**SA WG2 Meeting #143eS2-210xxxx**

**Feb 24th – March 9th, 2021 ; Elbonia (revision of S2-210)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **xx** | **rev** | **-** | **Current version:** | **16.7.0** |  |
|  |
| *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 | **x** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | SNPN with separate entity hosting subscription |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S2 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-01-18 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | TR 23.700-07 conclusion for the following item needs to be implemented in TS 23.501:

|  |  |
| --- | --- |
| KI#1:T1-b | Feature description: Architectures for access to SNPN using credentials from a separate entity |

- Separate entity with AUSF and UDM- Separate entity with PLMN subscriptionHere is the conclusion from TR 23.700-07 for access to SNPN using credential from separate entity hosting AUSF and UDM.8.1.6 Conclusions for scenario where the SNPN offers connectivity for UE(s) with credentials owned by separate entity offering AUSF and UDMThe scenario where the separate entity hosts UDM, AUSF and owns the subscription is supported. It is proposed to adopt the following conclusion principles:- Discovery of AUSF/UDM in the separate entity can be supported by cross network service discovery and registration procedure as specified in TS 23.502 [6] clause 4.17.5 where Home PLMN is replaced by the separate entity. In order to facilitate selection of the separate entity owning the subscription (i.e. AUSF, UDM in the Home SNPN), the SUPI/SUCI provided by the UE contains a Home Network Identifier. When the SUPI type is an IMSI, the Home Network Identifier should comprise of PLMN ID + NID that points to the external entity; if SUPI is a Network Specific Identifier, the domain name corresponds to the realm part and the realm should identify the external entity.- It is recommended to enhance Nudm, Nausf, Namf and Nsmf services to support access to an SNPN using credentials from a separate entity that has UDM and AUSF, with the limitation that Session Management procedures are only supported for PDU Sessions terminating in the SNPN.And:- Here is the conclusion from TR 23.700-07 for access to SNPN using credential from separate entity using PLMN subscription.8.1.5 Conclusions for UEs with a PLMN subscriptionThe following enhancements will be progressed in the normative phase on how to perform SNPN access network authentication of a UE based on 3GPP identities and credentials supplied by the PLMN:- SIB enhancements as described in clause 8.1.4. **-> out of scope for this CR**- UE configuration enhancements as described in clause 8.1.4. **-> out of scope for this CR**- PLMN controlled information for SNPN selection in the UE can be updated using the UE Parameters Update via UDM Control Plane Procedure as defined in TS 23.502 [6] clause 4.20.2 or Steering of Roaming (SoR) as defined in TS 23.122 [5] Annex C. **-> no changes to TS expected**- Network selection and registration.- To enable a UE with PLMN subscription to select an SNPN, the UE needs to enter SNPN access mode.- Once the UE has entered SNPN access mode, SNPN selection is performed as described in clause 8.1.4.- Once an SNPN has been selected the UE attempts registration using the PLMN credentials. |
|  |  |
| ***Summary of change:*** | Implement the above conclusion as follows:1. Introduce SNPN with separate entity (hosting UDM, AUSF) architecture
2. Update SUPI for identification of external entity.
3. Update SNPN General description to refer to the architecture and state the SM restriction.
4. Update UE subscription section to list SNPN selection method when it needs to select SNPN but contains PLMN subscription.
5. Update AUSF and UDM discovery and selection
 |
|  |  |
| ***Consequences if not approved:*** | eNPN Feature not implemented |
|  |  |
| ***Clauses affected:*** | 4.2.3, 5.9.2, 5.30.2.0, 5.30.2.3, 6.3.4, 6.3.8 |
|  |  |
|  | **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:*** |  |

*FIRST CHANGE*

### 4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.



Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

Figure 4.2.3-2 depicts the 5G System architecture in the non-roaming case, using the reference point representation showing how various network functions interact with each other.



NOTE 1: N9, N14 are not shown in all other figures however they may also be applicable for other scenarios.

NOTE 2: For the sake of clarity of the point-to-point diagrams, the UDSF, NEF and NRF have not been depicted. However, all depicted Network Functions can interact with the UDSF, UDR, NEF and NRF as necessary.

NOTE 3: The UDM uses subscription data and authentication data and the PCF uses policy data that may be stored in UDR (refer to clause 4.2.5).

NOTE 4: For clarity, the UDR and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on data storage architectures refer to clause 4.2.5.

