**3GPP TSG-SA2 Meeting # 147E** **(e-meeting) *S2-2107182r01***

 **Elbonia, October 18 - 22, 2021 (revision of)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **3254** | **rev** | **-** | **Current version:** | **17.2.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Clarification on Remote provisioning of credentials – User Plane |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNPN  |  | ***Date:*** | 2021-10-11 |
|  |  |  |  |  |
| ***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:*** | Section 5.39 defines the Remote provisioning of credentials for NSSAA or secondary authentication/authorization using UP procedure. It is however not specified when a UE triggers the procedure to be provisioned with the credentials used for NSSAA or secondary authentication/authorization over UP remote provisioning.  |
|  |  |
| ***Summary of change:*** | It is clarified when the UE triggers the procedure to be provisioned with the credentials used for NSSAA or secondary authentication/authorization over UP remote provisioning.The proposed updates do not have any impact on the procedures for NSSAA, secondary authentication/authorization or UP remote provisioning defined in TS 23.502.  |
|  |  |
| ***Consequences if not approved:*** | Incomplete/Unclear specification |
|  |  |
| ***Clauses affected:*** | 5.6.6, 5.15.10 |
|  |  |
|  | **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 CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.6.6 Secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session

At PDU Session Establishment to a DN:

- The DN-specific identity (TS 33.501 [29]) of a UE may be authenticated/authorized by the DN.

NOTE 1: the DN-AAA server may belong to the 5GC or to the DN.

- If the UE provides authentication/authorization information corresponding to a DN-specific identity during the Establishment of the PDU Session, and the SMF determines that Secondary authentication/authorization of the PDU Session Establishment is required based on the SMF policy associated with the DN, the SMF passes the authentication/authorization information of the UE to the DN-AAA server via the UPF if the DN-AAA server is located in the DN. If the SMF determines that Secondary authentication/authorization of the PDU Session Establishment is required but the UE has not provided a DN-specific identity as part of the PDU Session Establishment request, the SMF requests the UE to indicate a DN-specific identity using EAP procedures as described in TS 33.501 [29]. If the Secondary authentication/authorization of the PDU Session Establishment fails, the SMF rejects the PDU Session Establishment.

NOTE 2: If the DN-AAA server is located in the 5GC and reachable directly, then the SMF may communicate with it directly without involving the UPF.

- The DN-AAA server may authenticate/authorize the PDU Session Establishment.

- When DN-AAA server authorizes the PDU Session Establishment, it may send DN Authorization Data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:

- A DN Authorization Profile Index which is a reference to authorization data for policy and charging control locally configured in the SMF or PCF.

- a list of allowed MAC addresses for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.

- a list of allowed VLAN tags for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.

- DN authorized Session AMBR for the PDU Session. The DN Authorized Session AMBR for the PDU Session takes precedence over the subscribed Session-AMBR received from the UDM.

- Framed Route information (see clause 5.6.14) for the PDU Session.

- L2TP information, such as LNS IP address and/or LNS host name, as described in TS 29.561 [132].

SMF policies may require DN authorization without Secondary authentication/authorization. In that case, when contacting the DN-AAA server for authorization, the SMF provides the GPSI of the UE if available.

Such Secondary authentication/authorization takes place for the purpose of PDU Session authorization in addition to:

- The 5GC access authentication handled by AMF and described in clause 5.2.

- The PDU Session authorization enforced by SMF with regards to subscription data retrieved from UDM.

Based on local policies the SMF may initiate Secondary authentication/authorization at PDU Session Establishment. The SMF provides the GPSI, if available, in the signalling exchanged with the DN-AAA during Secondary authentication/authorization.

After the successful Secondary authentication/authorization, a session is kept between the SMF and the DN-AAA.

The UE provides the authentication/authorization information required to support Secondary authentication/authorization by the DN over NAS SM.

If a UE is configured with DNNs, which are subject to secondary authentication/authorization, the UE stores an association between the DNN and corresponding credentials for the secondary authentication/authorization.

