**3GPP TSG-WG SA2 Meeting #147E  *S2-21XXXX***

**E-meeting, October 18 – 22, 2021 (*revision of S2-21XXXXX*)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **-** | **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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Rapporteur's editorial cleanup for eNPN |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-10-11 |
|  |  |  |  |  |
| ***Category:*** | **D** |  | ***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:*** | Clause 5.30.2.10.4.1 contains an EN that should introduce the following clauses.Some inconsistent use of provisoning server, Provisioning Server and PVS.The PDU Session used for UP Remote Provisioning of credentials for NSSAA or secondary authentication is not required to be restricted, and as such the UE is not aware whether it is restricted. |
|  |  |
| ***Summary of change:*** | Added text in clause 5.30.2.10.4.1 introducing the following clauses.Usage of PVS instead of provisioning server.Removes the assumption that the PDU Session used for UP Remote Provisioning of credentials for NSSAA or secondary authentication is restricted. |
| ***--*** |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.30.2.10.4.1, 5.39.1, 5.39.2 |
|  |  |
|  | **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 changes \* \* \* \*

## 5.30 Support for non-public networks

### 5.30.1 General

A Non-Public Network (NPN) is a 5GS deployed for non-public use, see TS 22.261 [2]. An NPN is either:

- a Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN operator and not relying on network functions provided by a PLMN, or

- a Public Network Integrated NPN (PNI-NPN), i.e. a non-public network deployed with the support of a PLMN.

NOTE: An NPN and a PLMN can share NG-RAN as described in clause 5.18.

Stand-alone NPN are described in clause 5.30.2 and Public Network Integrated NPNs are described in clause 5.30.3.

### 5.30.2 Stand-alone non-public networks

#### 5.30.2.0 General

SNPN 5GS deployments are based on the architecture depicted in clause 4.2.3, the architecture for 5GC with untrusted non-3GPP access (Figure 4.2.8.2.1-1) for access to SNPN services via a PLMN (and vice versa) and the additional functionality covered in clause 5.30.2.

Alternatively, a Credentials Holder (CH) may authenticate and authorize access to an SNPN separate from the Credentials Holder based on the architecture specified in clause 5.30.2.9.

In this Release, direct access to SNPN is specified for 3GPP access only.

Interworking with EPS is not supported for SNPN. Also, emergency services are not supported for SNPN when the UE accesses the SNPN over NWu via a PLMN. Furthermore, roaming is not supported for SNPN, e.g. roaming between SNPNs. Handover between SNPNs, between SNPN and PLMN or PNI NPN are not supported. Idle mode mobility is supported as defined in clause 5.30.2.11. CIoT 5GS optimizations are not supported in SNPNs. CAG is not supported in SNPNs.

#### 5.30.2.1 Identifiers

The combination of a PLMN ID and Network identifier (NID) identifies an SNPN.

NOTE 1: The PLMN ID used for SNPNs is not required to be unique. PLMN IDs reserved for use by private networks can be used for non-public networks, e.g. based on mobile country code (MCC) 999 as assigned by ITU [78]). Alternatively, a PLMN operator can use its own PLMN IDs for SNPN(s) along with NID(s), but registration in a PLMN and mobility between a PLMN and an SNPN are not supported using an SNPN subscription given that the SNPNs are not relying on network functions provided by the PLMN.

The NID shall support two assignment models:

- Self-assignment: NIDs are chosen individually by SNPNs at deployment time (and may therefore not be unique) but use a different numbering space than the coordinated assignment NIDs as defined in TS 23.003 [19].

- Coordinated assignment: NIDs are assigned using one of the following two options:

1. The NID is assigned such that it is globally unique independent of the PLMN ID used; or

2. The NID is assigned such that the combination of the NID and the PLMN ID is globally unique.

NOTE 2: Which legal entities manage the number space is beyond the scope of this specification.

NOTE 3: The use of SNPN with self-assignment model NID such that the combination of PLMN ID and NID is not globally unique is not assumed for the architecture described in Figure 5.30.2.9.3-1, Figure 5.30.2.9.2-1. and for SNPN - SNPN Mobility as described in clause 5.30.2.10.

The GIN shall support two assignment models:

- Self-assignment: GINs are chosen individually and may therefore not be unique. It is defined as in TS 23.003 [19]

- Coordinated assignment: GIN uses a combination of PLMN ID and NID and is assigned using one of the following two options as defined in TS 23.003 [19].

1. The GIN is assigned such that the NID is globally unique (e.g. using IANA Private Enterprise Numbers) independent of the PLMN ID used; or

2. The GIN is assigned such that the combination of the NID and the PLMN ID is globally unique.

NOTE 4: Which legal entities manage the number space for GIN is beyond the scope of this specification.

An optional human-readable network name helps to identify an SNPN during manual SNPN selection. The human-readable network name and how it is used for SNPN manual selection is specified in TS 22.261 [2] and TS 23.122 [17].

#### 5.30.2.2 Broadcast system information

NG-RAN nodes which provide access to SNPNs broadcast the following information:

- One or multiple PLMN IDs

- List of NIDs per PLMN ID identifying the non-public networks NG-RAN provides access to

NOTE 1: It is assumed that an NG-RAN node supports broadcasting a total of twelve NIDs. Further details are defined in TS 38.331 [28].

NOTE°2: The presence of a list of NIDs for a PLMN ID indicates that the related PLMN ID and NIDs identify SNPNs.

- Optionally:

- A human-readable network name per SNPN;

NOTE 3: The human-readable network name per SNPN is only used for manual SNPN selection. The mechanism how human-readable network name is provided (i.e. whether it is broadcasted or unicasted) to the UE is specified in TS 38.331 [28].

- Information, as described in TS 38.300 [27], TS 38.331 [28] and in TS 38.304 [50], to prevent UEs not supporting SNPNs from accessing the cell, e.g. if the cell only provides access to non-public networks;

- An indication per SNPN of whether access using credentials from a Credentials Holder is supported;

- List of supported Group IDs for Network Selection (GINs) per SNPN;

- An indication per SNPN of whether the SNPN allows registration attempts from UEs that are not explicitly configured to select the SNPN, i.e. UEs that do not have any PLMN ID and NID nor GIN broadcast by the SNPN in the Credentials Holder controlled prioritized lists of preferred SNPNs/GINs.