NOTE 5: For clarity, the NWDAF and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on network data analytics architecture refer to TS 23.288 [86].

Figure 4.2.3-2: Non-Roaming 5G System Architecture in reference point representation

Figure 4.2.3-3 depicts the non-roaming architecture for UEs concurrently accessing two (e.g. local and central) data networks using multiple PDU Sessions, using the reference point representation. This figure shows the architecture for multiple PDU Sessions where two SMFs are selected for the two different PDU Sessions. However, each SMF may also have the capability to control both a local and a central UPF within a PDU Session.



Figure 4.2.3-3: Applying non-roaming 5G System architecture for multiple PDU Session in reference point representation

Figure 4.2.3-4 depicts the non-roaming architecture in the case of concurrent access to two (e.g. local and central) data networks is provided within a single PDU Session, using the reference point representation.



Figure 4.2.3-4: Applying non-roaming 5G System architecture for concurrent access to two (e.g. local and central) data networks (single PDU Session option) in reference point representation

Figure 4.2.3-5 depicts the non-roaming architecture for Network Exposure Function, using reference point representation.



Figure 4.2.3-5: Non-roaming architecture for Network Exposure Function in reference point representation

NOTE 1: In figure 4.2.3-5, Trust domain for NEF is same as Trust domain for SCEF as defined in TS 23.682 [36].

NOTE 2: In figure 4.2.3-5, 3GPP Interface represents southbound interfaces between NEF and 5GC Network Functions e.g. N29 interface between NEF and SMF, N30 interface between NEF and PCF, etc. All southbound interfaces from NEF are not shown for the sake of simplicity.

Figure 4.2.3-6 and Figure 4.2.3-7 depict the 5G System architecture (in service-based and reference point based representation respectively) for SNPN with separate entity owning the UE(s) subscription and with SNPN allowing access to UE(s) with credentials assigned by separate entity.



Figure 4.2.3-6: 5G System architecture with access to SNPN using credential from Separate entity - service-based interface representation



Figure 4.2.3-7: 5G System architecture with access to SNPN using credential from Separate entity - reference point representation

### 4.2.4 Roaming reference architectures

Figure 4.2.4-1 depicts the 5G System roaming architecture with local breakout with service-based interfaces within the Control Plane.



Figure 4.2.4-1: Roaming 5G System architecture- local breakout scenario in service-based interface representation

NOTE 1: In the LBO architecture. The PCF in the VPLMN may interact with the AF in order to generate PCC Rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation. The PCF in VPLMN has no access to subscriber policy information from the HPLMN.

NOTE 2: An SCP can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

Figure 4.2.4-3 depicts the 5G System roaming architecture in the case of home routed scenario with service-based interfaces within the Control Plane.



Figure 4.2.4-3: Roaming 5G System architecture - home routed scenario in service-based interface representation

NOTE 3: An SCP can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

NOTE 4: UPFs in the home routed scenario can be used also to support the IPUPS functionality (see clause 5.8.2.14).

Figure 4.2.4-4 depicts 5G System roaming architecture in the case of local break out scenario using the reference point representation.



Figure 4.2.4-4: Roaming 5G System architecture - local breakout scenario in reference point representation

NOTE 5: The NRF is not depicted in reference point architecture figures. Refer to Figure 4.2.4-7 for details on NRF and NF interfaces.

NOTE 6: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

The following figure 4.2.4-6 depicts the 5G System roaming architecture in the case of home routed scenario using the reference point representation.



Figure 4.2.4-6: Roaming 5G System architecture - Home routed scenario in reference point representation

For the roaming scenarios described above each PLMN implements proxy functionality to secure interconnection and hide topology on the inter-PLMN interfaces.



Figure 4.2.4-7: NRF Roaming architecture in reference point representation

NOTE 7: For the sake of clarity, SEPPs on both sides of PLMN borders are not depicted in figure 4.2.4-7.

Operators can deploy UPFs supporting the Inter PLMN UP Security (IPUPS) functionality at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios. The UPFs supporting the IPUPS functionality in VPLMN and HPLMN are controlled by the V-SMF and the H-SMF of that PDU Session respectively. A UPF supporting the IPUPS functionality terminates GTP-U N9 tunnels. The SMF can activate the IPUPS functionality together with other UP functionality in the same UPF, or insert a separate UPF for the IPUPS functionality in the UP path (which e.g. may be dedicated to be used for IPUPS functionality). Figure 4.2.4-9 depicts the home routed roaming architecture where a UPF is inserted in the UP path for the IPUPS functionality. Figure 4.2.4-3 depicts the home routed roaming architecture where the two UPFs perform the IPUPS functionality and other UP functionality for the PDU Session.