NOTE X: How the UE is aware that a DNN is subject to secondary authentication/authorization (e.g., based on local configuration) is out of scope of this specification.

The UE may support remote provisioning of credentials for secondary authentication/authorization, as specified in clause 5.39.

A UE that supports to be provisioned with the credentials used for secondary authentication/authorization over UP remote provisioning shall use connectivity over an S-NSSAI/DNN which can access the provisioning server to establish a PDU session for remote provisioning as defined in clause 5.39.

NOTE Y: The credentials for secondary authentication/authorization are not specified.

SMF policies or subscription information (such as defined in Table 5.2.3.3.1 of TS 23.502 [3]) may trigger the need for SMF to request the Secondary authentication/authorization and/or UE IP address / Prefix from the DN-AAA server.

When SMF adds a PDU Session Anchor (such as defined in clause 5.6.4) to a PDU Session Secondary authentication/authorization is not carried out, but SMF policies may require SMF to notify the DN when a new prefix or address has been added to or removed from a PDU Session or N6 traffic routing information has been changed for a PDU Session.

When SMF gets notified from UPF with the addition or removal of MAC addresses to/from a PDU Session, the SMF policies may require SMF to notify the DN-AAA server.

Indication of PDU Session Establishment rejection is transferred by SMF to the UE via NAS SM.

If the DN-AAA sends DN Authorization Data for the authorized PDU Session to the SMF and dynamic PCC is deployed, the SMF sends the PCF the DN authorized Session AMBR and/or DN Authorization Profile Index in the DN Authorization Data for the established PDU Session.

If the DN-AAA sends DN Authorization Profile Index in DN Authorization Data to the SMF and dynamic PCC is not deployed, the SMF uses the DN Authorization Profile Index to refer the locally configured information.

NOTE 4: DN Authorization Profile Index is assumed to be pre-negotiated between the operator and the administrator of DN-AAA server.

If the DN-AAA does not send DN Authorization Data for the established PDU Session, the SMF may use locally configured information.

At any time, a DN-AAA server may revoke the authorization for a PDU Session or update DN Authorization Data for a PDU Session. According to the request from DN-AAA server, the SMF may release or update the PDU Session. See clause 5.6.14 when the update involves Framed Route information.

At any time, a DN-AAA server or SMF may trigger Secondary Re-authentication procedure for a PDU Session established with Secondary Authentication as specified in clause 11.1.3 of TS 33.501 [29].

During Secondary Re-authentication/Re-authorization, if the SMF receives from DN-AAA the DN authorized Session AMBR and/or DN Authorization Profile Index, the SMF shall report the received value(s) to the PCF.

The procedure for secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session is described in clause 4.3.2.3 of TS 23.502 [3].

The support for L2TP on N6 is further specified in clause 5.8.2.16, and the procedure for establishment of L2TP tunnelling on N6 for a PDU Session is described in clause 4.3.2.4 of TS 23.502 [3].

NOTE 5: The L2TP Tunnel information sent to the SMF can e.g., be provisioned in the DN-AAA server per DNN/S-NSSAI or per SUPI or GPSI.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.15.10 Network Slice-Specific Authentication and Authorization

A serving PLMN shall perform Network Slice-Specific Authentication and Authorization for the S-NSSAIs of the HPLMN which are subject to it based on subscription information. The UE shall indicate in the Registration Request message in the UE 5GMM Core Network Capability whether it supports NSSAA feature. If the UE does not support NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, the AMF shall not trigger this procedure for the UE and they are rejected for the PLMN. If the UE supports NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, they are included in the list of Pending NSSAI for the PLMN, as described in clause 5.15.5.2.1.

If a UE is configured with S-NSSAIs, which are subject to Network Slice-Specific Authentication and Authorization, the UE stores an association between the S-NSSAI and corresponding credentials for the Network Slice-Specific Authentication and Authorization.

NOTE X: How the UE is aware that an S-NSSAI is subject to Network Slice-Specific Authentication and Authorization (e.g., based on local configuration) is out of scope of this specification.

