SA WG2 Meeting #143E (e-meeting) S2-20xxxxx

Elbonia, 24 Feburary - 9 March 2021

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **DRAFT** | **rev** |  | **Current version:** | **16.7.0** |  |
|  |
|  |
| *For* [***HELP***](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:***  | UE remote provisioning for PNI-NPN using Control Plane |
|  |  |
| ***Source to WG:*** | China Mobile, China Unicom? OPPO? |
| ***Source to TSG:*** | S2 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2020-11-09 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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-12 (Release 12)Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | It is concluded in TR 23.700-07 that remote provisioning of PNI-NPN credentials should be supported and both procedures using Control Plane and using User Plane protocols after establishing PDU session shall be enabled.This draftCR introduces functional description of remote provisioning of PNI-NPN credentials using Control Plane. |
|  |  |
| ***Summary of change:*** | This draftCR mainly creates a new clause to describe functionalities for remote provisioning of PNI-NPN credentials using Control Plane, along with modifications on Definitions and description of NSAA clause. |
|  |  |
| ***Consequences if not approved:*** | remote provisioning of PNI-NPN credentials using Control Plane can not be supported in this release. |
|  |  |
| ***Clauses affected:*** | 3.1, 5.6.6, 5.15.10, 5.30.3.1, 5.30.3.X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  |  |
| ***affected:*** |  | **X** |  Test specifications |  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

*FIRST CHANGE*

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**5GLAN Group:** A set of UEs using private communication for 5G LAN-type service.

**5G Access Network:** An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network.

**5G Core Network:** The core network specified in the present document. It connects to a 5G Access Network.

**5G LAN-Type Service:** A service over the 5G system offering private communication using IP and/or non-IP type communications.

**5G LAN-Virtual Network:** A virtual network over the 5G system capable of supporting 5G LAN-type service.

**5G QoS Flow:** The finest granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receive the same forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different QoS forwarding treatment requires separate 5G QoS Flow.

**5G QoS Identifier:** A scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow. This may be implemented in the access network by the 5QI referencing node specific parameters that control the QoS forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

**5G System:** 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE.

**5G-BRG:** The 5G-BRG is a 5G-RG defined in BBF.

**5G-CRG:** The 5G-CRG is a 5G-RG specified in DOCSIS MULPI [89].

**5G-RG:** A 5G-RG is a RG capable of connecting to 5GC playing the role of a UE with regard to the 5G core. It supports secure element and exchanges N1 signalling with 5GC. The 5G-RG can be either a 5G-BRG or 5G-CRG.

**Access Traffic Steering:** The procedure that selects an access network for a new data flow and transfers the traffic of this data flow over the selected access network. Access traffic steering is applicable between one 3GPP access and one non-3GPP access.

**Access Traffic Switching:** The procedure that moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. Access traffic switching is applicable between one 3GPP access and one non-3GPP access.

**Access Traffic Splitting:** The procedure that splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access. Access traffic splitting is applicable between one 3GPP access and one non-3GPP access.

**Allowed NSSAI**: NSSAI provided by the Serving PLMN during e.g. a Registration procedure, indicating the S-NSSAIs values the UE could use in the Serving PLMN for the current Registration Area.

**Allowed Area:** Area where the UE is allowed to initiate communication as specified in clause 5.3.2.3.

**AMF Region:** An AMF Region consists of one or multiple AMF Sets.

**AMF Set:** An AMF Set consists of some AMFs that serve a given area and Network Slice(s). AMF Set is unique within an AMF Region and it comprises of AMFs that support the same Network Slice(s). Multiple AMF Sets may be defined per AMF Region. The AMF instances in the same AMF Set may be geographically distributed but have access to the same context data.

**Application identifier:** An identifier that can be mapped to a specific application traffic detection rule.

**AUSF Group ID:** This refers to one or more AUSF instances managing a specific set of SUPIs. An AUSF Group consists of one or multiple AUSF Sets.

**Binding Indication:** Information included by a NF service producer to a NF service consumer in request responses or notifications to convey the scope within which selection/reselection of target NF/NF Services may be performed, or information included by the NF service consumer in requests or subscriptions to convey the scope within which selection/reselection of notification targets or the selection of other service(s) that the NF consumer produces for the same data context may be performed. See clause 6.3.1.0.

