**3GPP TSG-WG SA2 Meeting #147E  *S2-2107188r03***

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **3257** | **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, Nokia, Nokia Shanghai Bell, vivo, Deutsche Telekom |
| ***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:*** | 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.In TS 23.502 4.3.2.2.1, the PVS IP address/FQDN is included in the Nsmf\_PDUSession\_CreateSMContext Request message, not in N1 PDU Session Establishment Request from UE. |
|  |  |
| ***Summary of change:*** | 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. Put Note 2 to void about PLMN deregistration timer in clause 5.30.2.10.2.7 and added the same Note in clause 5.30.2.10.3.2 which is about PLMN selection and registration. Corrected cut and paste error in D.3 Replaces the PDU Session Establishment Request message with the Nsmf\_PDUSession\_CreateSMContext Request message when AMF provides the PVS IP address/FQDN to SMF in clause 5.30.2.10.4.2. |
| ***--*** |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.30.2.0, 5.30.2.3, 5.30.2.10.2.7, 5.30.2.10.3.2, 5.30.2.10.4.2, 5.39.1, 5.39.2, D.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ... |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR’s revision history:*** |  |

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

### 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.

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

#### 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 Routing Indicator can be used for AUSF/UDM discovery and selection as long as the Routing Indicator 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 Routing Indicator can be used as long as the Routing Indicator 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.

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

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 4.2.2.2.4 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: Void

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

##### 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.

NOTE x: 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 are only allowed for Remote Provisioning from staying at the PLMN indefinitely.

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

5.30.2.10.4.1 General

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

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 Nsmf\_PDUSession\_CreateSMContext Request message 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.

\* \* \* \* 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.

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

D.3 Support for access to PLMN services via Stand-alone Non-Public Network and access to Stand-alone Non Public Network services via PLMN



**Figure D.3-1: Access to PLMN services via Stand-alone Non-Public Network**

NOTE 1: The reference architecture in Figure D.3-1 and Figure D.3-2 only shows the network functions directly connected to the UPF or N3IWF and other parts of the architecture are same as defined in clause 4.2.

In order to obtain access to PLMN services when the UE is camping in NG-RAN of Stand-alone Non-Public Network, the UE obtains IP connectivity, discovers and establishes connectivity to an N3IWF in the PLMN.

In the Figure D.3-1, the N1 (for NPN) represents the reference point between UE and the AMF in Stand-alone Non-Public Network. The NWu (for PLMN) represents the reference point between the UE and the N3IWF in the PLMN for establishing secure tunnel between UE and the N3IWF over the Stand-alone Non-Public Network. N1 (for PLMN) represents the reference point between UE and the AMF in PLMN.



**Figure D.3-2: Access to Stand-alone Non-Public Network services via PLMN**

In order to obtain access to Non-Public Network services when the UE is camping in NG-RAN of a PLMN, the UE obtains IP connectivity, discovers and establishes connectivity to an N3IWF in the Stand-alone Non-Public Network.

In Figure D.3-2, the N1 (for PLMN~~NPN~~) represents the reference point between UE and the AMF in the PLMN ~~Stand-alone Non-Public Network~~. The NWu (for NPN) represents the reference point between the UE and the N3IWF in the stand-alone Non-Public Network for establishing a secure tunnel between UE and the N3IWF over the PLMN. The N1 (for NPN~~PLMN~~) represents the reference point between UE and the AMF in NPN~~PLMN~~.

When using the mechanism described above to access overlay network via underlay network, the overlay network can act as authorized 3rd party with AF to interact with NEF in the underlay network, to use the existing network exposure capabilities provided by the underlay network defined in clause 4.15 of TS 23.502 [3]. This interaction is subject of agreements between the overlay and the underlay network.

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