The UE may support remote provisioning of credentials for NSSAA, specified in clause 5.39.

A UE that supports to be provisioned with the credentials used for NSSAA over UP remote provisioning shall use connectivity over an S-NSSAI/DNN which can access the provisioning server to establish a PDU session for remote provisioning as defined in clause 5.39.NOTE Y: The credentials for Network Slice-Specific Authentication and Authorization are not specified.

To perform the Network Slice-Specific Authentication and Authorization for an S-NSSAI, the AMF invokes an EAP- based Network Slice-Specific authorization procedure documented in clause 4.2.9 of TS 23.502 [3] (see also TS 33.501 [29]) for the S-NSSAI. When an NSSAA procedure is started and is ongoing for an S-NSSAI, the AMF stores the NSSAA status of the S-NSSAI as pending and when the NSSAA is completed the S-NSSAI becomes either part of the Allowed NSSAI or a Rejected S-NSSAI. The NSSAA status of each S-NSSAI, if any is stored, is transferred when the AMF changes.

This procedure can be invoked for a supporting UE by an AMF at any time, e.g. when:

a. The UE registers with the AMF and one of the S-NSSAIs of the HPLMN which maps to an S-NSSAI in the Requested NSSAI is requiring Network Slice-Specific Authentication and Authorization (see clause 5.15.5.2.1 for details), and the S-NSSAI in the Requested NSSAI can be added to the Allowed NSSAI by the AMF once the Network Slice-Specific Authentication and Authorization for the HPLMN S-NSSAI succeeds; or

b. The Network Slice-Specific AAA Server triggers a UE re-authentication and re-authorization for an S-NSSAI; or

c. The AMF, based on operator policy or a subscription change, decides to initiate the Network Slice-Specific Authentication and Authorization procedure for a certain S-NSSAI which was previously authorized.

 In the case of re-authentication and re-authorization (b. and c. above) the following applies:

- If S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization map to S-NSSAIs that are included in the Allowed NSSAI for each Access Type, AMF selects an Access Type to be used to perform the Network Slice Specific Authentication and Authorization procedure based on network policies.

- If the Network Slice-Specific Authentication and Authorization for some S-NSSAIs mapped to some S-NSSAIs in the Allowed NSSAI is unsuccessful, the AMF shall update the Allowed NSSAI for each Access Type to the UE via UE Configuration Update procedure.

- If the Network Slice-Specific Authentication and Authorization fails for all S-NSSAIs mapped to all S-NSSAIs in the Allowed NSSAI, the AMF determines a new Allowed NSSAI including default S-NSSAI(s). If no default S-NSSAI(s) could be added, the AMF shall execute the Network-initiated Deregistration procedure described in clause 4.2.2.3.3 of TS 23.502 [3] and shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

After a successful or unsuccessful UE Network Slice-Specific Authentication and Authorization, the UE context in the AMF shall retain the authentication and authorization status for the UE for the related specific S-NSSAI of the HPLMN while the UE remains RM-REGISTERED in the PLMN, so that the AMF is not required to execute a Network Slice-Specific Authentication and Authorization for a UE at every Periodic Registration Update or Mobility Registration procedure with the PLMN.

A Network Slice-Specific AAA server may revoke the authorization or challenge the authentication and authorization of a UE at any time. When authorization is revoked for an S-NSSAI that maps to an S-NSSAI in the current Allowed NSSAI for an Access Type, the AMF shall provide a new Allowed NSSAI to the UE and trigger the release of all PDU sessions associated with the S-NSSAI, for this Access Type.

The AMF provides the GPSI of the UE related to the S-NSSAI to the AAA Server to allow the AAA server to initiate the Network Slice-Specific Authentication and Authorization, or the Authorization revocation procedure, where the current AMF serving the UE needs to be identified by the system, so the UE authorization status can be challenged or revoked.

The Network Slice-Specific Authentication and Authorization requires that the UE Primary Authentication and Authorization of the SUPI has successfully completed. If the SUPI authorization is revoked, then also the Network Slice-Specific authorization is revoked.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*