**Configured NSSAI:** NSSAI provisioned in the UE applicable to one or more PLMNs.

**CHF Group ID:** This refers to one or more CHF instances managing a specific set of SUPIs.

**Delegated Discovery:** This refers to delegating the discovery and associated selection of NF instances or NF service instances to an SCP.

**Direct Communication:** This refers to the communication between NFs or NF services without using an SCP.

**DN Access Identifier (DNAI):** Identifier of a user plane access to one or more DN(s) where applications are deployed.

**Emergency Registered:** A UE is considered Emergency Registered over an Access Type in a PLMN when registered for emergency services only over this Access Type in this PLMN.

**Endpoint Address:** An address in the format of an IP address or FQDN, which is used to determine the host/authority part of the target URI. This Target URI is used to access an NF service (i.e. to invoke service operations) of an NF service producer or for notifications to an NF service consumer.

**En-gNB:** as defined in TS 37.340 [31].

**Expected UE Behaviour:** Set of parameters provisioned by an external party to 5G network functions on the foreseen or expected UE behaviour, see clause 5.20.

**Fixed Network Residential Gateway:** A Fixed Network RG (FN-RG) is a RG that it does not support N1 signalling and it is not 5GC capable.

**Fixed Network Broadband Residential Gateway:** A Fixed Network RG (FN-BRG) is a FN-RG specified in BBF TR‑124 [90].

**Fixed Network Cable Residential Gateway:** A Fixed Network Cable RG (FN-CRG) is a FN-RG with cable modem specified in DOCSIS MULPI [89].

**Forbidden Area:** An area where the UE is not allowed to initiate communication as specified in clause 5.3.2.3.

**GBR QoS Flow:** A QoS Flow using the GBR resource type or the Delay-critical GBR resource type and requiring guaranteed flow bit rate.

**IAB-donor:** This is a NG-RAN node that supports Integrated access and backhaul (IAB) feature and provides connection to the core network to IAB-nodes. It supports the CU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

**IAB-node:** A relay node that supports wireless in-band and out-of-band relaying of NR access traffic via NR Uu backhaul links. It supports the UE function and the DU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

**Indirect Communication:** This refers to the communication between NFs or NF services via an SCP.

**Initial Registration:** UE registration in RM-DEREGISTERED state as specified in clause 5.3.2.

**Intermediate SMF (I-SMF):** An SMF that is inserted to support a PDU session as the UE is located in an area which cannot be controlled by the original SMF because the UPF(s) belong to a different SMF Service Area.

**Local Area Data Network:** a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.

**Local Break Out (LBO):** Roaming scenario for a PDU Session where the PDU Session Anchor and its controlling SMF are located in the serving PLMN (VPLMN).

**LTE-M:** a 3GPP RAT type Identifier used in the Core Network only, which is a sub-type of E-UTRA RAT type, and defined to identify in the Core Network the E-UTRA when used by a UE indicating Category M.

**MA PDU Session:** A PDU Session that provides a PDU connectivity service, which can use one access network at a time, or simultaneously one 3GPP access network and one non-3GPP access network.

**Mobility Pattern:** Network concept of determining within the AMF the UE mobility parameters as specified in clause 5.3.2.4.

**Mobility Registration Update:** UE re-registration when entering new TA outside the TAI List as specified in clause 5.3.2.

**MPS-subscribed UE:** A UE having a USIM with MPS subscription.

**NB-IoT UE Priority:** Numerical value used by the NG-RAN to prioritise between different UEs accessing via NB-IoT.

**NGAP UE association:** The logical per UE association between a 5G-AN node and an AMF.

**NGAP UE-TNLA-binding:** The binding between a NGAP UE association and a specific TNL association for a given UE.

**Network Function:** A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces.

NOTE 1: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

**Network Instance**: Information identifying a domain. Used by the UPF for traffic detection and routing.

**Network Slice:** A logical network that provides specific network capabilities and network characteristics.

**Network Slice instance:** A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.

**Non-GBR QoS Flow:** A QoS Flow using the Non-GBR resource type and not requiring guaranteed flow bit rate.

**NSI ID:** an identifier for identifying the Core Network part of a Network Slice instance when multiple Network Slice instances of the same Network Slice are deployed, and there is a need to differentiate between them in the 5GC.

**NF instance:** an identifiable instance of the NF.

**NF service:** a functionality exposed by a NF through a service based interface and consumed by other authorized NFs.

**NF service instance:** an identifiable instance of the NF service.

**NF service operation:** An elementary unit a NF service is composed of.

**NF Service Set:** A group of interchangeable NF service instances of the same service type within an NF instance. The NF service instances in the same NF Service Set have access to the same context data.