NOTE 4: Further details (including number of supported GINs per SNPN) are defined in TS 38.331 [28].

#### 5.30.2.3 UE configuration and subscription aspects

An SNPN-enabled UE is configured with the following information for each subscribed SNPN:

- PLMN ID and NID of the subscribed SNPN;

- Subscription identifier (SUPI) and credentials for the subscribed SNPN;

- Optionally, an N3IWF FQDN and an identifier of the country where the configured N3IWF is located;

- Optionally, if the UE supports access to an SNPN using credentials from a Credentials Holder:

- User controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of GINs.

The Credentials Holder controlled prioritized lists of preferred SNPNs and GINs may be updated by the Credentials Holder using the Steering of Roaming (SoR) procedure as defined in Annex C of TS 23.122 [17].

A subscriber of an SNPN is either:

- identified by a SUPI containing a network-specific identifier that takes the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [20] based user identification as defined in clause 28.7.2 of TS 23.003 [19]. The realm part of the NAI may include the NID of the SNPN; or

- identified by a SUPI containing an IMSI.

In the case of access to an SNPN using credentials owned by a Credentials Holder as specified in clause 5.30.2.9.2 and clause 5.30.2.9.3, the SUPI shall also contain identification for the Credentials Holder (i.e. the realm in the case of Network Specific Identifier based SUPI or the MCC and MNC in the case of an IMSI based SUPI).

NOTE 1: When Credentials Holder is an SNPN, and the MCC and MNC of the SNPN is not unique, then IMSI based SUPI is not supported as the MCC and MNC need not be globally unique always; instead USIM credentials are supported using Network Specific Identifier based SUPI.

NOTE 2: Network Specific Identifier are not supported for the case the Credentials Holder is provided by a PLMN.

NOTE 3: When Credentials Holder is a PLMN, it is assumed that normally the SNPN and the Credentials Holder use different PLMN ID. If SNPN and CHs share PLMN ID, and IMSI based SUPI is used, then RID can be used for AUSF/UDM discovery and selection as long as the RID values are coordinated among the involved SNPN and CHs. When the PLMN ID is not shared between SNPNs and CHs, then PLMN ID is sufficient to be used for AUSF/UDM discovery & selection unless the CHs deploys multiple AUSF/UDM in which case also RID can be used as long as the RID values are coordinated within the CH.

In the case of access to an SNPN using credentials owned by a Credentials Holder using AAA-S as specified in clause 5.30.2.9.2, only Network Specific Identifier based SUPI is supported.

An SNPN-enabled UE that supports access to an SNPN using credentials from a Credentials Holder and that is equipped with a PLMN subscription may additionally be configured with the following information for SNPN selection and registration using the PLMN subscription in SNPN access mode:

- User controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of preferred SNPNs;

- Credentials Holder controlled prioritized list of preferred GINs.

The Credentials Holder controlled prioritized lists of preferred SNPNs and GINs may be updated by the Credentials Holder using the Steering of Roaming (SoR) procedure as defined in Annex C of TS 23.122 [17].

When the Credentials Holder updates a UE with the Credentials Holder controlled prioritized lists of preferred SNPNs and GINs the UE may perform SNPN selection again, e.g. to potentially select a higher prioritized SNPN.

#### 5.30.2.4 Network selection in SNPN access mode

##### 5.30.2.4.1 General

An SNPN-enabled UE supports the SNPN access mode. When the UE is set to operate in SNPN access mode the UE only selects and registers with SNPNs over Uu as described in clause 5.30.2.4.

Emergency services are supported in SNPN access mode. If the UE is in limited service state, the UE shall attempt to camp on an acceptable cell of any available SNPN supporting emergency calls (irrespective of SNPN ID or GIN) or on any available PLMN supporting emergency calls (irrespective of PLMN ID).

If a UE is not set to operate in SNPN access mode, even if it is SNPN-enabled, the UE does not select and register with SNPNs. A UE not set to operate in SNPN access mode performs PLMN selection procedures as defined in clause 4.4 of TS 23.122 [17]. For a UE capable of simultaneously connecting to an SNPN and a PLMN, the setting for operation in SNPN access mode is applied only to the Uu interface for connection to the SNPN. Clause D.4 provides more details.

An SNPN-enabled UE that supports access to an SNPN using credentials from a Credentials Holder and that is equipped with a PLMN subscription needs to first enter SNPN access mode to be able to select SNPNs. Once the UE has entered SNPN access mode, SNPN selection is performed as described in clause 5.30.2.4. Once an SNPN has been selected the UE attempts registration in the SNPN using the PLMN credentials.

NOTE: Details of activation and deactivation of SNPN access mode are up to UE implementation.

When a UE is set to operate in SNPN access mode the UE does not perform normal PLMN selection procedures as defined in clause 4.4 of TS 23.122 [17].

UEs operating in SNPN access mode read the information described in clause 5.30.2.2 from the broadcast system information and take them into account during network selection.

##### 5.30.2.4.2 Automatic network selection

NOTE 1: If the UE has multiple SNPN subscriptions it is assumed that the subscription to use for automatic selection is determined by implementation specific means prior to network selection.

For automatic network selection the UE selects and attempts registration on available and allowable SNPNs in the following order:

- the SNPN the UE was last registered with (if available);

- the subscribed SNPN, which is identified by the PLMN ID and NID for which the UE has SUPI and credentials.;

- If the UEs supports access to an SNPN using credentials from a Credentials Holder then the UE continues by selecting and attempting registration on available and allowable SNPNs which broadcast the indication that access using credentials from a Credentials Holder is supported in the following order:

- SNPNs in the user controlled prioritized list of preferred SNPNs (in priority order);

- SNPNs in the Credentials Holder controlled prioritized list of preferred SNPNs (in priority order);

- SNPNs, which additionally broadcast a GIN contained in the Credentials Holder controlled prioritized list of preferred GINs (in priority order);

NOTE 2: If multiple SNPNs are available that broadcast the same GIN, the order in which the UE selects and attempts a registration with those SNPNs is implementation specific.