NOTE 8: Operators are not prohibited from deploying the IPUPS functionality as a separate Network Function from the UPF, acting as a transparent proxy which can transparently read N4 and N9 interfaces. However, such deployment option is not specified and needs to take at least into account very long lasting PDU Sessions with infrequent traffic and Inter-PLMN handover.

The IPUPS functionality is specified in clause 5.8.2.14 and TS 33.501 [29].



Figure 4.2.4-9: Roaming 5G System architecture - home routed roaming scenario in service-based interface representation employing UPF dedicated to IPUPS

*NEXT CHANGE*

### 5.9.2 Subscription Permanent Identifier

A globally unique 5G Subscription Permanent Identifier (SUPI) shall be allocated to each subscriber in the 5G System and provisioned in the UDM/UDR. The SUPI is used only inside 3GPP system, and its privacy is specified in TS 33.501 [29].

The SUPI may contain:

- an IMSI as defined in TS 23.003 [19], or

- a network-specific identifier, used for private networks as defined in TS 22.261 [2].

- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [84].

- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [84].

A SUPI containing a network-specific identifier shall take the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [20] based user identification as defined in TS 23.003 [19].

When UE needs to indicate its SUPI to the network (e.g. as part of the Registration procedure), the UE provides the SUPI in concealed form as defined in TS 23.003 [19].

In order to enable roaming scenarios, the SUPI shall contain the address of the home network (e.g. the MCC and MNC in the case of an IMSI based SUPI).

In case of SNPN with separate entity hosting subscription, the IMSI based SUPI shall also include NID along with the MCC and MNC as part of home network address that points to the separate entity. If SUPI is a Network Specific Identifier in the form of username@realm, the domain name corresponds to the realm part and the realm should identify the separate entity.

For interworking with the EPC, the SUPI allocated to the 3GPP UE shall always be based on an IMSI to enable the UE to present an IMSI to the EPC.

The usage of SUPI for W-5GAN is further specified in TS 23.316 [84].

*NEXT CHANGE*

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

SNPN also supports access to UE(s) using credentials assigned by a separate entity. An architecture in which the separate entity hosts UE’s subscription is shown in figure 4.2.3-6, 4.2.3-7. For such an architecture, the limitation is that the Session Management procedures (i.e. PDU Sessions) terminate in the SNPN.

Interworking with EPS is not supported for SNPN. Also, emergency services are not supported for SNPN. 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. CIoT 5GS optimizations are not supported in SNPNs.

*NEXT CHANGE*

#### 5.30.2.3 UE configuration and subscription aspects

An SNPN-enabled UE is configured with subscriber identifier (SUPI), credentials for each subscribed SNPN identified by the combination of PLMN ID and NID. If an SNPN-enabled UE is configured with an N3IWF, it is also configured with an identifier of the country where the configured N3IWF is located.

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 TS 23.003 [19] clause 28.7.2. The realm part of the NAI may include the NID of the SNPN; or

- identified by a SUPI containing an IMSI.

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 not supported in SNPN access mode.

NOTE 1: Voice support with emergency services in SNPN access mode is not specified in this release.

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. Annex D.4 provides more details.

NOTE 2: Details of activation and deactivation of SNPN access mode are up to UE implementation.

If the UE has credentials supplied by the PLMN and subscription from PLMN, the UE needs to enter SNPN access mode in order to select SNPN. 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 using the PLMN credentials.*NEXT CHANGE*

### 6.3.4 AUSF discovery and selection

In the case of NF consumer based discovery and selection, the following applies:

- The AMF performs AUSF selection to allocate an AUSF Instance that performs authentication between the UE and 5G CN in the HPLMN. The AMF shall utilize the NRF to discover the AUSF instance(s) unless AUSF information is available by other means, e.g. locally configured on AMF. The AUSF selection function in the AMF selects an AUSF instance based on the available AUSF instances (obtained from the NRF or locally configured in the AMF).

- The UDM shall utilize the NRF to discover the AUSF instance(s) unless AUSF information is available by other means, e.g. locally configured on UDM. The UDM selects an AUSF instance based on the available AUSF instance(s) obtained from the NRF or based on locally configured information, and information stored (by the UDM) from a previously successful authentication.