**NF Set:** A group of interchangeable NF instances of the same type, supporting the same services and the same Network Slice(s). The NF instances in the same NF Set may be geographically distributed but have access to the same context data.

**NG-RAN:** A radio access network that supports one or more of the following options with the common characteristics that it connects to 5GC:

1) Standalone New Radio.

2) New Radio is the anchor with E-UTRA extensions.

3) Standalone E-UTRA.

4) E-UTRA is the anchor with New Radio extensions.

**Non-Allowed Area:** Area where the UE is allowed to initiate Registration procedure but no other communication as specified in clause 5.3.2.3.

Non-Public Network: See definition in TS 22.261 [2].

**Non-Seamless Non-3GPP offload:** The offload of user plane traffic via non-3GPP access without traversing either N3IWF/TNGF or UPF.

**PCF Group ID:** This refers to one or more PCF instances managing a specific set of SUPIs. A PCF Group consists of one or multiple PCF Sets.

**Pending NSSAI:** NSSAI provided by the Serving PLMN during a Registration procedure, indicating the S-NSSAI(s) for which the network slice-specific authentication and authorization procedure is pending.

**PDU Connectivity Service:** A service that provides exchange of PDUs between a UE and a Data Network.

**PDU Session:** Association between the UE and a Data Network that provides a PDU connectivity service.

**PDU Session Type:** The type of PDU Session which can be IPv4, IPv6, IPv4v6, Ethernet or Unstructured.

**Periodic Registration Update:** UE re-registration at expiry of periodic registration timer as specified in clause 5.3.2.

**Private communication:** See definition in TS 22.261 [2].

**Provisioning Server for PNI-NPN:** The server that generates, stores and provisions the PNI-NPN credentials other than primary authentication of the UE, e.g. credentials for NSAA or secondary authentication.

**Public network integrated NPN:** A non-public network deployed with the support of a PLMN.

**(Radio) Access Network**: See 5G Access Network.

**RAT type:** Identifies the transmission technology used in the access network for both 3GPP accesses and non-3GPP Accesses, for example, NR, NB-IOT, Untrusted Non-3GPP, Trusted Non-3GPP, Trusted IEEE 802.11 Non-3GPP access, Wireline, Wireline-Cable, Wireline-BBF, etc.

**Requested NSSAI:** NSSAI provided by the UE to the Serving PLMN during registration.

**Residential Gateway:** The Residential Gateway (RG) is a device providing, for example voice, data, broadcast video, video on demand, to other devices in customer premises.

**Routing Binding Indication:** Information included in a request or notification and that can be used by the SCP for discovery and associated selection to of a suitable target. See clauses 6.3.1.0 and 7.1.2

**Routing Indicator:** Indicator that allows together with SUCI/SUPI Home Network Identifier to route network signalling to AUSF and UDM instances capable to serve the subscriber.

**SCP Domain:** A configured group of one or more SCP(s) and zero or more NF instances(s). An SCP within the group can communicate with any NF instance or SCP within the same group directly, i.e. without passing through an intermediate SCP.

**SNPN enabled UE:** A UE configured to use stand-alone Non-Public Networks.

**SNPN access mode:** A UE operating in SNPN access mode only selects stand-alone Non-Public Networks over Uu.

**Service based interface:** It represents how a set of services is provided/exposed by a given NF.

**Service Continuity:** The uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point change.

**Service Data Flow Filter:** A set of packet flow header parameter values/ranges used to identify one or more of the packet (IP or Ethernet) flows constituting a Service Data Flow.

**Service Data Flow Template:** The set of Service Data Flow filters in a policy rule or an application identifier in a policy rule referring to an application detection filter, required for defining a Service Data Flow.

**Session Continuity:** The continuity of a PDU Session. For PDU Session of IPv4 or IPv6 or IPv4v6 type "session continuity" implies that the IP address is preserved for the lifetime of the PDU Session.

**SMF Service Area:** The collection of UPF Service Areas of all UPFs which can be controlled by one SMF.

**Stand-alone Non-Public Network:** A non-public network not relying on network functions provided by a PLMN

**Subscribed S-NSSAI**: S-NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN

**Time Sensitive Communication (TSC):** A communication service that supports deterministic communication and/or isochronous communication with high reliability and availability. It is about providing packet transport with QoS characteristics such as bounds on latency, loss, and reliability, where end systems and relay/transmit nodes can be strictly synchronized.