- SNPNs, which additionally broadcast an indication that the SNPN allows registration attempts from UEs that are not explicitly configured to select the SNPN, i.e. the broadcasted NID or GIN is not present in the Credentials Holder controlled prioritized lists of preferred SNPNs/GINs in the UE.

NOTE 3: If multiple SNPNs are available that broadcast the indication that the SNPN allows registration attempts from UEs that are not explicitly configured to select the SNPN, the order in which the UE selects and attempts a registration with those SNPNs is implementation specific.

When a UE performs Initial Registration to an SNPN, the UE shall indicate the PLMN ID and NID as broadcast by the selected SNPN to NG-RAN. NG-RAN shall inform the AMF of the selected PLMN ID and NID.

##### 5.30.2.4.3 Manual network selection

For manual network selection UEs operating in SNPN access mode provide to the user the list of SNPNs (each is identified by a PLMN ID and NID) and related human-readable names (if available) of the available SNPNs the UE has respective SUPI and credentials for. If the UEs supports access to an SNPN using credentials from a Credentials Holder, the UE also presents available SNPNs which broadcast the "access using credentials from a Credentials Holder is supported" indication and the human-readable names related to the SNPNs (if available).

NOTE: The details of manual SNPN selection are defined in TS 23.122 [17].

When a UE performs Initial Registration to an SNPN, the UE shall indicate the selected PLMN ID and NID as broadcast by the selected SNPN to NG-RAN. NG-RAN shall inform the AMF of the selected PLMN ID and NID.

#### 5.30.2.5 Network access control

If a UE performs the registration or service request procedure in an SNPN identified by a PLMN ID and a self-assigned NID and there is no subscription for the UE, then the AMF shall reject the UE with an appropriate cause code to temporarily prevent the UE from automatically selecting and registering with the same SNPN.

If a UE performs the registration or service request procedure in an SNPN identified by a PLMN ID and a coordinated assigned NID and there is no subscription for the UE, then the AMF shall reject the UE with an appropriate cause code to permanently prevent the UE from automatically selecting and registering with the same SNPN.

NOTE: The details of rejection and cause codes is defined in TS 24.501 [47].

If a UE performs the registration in an SNPN using credentials from a Credentials Holder and UE is not authorized to access that specific SNPN, then the UDM can reject the UE which results in AMF rejecting the registration request from the UE with an appropriate cause code to prevent the UE from selecting and registering with the same SNPN using credentials from the Credentials Holder as described in TS 24.501 [47].

In order to prevent access to SNPNs for authorized UE(s) in the case of network congestion/overload, Unified Access Control information is configured per SNPN (i.e. as part of the subscription information that the UE has for a given SNPN) and provided to the UE as described in TS 24.501 [47].

#### 5.30.2.6 Cell (re-)selection in SNPN access mode

UEs operating in SNPN access mode only select cells and networks broadcasting both PLMN ID and NID of the selected SNPN.

NOTE: Further details on the NR idle and inactive mode procedures for SNPN cell selection is defined in TS 38.331 [28] and in TS 38.304 [50].

#### 5.30.2.7 Access to PLMN services via stand-alone non-public networks

To access PLMN services, a UE in SNPN access mode that has successfully registered with an SNPN may perform another registration via the SNPN User Plane with a PLMN (using the credentials of that PLMN) following the same architectural principles as specified in clause 4.2.8 (including the optional support for PDU Session continuity between PLMN and SNPN using the Handover of a PDU Session procedures in clauses 4.9.2.1 and 4.9.2.2 of TS 23.502 [3]) and the SNPN taking the role of "Untrusted non-3GPP access". Annex D, clause D.3 provides additional details.

NOTE: QoS differentiation in the SNPN can be provided on per-IPsec Child Security Association basis by using the UE or network requested PDU Session Modification procedure described in clause 4.3.3.2 of TS 23.502 [3]. In the PLMN, N3IWF determines the IPsec child SAs as defined in clause 4.12 of TS 23.502 [3]. The N3IWF is preconfigured by PLMN to allocate different IPsec child SAs for QoS Flows with different QoS profiles.

 To support QoS differentiation in the SNPN with network-initiated QoS, the mapping rules between the SNPN and the PLMN are assumed to be governed by an SLA including: 1) mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS, which is the QoS requirement of the PLMN and is expected to be provided by the SNPN, and 2) N3IWF IP address(es) in the PLMN. The non-alteration of the DSCP field on NWu is also assumed to be governed by an SLA and by transport-level arrangements that are outside of 3GPP scope. The packet detection filters in the SNPN can be based on the N3IWF IP address and the DSCP markings on NWu.

 To support QoS differentiation in the SNPN with UE-requested QoS, the UE can request for an IPsec SA the same 5QI from the SNPN as the 5QI provided by the PLMN. It is assumed that UE-requested QoS is used only when the 5QIs used by the PLMN are from the range of standardized 5QIs. The packet filters in the requested QoS rule can be based on the N3IWF IP address and the SPI associated with the IPsec SA.

 Refer to clause D.7 for details on how to support QoS differentiation.

When the UE accesses the PLMN over NWu via a SNPN, the AMF in the serving PLMN shall send an indication toward the UE during the Registration procedure to indicate whether an IMS voice over PS session is supported or not.

#### 5.30.2.8 Access to stand-alone non-public network services via PLMN

To access SNPN services, a UE that has successfully registered with a PLMN over 3GPP access may perform another registration via the PLMN User Plane with an SNPN (using the credentials of that SNPN) following the same architectural principles as specified in clause 4.2.8 (including the optional support for PDU Session continuity between PLMN and SNPN using the Handover of a PDU Session procedures in clauses 4.9.2.1 and 4.9.2.2 of TS 23.502 [3]) and the PLMN taking the role of "Untrusted non-3GPP access" of the SNPN, i.e. using the procedures for Untrusted non-3GPP access in clause 4.12.2 of TS 23.502 [3]. Annex D, clause D.3 provides additional details. The case where UE that has successfully registered with a PLMN over non-3GPP access to access SNPN services is not specified in this Release.