AUSF selection is applicable to both 3GPP access and non-3GPP access.

The AUSF selection function in AUSF NF consumers or in SCP should consider one of the following factors when available:

1. Home Network Identifier (e.g., MNC and MCC) of SUCI/SUPI (by an NF consumer in the Serving network) along with identification for separate entity (if NID is available in the Home Network Identifier within the SUCI provided by the UE or the UE provides a realm that identifies the separate entity; otherwise, it uses the NID provided by the NG-RAN) in the case of SNPN and Routing Indicator.

NOTE 1: The UE provides the Routing Indicator to the AMF as part of the SUCI as defined in TS 23.003 [19] during initial registration. The AMF can provide the UE's Routing Indicator to other AMFs as described in TS 23.502 [3].

NOTE 2: In the case of SNPN, the AMF uses the NID that is part of Home Network Identifier available in the SUCI provided by the UE. If the SUCI does not include the NID, then it uses the selected NID provided by the NG-RAN together with the selected PLMN ID (from SUCI/SUPI) as the SUCI/SUPI does not always include the NID.

 When the UE's Routing Indicator is set to its default value as defined in TS 23.003 [19], the AUSF NF consumer can select any AUSF instance within the home network for the UE.

2. AUSF Group ID the UE's SUPI belongs to.

NOTE 3: The AMF can infer the AUSF Group ID the UE's SUPI belongs to, based on the results of AUSF discovery procedures with NRF. The AMF provides the AUSF Group ID the SUPI belongs to other AMFs as described in TS 23.502 [3].

3. SUPI; e.g. the AMF selects an AUSF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for AUSF discovery.

In the case of delegated discovery and selection in SCP, the AUSF NF consumer shall send all available factors to the SCP.

*NEXT CHANGE*

### 6.3.8 UDM discovery and selection

The NF consumer or the SCP performs UDM discovery to discover a UDM instance that manages the user subscriptions.

If the NF consumer performs discovery and selection, the NF consumers shall utilize the NRF to discover the UDM instance(s) unless UDM information is available by other means, e.g. locally configured on NF consumers. The UDM selection function in NF consumers selects a UDM instance based on the available UDM instances (obtained from the NRF or locally configured).

The UDM selection functionality is applicable to both 3GPP access and non-3GPP access.

The UDM selection functionality in NF consumer or in SCP should consider one of the following factors:

1. Home Network Identifier (e.g. MNC and MCC) of SUCI/SUPI, along with identification for separate entity (if NID is available in the Home Network Identifier within the SUCI provided by the UE or the UE provides a realm that identifies the separate entity; otherwise, it uses the NID provided by the NG-RAN) in the case of SNPN, and UE's Routing Indicator.

NOTE 1: The UE provides the Routing Indicator to the AMF as part of the SUCI as defined in TS 23.003 [19] during initial registration. The AMF provides the UE's Routing Indicator to other NF consumers (of UDM) as described in TS 23.502 [3].

NOTE 2: In the case of SNPN, the AMF uses the NID that is part of Home Network Identifier available in the SUCI provided by the UE. If the SUCI does not include the NID or the UE does not provide a realm that identifies the separate entity, then it uses the selected NID provided by the NG-RAN together with the selected PLMN ID (from SUCI/SUPI).

 When the UE's Routing Indicator is set to its default value as defined in TS 23.003 [19], the UDM NF consumer can select any UDM instance within the home network of the SUCI/SUPI.

2. UDM Group ID of the UE's SUPI.

NOTE 3: The AMF can infer the UDM Group ID the UE's SUPI belongs to, based on the results of UDM discovery procedures with NRF. The AMF provides the UDM Group ID the SUPI belongs to other UDM NF consumers as described in TS 23.502 [3].

3. SUPI or Internal Group ID; the UDM NF consumer selects a UDM instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI or Internal Group ID as input for UDM discovery.

4. GPSI or External Group ID; UDM NF consumers which manage network signalling not based on SUPI/SUCI (e.g. the NEF) select a UDM instance based on the GPSI or External Group ID range the UE's GPSI or External Group ID belongs to or based on the results of a discovery procedure with NRF using the UE's GPSI or External Group ID as input for UDM discovery.

In the case of delegated discovery and selection in SCP, NF consumer shall include one of these factors in the request towards SCP.

*END CHANGE*