**TSN working domain:** Synchronization domain for a localized set of devices collaborating on a specific task or work function in a TSN network, corresponding to a gPTP domain defined in IEEE 802.1AS [104].

**UDM Group ID:** This refers to one or more UDM instances managing a specific set of SUPIs. An UDM Group consists of one or multiple UDM Sets.

**UDR Group ID:** This refers to one or more UDR instances managing a specific set of SUPIs. An UDR Group consists of one or multiple UDR Sets.

**UPF Service Area**: An area consisting of one or more TA(s) within which PDU Session associated with the UPF can be served by (R)AN nodes via a N3 interface between the (R)AN and the UPF without need to add a new UPF in between or to remove/re-allocate the UPF.

**Uplink Classifier:** UPF functionality that aims at diverting Uplink traffic, based on filter rules provided by SMF, towards Data Network.

**WB-E-UTRA:** In the RAN, WB-E-UTRA is the part of E-UTRA that excludes NB-IoT. In the Core Network, WB-E-UTRA also excludes LTE-M.

**Wireline 5G Access Network:** The Wireline 5G Access Network (W-5GAN) is a wireline AN that connects to a 5GC via N2 and N3 reference points. The W-5GAN can be either a W-5GBAN or W-5GCAN.

**Wireline 5G Cable Access Network:** The Wireline 5G Cable Access Network (W-5GCAN) is the Access Network defined in CableLabs.

**Wireline BBF Access Network:** The Wireline 5G BBF Access Network (W-5GBAN) is the Access Network defined in BBF.

**Wireline Access Gateway Function (W-AGF):** The Wireline Access Gateway Function (W-AGF) is a Network function in W-5GAN that provides connectivity to the 5G Core to 5G-RG and FN-RG.

NOTE 2: If one AUSF/PCF/UDR/UDM group consists of multiple AUSF/PCF/UDR/UDM Sets, AUSF/PCF/UDR/UDM instance from different Set may be selected to serve the same UE. The temporary data which is not shared across different Sets may be lost, e.g. the event subscriptions stored at one UDM instance are lost if another UDM instance from different Set is selected and no data shared across the UDM Sets.

*NEXT 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.

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 regard 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.

NOTE 3: The way for the UE to acquire such information is not defined.

SMF policies or subscription information (such as defined in TS 23.502 [3] Table 5.2.3.3.1) 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 in 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 TS 23.502 [3] clause 4.3.2.3.

The remote provisioning of PNI-NPN credentials specified in clause 5.30.3.X applies for provisioning of credentials for secondary authentication/authorization.

*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.

The remote provisioning of PNI-NPN credentials specified in clause 5.30.3.X applies for provisioning of credentials for Network Slice-Specific Authentication and Authorization.

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 TS 23.502 [3] clause 4.2.9 (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 shall execute the Network-initiated Deregistration procedure described in TS 23.502 [3], clause 4.2.2.3.3, 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.

*NEXT CHANGE*

5.30.3 Public Network Integrated NPN

5.30.3.1 General

Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN. The existing network slicing functionalities apply as described in clause 5.15. When a PNI-NPN is made available via a PLMN, then the UE shall have a subscription for the PLMN in order to access PNI-NPN.

NOTE 1: Annex D provides additional consideration to consider when supporting Non-Public Network as a Network Slice of a PLMN.

As network slicing does not enable the possibility to prevent UEs from trying to access the network in areas where the UE is not allowed to use the Network Slice allocated for the NPN, Closed Access Groups may optionally be used to apply access control.

A Closed Access Group identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG.

CAG is used for the PNI-NPNs to prevent UE(s), which are not allowed to access the NPN via the associated cell(s), from automatically selecting and accessing the associated CAG cell(s).

NOTE 2: CAG is used for access control e.g. authorization at cell selection and configured in the subscription as part of the Mobility Restrictions i.e. independent from any S-NSSAI. CAG is not used as input to AMF selection nor Network Slice selection. If NPN isolation is desired, operator can better support NPN isolation by deploying network slicing for PNI-NPN, configuring dedicated S-NSSAI(s) for the given NPN as specified in Annex D, clause D.2 and restricting NPN's UE subscriptions to these dedicated S-NSSAI(s).