NOTE: QoS differentiation in the PLMN can be provided on per-IPsec Child Security Association basis by using the UE or network requested PDU Session Modification procedure described in clause 4.3.3.2 of TS 23.502 [3]. In the SNPN, N3IWF determines the IPsec child SAs as defined in clause 4.12 of TS 23.502 [3]. The N3IWF is preconfigured by SNPN to allocate different IPsec child SAs for QoS Flows with different QoS profiles.

 To support QoS differentiation in the PLMN with network-initiated QoS, the mapping rules between the PLMN and the SNPN are assumed to be governed by an SLA including: 1) mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS, which is the QoS requirement of the SNPN and is expected to be provided by the PLMN, and 2) N3IWF IP address(es) in the SNPN. The non-alteration of the DSCP field on NWu is also assumed to be governed by an SLA and by transport-level arrangements that are outside of 3GPP scope. The packet detection filters in the PLMN can be based on the N3IWF IP address and the DSCP markings on NWu.

 To support QoS differentiation in the PLMN with UE-requested QoS, the UE can request for an IPsec SA the same 5QI from the PLMN as the 5QI provided by the SNPN. It is assumed that UE-requested QoS is used only when the 5QIs used by the SNPN are from the range of standardized 5QIs. The packet filters in the requested QoS rule can be based on the N3IWF IP address and the SPI associated with the IPsec SA.

 Refer to clause D.7 for details on how to support QoS differentiation.

When the UE accesses the SNPN over NWu via a PLMN, the AMF in the SNPN shall send an indication toward the UE during the Registration procedure to indicate whether an IMS voice over PS session is supported or not.

#### 5.30.2.9 SNPN connectivity for UEs with credentials owned by Credentials Holder

##### 5.30.2.9.1 General

SNPNs may support UE access using credentials owned by a Credentials Holder separate from the SNPN. In this case the Session Management procedures (i.e. PDU Sessions) terminate in an SMF in the SNPN.

When an SNPN supports UE access using credentials assigned by a Credentials Holder separate from the SNPN, it is assumed that is supported is homogeneously within the whole SNPN.

Credentials Holder using AAA Server for primary authentication and authorization is described in clause 5.30.2.9.2 and Credentials Holder using AUSF and UDM for primary authentication and authorization is described in clause 5.30.2.9.3.

##### 5.30.2.9.2 Credentials Holder using AAA Server for primary authentication and authorization

The AUSF in SNPN may support primary authentication and authorization of UEs that use credentials from an AAA Server in a Credentials Holder (CH).

- If the UDM decides that the primary authentication is performed by AAA Server in CH based on UE subscription data and UE's SUPI, which is de-concealed by UDM from the SUCI received from AUSF, then the UDM instructs AUSF that primary authentication by a AAA server in a CH is required, the AUSF shall discover and select the NSSAAF, and then forward EAP messages to the NSSAAF. The NSSAAF selects AAA Server based on the domain name corresponds to the realm part of the SUPI, relays EAP messages between AUSF and AAA Server (or AAA proxy) and performs related protocol conversion. The AAA server acts as the EAP Server for the purpose of primary authentication.

- The SUPI is used to identify the UE during primary authentication and authorization towards the AAA sever. SUPI privacy is achieved according to existing methods in Annex I.5 of TS 33.501 [29].

- The AMF discovers and selects the AUSF as described in clause 6.3.4 using the Home Network Identifier (realm part) and Routing Indicator present in the SUCI provided by the UE.

- The AMF and SMF shall retrieve the UE subscription data from UDM using SUPI.

Figure 5.30.2.9.2-1 depicts the 5G System architecture for SNPN with Credentials Holder using AAA Server for primary authentication and authorization.



Figure 5.30.2.9.2-1: 5G System architecture with access to SNPN using credentials from Credentials Holder using AAA Server

##### 5.30.2.9.3 Credentials Holder using AUSF and UDM for primary authentication and authorization

Figure 5.30.2.9.3-1 depicts the 5G System architecture for SNPN with Credentials Holder using AUSF and UDM for primary authentication and authorization.

NOTE: The architecture for SNPN and Credentials Holder is depicted as a non-roaming reference architecture as the UE is not considered to be roaming, even though some of the roaming architecture reference points are also used.



Figure 5.30.2.9.3-1: 5G System architecture with access to SNPN using credentials from Credentials Holder using AUSF and UDM

#### 5.30.2.10 Onboarding of UEs for SNPNs

##### 5.30.2.10.1 General

Onboarding of UEs for SNPNs allows the UE to access an Onboarding Network (ONN) based on Default UE credentials for the purpose of provisioning the UE with SNPN credentials for primary authentication and other information to enable access to a desired SNPN, i.e. (re-)select and (re-)register with SNPN.

To provision SNPN credentials in a UE that is configured with Default UE credentials (see clause 5.30.2.10.2.4), the UE selects an SNPN as ONN and establishes a secure connection with that SNPN referred to as Onboarding SNPN (ON-SNPN), see more details in clause 5.30.2.10.2.

NOTE: If the UE is already provisioned with a set of CH credentials and needs to be provisioned with an additional set of SNPN credentials, the UE can leverage the User Plane connection enabled by the available set of CH credentials to get access to a PVS.

To provision SNPN credentials in a UE that is equipped with a USIM configured with PLMN credentials, the UE selects a PLMN as ONN and establishes a secure connection with that PLMN, see more details in clause 5.30.2.10.3.

After the secure connection is established, the UE is provisioned with SNPN credentials and possibly other data to enable discovery, (re-)selection and (re-)registration for a desired SNPN, see more details in clause 5.30.2.10.4.

ON-SNPN and SO-SNPN can be roles taken by either an SNPN or different SNPNs. It is possible for the same network to be in both roles with respect to a specific UE.

##### 5.30.2.10.2 Onboarding Network is an SNPN

5.30.2.10.2.1 General

A UE configured with Default UE credentials may register with an SNPN for the provisioning of SO-SNPN credentials.

