAA\_RevocationNotification service operation

**Service operation name:** Nausf\_NSSAA\_RevocationNotification

**Description:** AUSFnotifies the NF consumer to trigger a Network Slice specific revocation procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nausf\_NSSAA\_RevocationNotification service operations.

**Input, Required:** GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

\*\*\* END OF 3rd CHANGE \*\*\*