PNI-NPN may support remote provisioning of credentials other than primary authentication, e.g. credentials for NSAA or secondary authentication to the UE, when the UE subscribes to Network Slice-Specific Authentication or Secondary authentication/authorization but is not preconfigured with those credentials.

NOTE 3: The UE of a PNI-NPN has been subscribed to the PLMN providing the PNI-NPN and a USIM has been provisioned with primary authentication credentials for accessing this PLMN.

PNI-NPN provisions crendetials to the UE via NAS signalling (Control Plane) or a PDU session specific for credential provisioning (User Plane) as specified in clause 5.30.3.X.

*NEXT CHANGE*

#### 5.30.3.X Remote provisioning for PNI-NPN credentials

##### 5.30.3.X.Y Remote provisioning for PNI-NPN credentials using Control Plane

This clause describes the functionalities for PNI-NPN to support remote provisioning of credentials to the UE via Control Plane.

When Network Slice-Specific Authentication or Secondary authentication/authorization is subscribed to PNI-NPN UE, the corresponding credentials are generated by the Provisioning Server for PNI-NPN owned by the PNI-NPN owner. The credentials are combined with the GPSI of the UE and S-NSSAI/DNN for the PNI-NPN in the Provisioning Server for PNI-NPN.

After generated the credentials may be stored in Provisioning Server for PNI-NPN or in the UDM of PLMN providing the PNI-NPN.

If the credentials are to be stored in the UDM, the credentials are sent from the Provisioning Server for PNI-NPN, along with the combined GPSI and S-NSSAI/DNN for the PNI-NPN, to the NEF. The NEF discovers the UDM and forwards the credentials to the UDM. The UDM stores the credentials as part of subscription data for further provisioning.

Editor's note: It’s FFS how to enhance services of UDM and NEF to transport the credentials.

During the registration procedure, when the AMF retrieves subscription data from the UDM, the UDM may include the credentials in the subscription data as follows:

* if the credentials are to be stored in ME by the UE, the UDM checks if the PEI of the UE included in registration request is same with the one saved in the UDM. If there is no PEI saved, or the PEI of the UE is not same with the saved PEI (e.g. the user get a new mobile phone with UICC unchanged), or the PEI of UE is the same with the PEI stored in UDM but the "NPN credential changed" indication(s) of the UE is set in the UDM, the UDM includes the credentials when sending UE subscription data to the AMF. The UDM saves the PEI of the UE afterwards.
* if the NPN credentials are to be stored in UICC by the UE, the UDM check whether there exists "NPN credential changed" indication(s) in UDM for this UE. If so, UDM provides UE with credentials for S-NSSAI(s)/DNN(s) according to "NPN credential changed" indication(s).

The UDM may retrieve the credentials from the Provisioning Server for PNI-NPN via NEF, if the credentials are stored in the Provisioning Server for PNI-NPN. The Provisioning Server for PNI-NPN may check with the device manufacturer or its database for e.g. about validity of the device, to decide whether the credentials are sent to the UDM.

NOTE: The check can also be done by operator and the procedure between the Provisioning Server for PNI-NPN and the device manufacturer is out of 3GPP scope.

Editor's note: It’s FFS how the NEF discover and retrieve credentials from the Provisioning Server for PNI-NPN.

If the registration is successful, or the UE is authenticated successfully by PLMN, but to the S-NSSAIs that require NSSAA are put in pending state, the AMF includes all credentials for all S-NSSAIs or DNNs requiring NSSAA or secondary authentication to the UE in Registration Accept message.

The security mechanisms of steering of roaming mechanism as specified in TS 33.501 [7] are used for credentials protection between UE and 5GC. The existing domain security mechanisms as specified in TS 33.210 [21] and TS 33.310 [35] are used between 5GC and PNI-NPN provisioning platform to protect the credentials.

The UDM clears the "NPN credential changed" indication if it receives the acknowledgement from UE that the corresponding credential has been successfully provisioned or updated.

After successful remote provisioning, the credentials may be updated to UE by using UE Parameters Update procedure procedure defined in clause 4.20 of TS 23.502 [3]. If the credentials stored in UDM change, or the credentials stored in the Provisioning Server for PNI-NPN change and UDM receives the notification from the Provisioning Server for PNI-NPN, the UDM sets "NPN credential changed" indication(s) associated with S-NSSAI(s)/DNN(s) and initiates UE Parameters Update procedure to provision the updated credentials to the UE.

*END OF CHANGES*