5.30.2.10.2.2 Architecture

Figure 5.30.2.10.2.2-1 depicts the architecture for Onboarding of UEs in an ON-SNPN.



Figure 5.30.2.10.2.2-1: Architecture for UE Onboarding in ON-SNPN

NOTE 1: AUSF in the ON-SNPN interfaces with the DCS owned by an entity that is internal or external to the ON-SNPN.

NOTE 2: The functionality with respect to exchange information between PVS and SO-SNPN to provision SNPN credentials and other data from the SO-SNPN in the UE is out of 3GPP scope.

NOTE 3: The dotted lines in Figure 5.30.2.10.2.2-1 indicate that domains (e.g. DCS domain, PVS domain, and SO-SNPN) may not be separated depending on the deployment scenario.

NOTE 4: See TS 33.501 [29] for the functionality beyond AUSF, and other interfaces required for security.

Editor's note: The Architecture Figure 5.30.2.10.2.2-1 is assumed as baseline but should be confirmed by SA WG3 including the DCS functionality supported.

The DCS is used to perform authentication based on the UE default credentials during the Onboarding procedure.

NOTE 5: The DCS and PVS can be owned by an administrative entity that can be different from either the ON-SNPN or SO-SNPN. The ownership of DCS and PVS is outside the scope of 3GPP.

5.30.2.10.2.3 Broadcast system information

When the SNPN supports Onboarding of UEs for SNPNs (i.e. the SNPN can be used as ON-SNPN), the NG-RAN node additionally broadcasts the following information:

- An onboarding enabled indication that indicates whether onboarding is currently enabled for the SNPN. The onboarding enabled indication is broadcasted per cell e.g. to allow start of the onboarding procedure only in parts of the SNPN.

NOTE: Onboarding enabled indication per cell does not affect mobility management functions, i.e. once the UE selects the ON-SNPN as described in clause 5.30.2.10.2.5 and successfully registers within ON-SNPN as described in clause 5.30.2.10.2.6, the UE can move to a cell of the ON-SNPN not indicating onboarding support and continue with the remote provisioning as described in clause 5.30.2.10.4.

5.30.2.10.2.4 UE Configuration Aspects

A UE enabled to support UE Onboarding, shall be pre-configured with Default UE credentials, and the UE may be pre-configured with ON-SNPN selection information.

NOTE 1: The content of the ON-SNPN network selection information depends on UE implementation and can include SNPN network identifiers and/or GIN(s).

The UE uses the ON-SNPN selection information for selection of ON-SNPN (see clause 5.30.2.10.2.5).

NOTE 2: It is assumed that the UE is not pre-configured with a S-NSSAI and DNN for the purpose of UE onboarding in the ON-SNPN.

NOTE 3: The Default UE credentials is used to derive a SUPI. When the UE derives the SUPI from the Default UE credentials, the UE performs specific onboarding procedure as described in clause 5.30.2.10.2.

5.30.2.10.2.5 Network selection

This clause applies only when the UE is in SNPN access mode.

When the UE wants to perform UE onboarding via an SNPN, the UE shall perform ON-SNPN selection as described below. An ON-SNPN is an SNPN providing access to the UE for UE onboarding.

NOTE: The trigger for the UE to initiate the UE Onboarding procedure is UE implementation dependent (e.g. the trigger can be a power-on event in the UE, or an input by the user).

For automatic or manual selection, the UE may select and attempt to register to an ON-SNPN which broadcast the Onboarding enabled indication described in clause 5.30.2.10.2.3 and matches the pre-configured ON-SNPN selection information such as SNPN network identifier and/or GIN(s) (if available) described in clause 5.30.2.10.2.4 according to the UE implementation-specific logic. If the registration fails, the UE may select and attempt to register to a different ON-SNPN in accordance with the pre-configured ON-SNPN selection information.

5.30.2.10.2.6 Registration for UE onboarding

When the user or UE has selected an ON-SNPN according to clause 5.30.2.10.2.5, the UE establishes an RRC connection towards the NG-RAN node of the ON-SNPN. The UE provides an indication in RRC Connection Establishment that the RRC connection is for onboarding as defined in TS 38.331 [28]. This indication allows the NG-RAN node to select an appropriate AMF that supports the UE onboarding procedures. The UE indicates the ON-SNPN as the selected network, and the NG-RAN node shall indicate the selected PLMN ID and NID of the ON-SNPN to the AMF.

NOTE: As the configuration information in the UE does not include any S-NSSAI and DNN used for onboarding, the UE does not include S-NSSAI and DNN in RRC when it registers for UE onboarding purposes to the ONN.

The UE shall initiate the NAS registration procedure by sending a NAS Registration Request message with the following characteristics:

- The UE shall set the 5GS Registration Type to the value "SNPN Onboarding" indicating that the registration request is for onboarding.

- The UE shall provide a SUCI derived from a SUPI as specified in TS 23.003 [19] and TS 33.501 [29]. The SUPI shall uniquely identify the UE and shall be derived from the Default UE Credentials. The ON-SNPN may determine the corresponding DCS identity or address/domain, based on the SUCI (i.e. based on the Home Network Identifier of the SUCI).

The UE does not include a Requested NSSAI in NAS signalling when it registers for UE onboarding purposes to the ONN.

The AMF supporting UE onboarding is configured with AMF Onboarding Configuration Data that may include e.g.:

- S-NSSAI and DNN to be used for UE onboarding or a configured SMF for the DNN and S-NSSAI used for UE onboarding;

- Information to enable User Plane Remote Provisioning of UEs in SNPNs, see clause 5.30.2.10.4.

- Information to use a local AUSF(s) within the ON-SNPN for onboarding of UEs with a SUCI for a DCS with AAA server.

When the AMF receives a NAS Registration Request with a 5GS Registration Type set to "SNPN Onboarding", the AMF:

- starts an authentication procedure towards the AUSF, the authentication procedure is specified in TS 33.501 [29]. The AMF selects an appropriate AUSF as described in clause 6.3.4 based on the Home Network Identifier of the SUCI used during onboarding.

- applies the AMF Onboarding Configuration Data e.g. used to restrict UE network usage to only onboarding for user plane remote provisioning of UE as described in clause 5.30.2.10.4.3.

- stores in the UE context in AMF an indication that the UE is registered for SNPN onboarding.

Upon successful authentication from AUSF, the AMF informs the UE about the result of the registration. If the UE is not successfully authenticated, the AMF shall reject the registration procedure for onboarding, and the UE may select a different ON-SNPN to attempt to register.

5.30.2.10.2.7 Deregistration from the ON-SNPN for onboarding registered UE

Once remote provisioning of SO-SNPN credentials is completed, the UE should initiate deregistration from the ON-SNPN.

Based on ON-SNPN policies, the AMF may start an implementation specific timer once the UE has registered to the ON-SNPN for the purpose of onboarding. Expiry of this timer triggers the AMF to deregister the onboarding registered UE from the ON-SNPN.

When AMF re-allocation occurs for a UE registered for SNPN onboarding during mobility registration update procedure as described in TS 23.502 [3] in clause 4.2.2.2.2 or during N2 based handover as described in TS 23.502 [3] clause 4.9.1.3, the new AMF supporting UE SNPN onboarding should be selected as described in clause 6.3.5. If the new AMF receives in UE context the indication that the UE is registered for SNPN onboarding, the new AMF may start an implementation specific timer for when to deregister the UE when the new AMF completes the Registration procedure (i.e. sends Registration Accept to the UE) or completes the N2 based handover procedure.

NOTE 1: This specific timer is used to prevent onboarding registered UEs from staying at the ON-SNPN indefinitely.

NOTE 2: When Onboarding network is a PLMN and the UE's subscription only allows for Remote Provisioning, then based on PLMN policies, the AMF can start an implementation specific timer once the UE has registered to the PLMN. Expiry of this timer triggers the AMF to deregister the UE from the PLMN. This specific timer is used to prevent registered UEs that only allow for Remote Provisioning from staying at the PLMN indefinitely.

##### 5.30.2.10.3 Onboarding Network is a PLMN

5.30.2.10.3.1 General

A UE configured with PLMN credentials in USIM for primary authentication may register with a PLMN for the provisioning of SO-SNPN credentials.

5.30.2.10.3.2 Network selection and Registration

This clause applies only when the UE is not in SNPN access mode.

When the UE is using PLMN credentials for accessing a PLMN as the Onboarding Network (ONN), then regular network selection, as per TS 23.122 [17] and regular initial registration procedures apply, as per TS 23.502 [3]. After successfully registering to the ON-PLMN, the UE is provisioned with the SO-SNPN credentials via User Plane as in clause 5.30.2.10.4.4.

##### 5.30.2.10.4 Remote Provisioning of UEs in Onboarding Network

5.30.2.10.4.1 General

Once the UE has registered, and a PDU Session is established the UE uses configuration data to select and communicate with a PVS for initiating Remote Provisioning. The PDU Session may be restricted to be used for Remote Provisioning of the UE.

5.30.2.10.4.2 Onboarding configuration for the UE

In order to enable UP Remote Provisioning of SNPN credentials for a UE, UE Configuration Data for UP Remote Provisioning are either pre-configured on the UE or provided by the ON-SNPN. UE Configuration Data for UP Remote Provisioning provided by the ON-SNPN take precedence over corresponding configuration data stored in the UE.

UE Configuration Data for UP Remote Provisioning consist of PVS IP address or PVS FQDN.

If the UE does not have any PVS IP address or PVS FQDN after the establishment of the restricted PDU Session used for onboarding, the UE may construct an FQDN for PVS discovery as defined in TS 23.003 [19].

The UE Configuration Data for UP Remote Provisioning may be stored in the ME.

The UE Configuration Data for UP Remote Provisioning (i.e. PVS IP address or PVS FQDN) may be either:

- locally configured in the SMF of ON-SNPN; or

- provided by the DCS to the AMF of ON-SNPN as part of the authentication procedure as specified in TS 33.501 [29] and sent by the AMF in the PDU Session Establishment Request to the SMF. If PCF is used for UP Remote Provisioning, SMF provides the UE Configuration Data to PCF when requesting an SM Policy Association.

The UE Configuration Data for UP Remote Provisioning may be provided to the UE during the establishment of the restricted PDU Session as part of Protocol Configuration Options (PCO) in the PDU Session Establishment Response.

5.30.2.10.4.3 User Plane Remote Provisioning of UEs when Onboarding Network is an ON-SNPN

If Onboarding Services are provided using a restricted PDU Session for remote provisioning of UE via User Plane, the AMF selects an SMF used for Onboarding Services using the SMF discovery and selection functionality as described in clause 6.3.2. The AMF Onboarding Configuration Data may contain an S-NSSAI and a DNN used for Onboarding to select an SMF used for Onboarding Services or may contain a configured SMF for the DNN used for Onboarding.

When a UPF is selected for Onboarding Services, the UPF selection function described in clause 6.3.3 for normal services is applied considering the DNN used for Onboarding.

The SMF or the PCF may store S-NSSAI and DNN information used for Onboarding. Onboarding Configuration Data available to PCF (for details see TS 23.503 [45]) and/or SMF may include PVS FQDN and PVS IP address(es).

When the UE registered for Onboarding successfully completes the user plane remote provisioning of SNPN credentials via the Onboarding Network, then the UE should deregister from the Onboarding Network.

Initial QoS parameters used for establishing Onboarding Services are configured in the SMF when dynamic PCC is not used.

Dynamic PCC may be used for a PDU session that is established for Onboarding Services as described in TS 23.503 [45]).

The QoS Flows of a PDU Session associated with the restricted DNN shall be dedicated to Onboarding Services. The SMF may configure PDR and FAR including PVS and DNS server IP addresses for the UPF to block any traffic that is not from or to PVS and DNS server addresses.

If the UE is registered for Onboarding, the network should apply S-NSSAI and DNN in the Onboarding Configuration Data for the PDU Session Establishment request from the UE.

5.30.2.10.4.4 User Plane Remote Provisioning of UEs when Onboarding Network is a PLMN

Onboarding Services for a UE may be provided via PLMN using PDU Session for DNN(s) and S-NSSAI(s) used for onboarding. Subscription data of such a UE shall contain the DNN and S-NSSAI used for onboarding.

The AMF selects an SMF used for remote provisioning using the SMF discovery and selection functionality as described in clause 6.3.2, considering the DNN and S-NSSAI used for onboarding provided by the UE or the default DNN and S-NSSAI provided by UDM.

The UPF selection function described in clause 6.3.3 is applied, considering the DNN and S-NSSAI used for onboarding.

The SMF may be configured with one or more PVS FQDN and/or PVS IP address(es) per DNN and S-NSSAI used for onboarding. The SMF may send the PVS FQDN and/or PVS IP address(es) associated to the DNN and S-NSSAI of the PDU Session to the UE as part of Protocol Configuration Options (PCO) in the PDU Session Establishment Response.

#### 5.30.2.11 UE Mobility support for SNPN

If the UE moves its 3GPP access between SNPN and PLMN the UE performs initial registration as specified in clause 4.2.2.2.2 of TS 23.502 [3].

If the UE moves its 3GPP access between SNPNs, then the UE performs initial or mobility registration as specified in clause 4.2.2.2.2 of TS 23.502 [3].

NOTE: When the UE moves its 3GPP access between SNPNs, it is up to UE implementation whether and when to establish again PDU Sessions using existing mechanism.

### 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).

The UE and PNI-NPN may support remote provisioning of credentials for NSSAA or credentials for secondary authentication/authorization to the UE, as specified in clause 5.39.

NOTE 3: After successful provisioning of the credentials to the UE, specific service subscription data (e.g. to enable the use of PNI-NPN) can be activated in the UE Subscription data in the UDR/UDM. This can result in a change of the UE Subscription Data to include new S-NSSAI, DNN or CAG information, which can trigger update of the UE configurations, e.g. described in clause 5.15.5.2.2.

NOTE 4: The UE always has subscription to the HPLMN providing the PNI-NPN and has a USIM that contains primary authentication credentials.

#### 5.30.3.2 Identifiers

The following is required for identification:

- A CAG is identified by a CAG Identifier which is unique within the scope of a PLMN ID;

- A CAG cell broadcasts one or multiple CAG Identifiers per PLMN;

NOTE 1: It is assumed that a cell supports broadcasting a total of twelve CAG Identifiers. Further details are defined in TS 38.331 [28].

- A CAG cell may in addition broadcast a human-readable network name per CAG Identifier:

NOTE 2: The human-readable network name per CAG Identifier is only used for presentation to user when user requests a manual CAG selection.

#### 5.30.3.3 UE configuration, subscription aspects and storage

To use CAG, the UE, that supports CAG as indicated as part of the UE 5GMM Core Network Capability, may be pre-configured or (re)configured with the following CAG information, included in the subscription as part of the Mobility Restrictions:

- an Allowed CAG list i.e. a list of CAG Identifiers the UE is allowed to access; and

- optionally, a CAG-only indication whether the UE is only allowed to access 5GS via CAG cells (see TS 38.304 [50] for how the UE identifies whether a cell is a CAG cell);

The HPLMN may configure or re-configure a UE with the above CAG information using the UE Configuration Update procedure for access and mobility management related parameters described in clause 4.2.4.2 of TS 23.502 [3].

The above CAG information is provided by the HPLMN on a per PLMN basis. In a PLMN the UE shall only consider the CAG information provided for this PLMN.

When the subscribed CAG information changes, UDM sets a CAG information Subscription Change Indication and sends it to the AMF. The AMF shall provide the UE with the CAG information when the UDM indicates that the CAG information within the Access and Mobility Subscription data has been changed. When AMF receives the indication from the UDM that the CAG information within the Access and Mobility Subscription has changed, the AMF uses the CAG information received from the UDM to update the UE. Once the AMF updates the UE and obtains an acknowledgment from the UE, the AMF informs the UDM that the update was successful and the UDM clears the CAG information Subscription Change Indication flag.

The AMF may update the UE using either the UE Configuration Update procedure after registration procedure is completed, or by including the new CAG information in the Registration Accept or in the Registration Reject or in the Deregistration Request or in the Service Reject.

When the UE is roaming and the Serving PLMN provides CAG information, the UE shall update only the CAG information provided for the Serving PLMN while the stored CAG information for other PLMNs are not updated. When the UE is not roaming and the HPLMN provides CAG information, the UE shall update the CAG information stored in the UE with the received CAG information for all the PLMNs.

The UE shall store the latest available CAG information for every PLMN for which it is provided and keep it stored when the UE is de-registered or switched off, as described in TS 24.501 [47].

The CAG information is only applicable with 5GS.

NOTE: CAG information has no implication on whether and how the UE accesses 5GS over non-3GPP access.

#### 5.30.3.4 Network and cell (re-)selection, and access control

The following is assumed for network and cell selection, and access control:

- The CAG cell shall broadcast information such that only UEs supporting CAG are accessing the cell (see TS 38.300 [27], TS 38.304 [50]);

NOTE 1: The above also implies that cells are either CAG cells or normal PLMN cells. For network sharing scenario between SNPN, PNI-NPN and PLMNs, please see clause 5.18.

- In order to prevent access to NPNs for authorized UE(s) in the case of network congestion/overload, existing mechanisms defined for Control Plane load control, congestion and overload control in clause 5.19 can be used, as well as the access control and barring functionality described in clause 5.2.5, or Unified Access Control using the access categories as defined in TS 24.501 [47] can be used.

- For aspects of automatic and manual network selection in relation to CAG, see TS 23.122 [17];

- For aspects related to cell (re-)selection, see TS 38.304 [50];

- The Mobility Restrictions shall be able to restrict the UE's mobility according to the Allowed CAG list (if configured in the subscription) and include an indication whether the UE is only allowed to access 5GS via CAG cells (if configured in the subscription) as described in clause 5.30.3.3;

- During transition from CM-IDLE to CM-CONNECTED and during Registration after connected mode mobility from E-UTRAN to NG-RAN as described in clause 4.11.1.2.2 of TS 23.502 [3]:

- The AMF shall verify whether UE access is allowed by Mobility Restrictions:

NOTE 2: It is assumed that the AMF is made aware of the supported CAG Identifier(s) of the CAG cell by the NG-RAN.

- If the UE is accessing the 5GS via a CAG cell and if at least one of the CAG Identifier(s) received from the NG-RAN is part of the UE's Allowed CAG list, then the AMF accepts the NAS request;

- If the UE is accessing the 5GS via a CAG cell and if none of the CAG Identifier(s) received from the NG-RAN are part of the UE's Allowed CAG list, then the AMF rejects the NAS request and the AMF should include CAG information in the NAS reject message. The AMF shall then release the NAS signalling connection for the UE by triggering the AN release procedure; and

- If the UE is accessing the 5GS via a non-CAG cell and the UE's subscription contains an indication that the UE is only allowed to access CAG cells, then the AMF rejects the NAS request and the AMF should include CAG information in the NAS reject message. The AMF shall then release the NAS signalling connection for the UE by triggering the AN release procedure.

- During transition from RRC Inactive to RRC Connected state:

- When the UE initiates the RRC Resume procedure for RRC Inactive to RRC Connected state transition in a CAG cell, NG-RAN shall reject the RRC Resume request from the UE if none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list according to the Mobility Restrictions received from the AMF.

- When the UE initiates the RRC Resume procedure for RRC Inactive to RRC Connected state transition in a non-CAG cell, NG-RAN shall reject the UE's Resume request if the UE is only allowed to access CAG cells according to the Mobility Restrictions received from the AMF.

- During connected mode mobility procedures within NG-RAN, i.e., handover procedures as described in clause 4.9.1 of TS 23.502 [3]:

- Based on the Mobility Restrictions received from the AMF:

- Source NG-RAN shall not handover the UE to a target NG-RAN node if the target is a CAG cell and none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list;

- Source NG-RAN shall not handover the UE to a non-CAG cell if the UE is only allowed to access CAG cells;

- If the target cell is a CAG cell, target NG-RAN shall reject the N2 based handover procedure if none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list in the Mobility Restriction List;

- If the target cell is a non-CAG cell, target NG-RAN shall reject the N2 based handover procedure if the UE is only allowed to access CAG cells based on the Mobility Restriction List.

- Update of Mobility Restrictions:

- When the AMF receives the Nudm\_SDM\_Notification from the UDM and the AMF determines that the Allowed CAG list or the indication whether the UE is only allowed to access CAG cells have changed;

- The AMF shall update the Mobility Restrictions in the UE and NG-RAN accordingly under the conditions as described in clause 4.2.4.2 of TS 23.502 [3].

NOTE 3: When the UE is accessing the network for emergency service the conditions for AMF in clause 5.16.4.3 apply.

#### 5.30.3.5 Support of emergency services in CAG cells

Emergency Services are supported in CAG cells, for UEs supporting CAG, whether normally registered or emergency registered as described in clause 5.16.4 and in clause 4.13.4 of TS 23.502 [3].

A UE may camp on an acceptable CAG cell in limited service state as specified in TS 23.122 [17] and TS 38.304 [50], based on operator policy defined in TS 38.300 [27].

NOTE: Support for Emergency services requires each cell with a Cell Identity associated with PLMNs or PNI-NPNs to only be connected to AMFs that supports emergency services.

The UE shall select a PLMN (of a CAG cell or non-CAG cell), as described in TS 23.122 [17] and TS 23.167 [18], when initiating emergency services from limited service state.

During handover to a CAG cell, if the UE is not authorized to access the target CAG cell and has emergency services, the target NG-RAN node only accepts the emergency PDU sessions and the target AMF releases the non-emergency PDU connections that were not accepted by the NG-RAN node. Upon completion of handover the UE behave as emergency registered.

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

## 5.39 Remote provisioning of credentials for NSSAA or secondary authentication/authorization

### 5.39.1 General

The UE and the HPLMN may provide functionalities to provision or update the credentials used for NSSAA or credentials used for secondary authentication/authorization to the UE. The provisioning via UE Parameters Update procedure as defined in clause 4.20 of TS 23.502 [3] and via User Plane are both supported.

Editor's note: It is FFS whether and how the credentials can be sent from a provisioning server (e.g. using an AF) to the UDM and whether NEF is needed.

For User Plane provisioning, the UE establishes a PDU Session that is used for remote provisioning, e.g. by using DNN(s)/S-NSSAI(s) which can access the PVS. If the SMF is configured with the PVS address(es) and/or PVS FQDN(s), the SMF shall send the address of the PVS per DNN/S-NSSAI to the UE via PCO during PDU Session establishment procedure. Alternatively, the UE may be configured with an address of a PVS or the PVS may subscribe for UE Reachability Notification and may use the Application Triggering procedure as specified in TS 23.502 [3] to trigger the UE to initiate the setup of a connection for remote provisioning.

### 5.39.2 Configuration for the UE

In order to enable UP Remote Provisioning of credentials for NSSAA or secondary authentication/authorization, UE Configuration Data for UP Remote Provisioning are either pre-configured on the UE or provided by the network to the UE. UE Configuration Data for UP Remote Provisioning provided by the network take precedence over corresponding configuration data stored in the UE.

UE Configuration Data for UP Remote Provisioning consist of PVS IP address(es) and/or PVS FQDN(s). The PVS IP address or PVS FQDN may be associated with dedicated DNN(s) and/or S-NSSAI(s).

If the UE does not have any PVS IP address or PVS FQDN after the establishment of a PDU Session used for UP remote provisioning, the UE may construct an FQDN for PVS discovery as defined in TS 23.003 [19].

The UE Configuration Data for UP Remote Provisioning may be stored in the ME.

The UE Configuration Data for UP Remote Provisioning (i.e. PVS IP address(es) or PVS FQDN(s)) associated with dedicated DNN(s) and/or S-NSSAI(s) may be locally configured in the SMF and may be provided to the UE during the establishment of any PDU Session used for UP Remote Provisioning as part of Protocol Configuration Options (PCO) in the PDU Session Establishment Response.

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