**3GPP TSG-WG SA2 Meeting #162S2-240xxxx**

**15 – 19 April 2024, Changsha, CN (revision of S2-2402085)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.501** | **CR** | **-** | **rev** | **-** | **Current version:** | **18.5.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | RVAS with NF selection in target PLMN enhancement. | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Nokia, Nokia Shanghai Bell, Deutsche Telekom, AT&T | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI19\_RVAS | | | | |  | ***Date:*** | | | 2024-04-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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 can be 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | To address the scenario described in TEI19-xxx where HPLMN may desire to control and allocate certain NF instance (e.g. the anchor SMF for aPDU session) in a partner network to receive services. Thus, the SMF selection function can be enhanced based on extra subscription data e.g. target network identifier (similar to the APN-OI-Replacement parameter in EPS), locality. With these parameters, the HPLMN can influence on the NRF query parameters formulated by AMF during SMF selection.  The HPLMN NRF handling may utilize the NRF in the partner network to resolve the NF instance. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Introduce SMF selection enhancement considering the additional parameters provided in the subscription data.  Clarify the hNRF handling considering the partner/target PLMN scenario. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Missing functionality. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.3, 4.2.4, 5.6.1, 6.2.6.1, 6.3.1, 6.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* \* 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: Non-Roaming 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.



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

Subscription-based routing to a particular core network deployment as specified in clause 6.44 of TS 22.261 [2] forwards the signalling and user traffic of certain UEs to another target (partner) PLMN that may not be the serving (HPLMN) of the UE, this is achieved by selecting NFs residing in another target PLMN when network functions communicate with each other. The NRF of the serving PLMN, with optional support of the NRF in another target PLMN as sepcified in clause 4.17.4 of TS 23.502 [3], is responsible to provide proper network function instance information during network function discovery and selection.

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(s), DCCF, MFAF and ADRF and their connections with other NFs, 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].

NOTE 6: For clarity, the 5G DDNMF and its connections with other NFs, e.g. UDM, PCF are not depicted in the point-to-point and service-based architecture diagrams. For more information on ProSe architecture refer to TS 23.304 [128].

NOTE 7: For clarity, the TSCTSF and its connections with other NFs, e.g. PCF, NEF, UDR are not depicted in the point-to-point and service-based architecture diagrams. For more information on TSC architecture refer to clause 4.4.8.

NOTE 8: For exposure of the QoS monitoring information as specified in clause 5.8.2.18, exposure of data collected for analytics as specified in clause 5.2.26.2 of TS 23.502 [3], and exposure of the TSC management information as specified in clause 5.8.5.14, direct interaction between UPF and NFs can be supported via the Nupf interface (see clause 4.2.16).

NOTE 9: For clarity, the EASDF and its connections with SMF is not depicted in the point-to-point and service-based architecture diagrams. For more information on edge computing architecture refer to TS 23.548 [130].

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.

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

### 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.

NOTE 3: For clarity, the NWDAF(s) with roaming exchange capability (RE-NWDAF) and their connections with other NFs, are not depicted in the service-based architecture diagram. For more information on network data analytics architecture refer to TS 23.288 [86].

NOTE 4: Depending on the architecture deployed, the Primary or Centralized NSACF at the VPLMN can fetch the maximum number of registered UEs or the maximum number of LBO PDU sessions to be enforced from the HPLMN Primary or Centralized NSACF as described in clause 5.15.11.3.1.

Figure 4.2.4-2: Void

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 4: 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 5: UPFs in the home routed scenario can be used also to support the IPUPS functionality (see clause 5.8.2.14).

NOTE 6: For clarity, the NWDAF(s) with roaming exchange capability (RE-NWDAF) and their connections with other NFs, are not depicted in the service-based architecture diagram. For more information on network data analytics architecture refer to TS 23.288 [86].

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 7: 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 8: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 9: For clarity, the NWDAF(s) with roaming exchange capability (RE-NWDAF) and their connections with other NFs, are not depicted in the reference point architecture figure. For more information on network data analytics architecture refer to TS 23.288 [86].

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

The N38 references point can be between V-SMFs in the same VPLMN, or between V-SMFs in different VPLMNs (to enable inter-PLMN mobility).

NOTE 10: For clarity, the NWDAF(s) with roaming exchange capability (RE-NWDAF) and their connections with other NFs, are not depicted in the reference point architecture figure. For more information on network data analytics architecture refer to TS 23.288 [86].

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

Subscription-based routing to a particular core network deployment as specified in clause 6.44 of TS 22.261 [2] forwards the signalling and user traffic of certain UEs to another target PLMN that may be neither the serving PLMN nor the HPLMN of the UE, this is achieved by selecting NFs residing in another target PLMN when network functions communicate with each other. The NRF of the HPLMN, with optional support of the NRF in another target PLMN as sepcified in clause 4.17.5 of TS 23.502 [3], is responsible to provide proper network function instance information during network function discovery and selection.



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

NOTE 11: For the sake of clarity, SEPPs on both sides of PLMN borders are not depicted in figure 4.2.4-7.

Figure 4.2.4-8: Void

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 12: 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 \* \* \* \*

### 5.6.1 Overview

The 5GC supports a PDU Connectivity Service i.e. a service that provides exchange of PDUs between a UE and a data network identified by a DNN. The PDU Connectivity Service is supported via PDU Sessions that are established upon request from the UE.

The Subscription Information for each S-NSSAI may contain a Subscribed DNN list and one default DNN. When the UE does not provide a DNN in a NAS Message containing PDU Session Establishment Request for a given S-NSSAI, the serving AMF determines the DNN for the requested PDU Session by selecting the default DNN for this S-NSSAI if a default DNN is present in the UE's Subscription Information; otherwise the serving AMF selects a locally configured DNN for this S-NSSAI.

The expectation is that the URSP in the UE is always up to date using the procedure defined in clause 4.16.12.2 of TS 23.502 [3] and therefore the UE requested DNN will be up to date.

In order to cover cases that UE operates using local configuration, but also other cases where operator policies can be used in order to replace an "up to date" UE requested DNN with another DNN used only internally in the network, during UE Registration procedure the PCF may indicate, to the AMF, the operator policies to be used at PDU Session Establishment for DNN replacement of a UE requested DNN. PCF may indicate a policy for DNN replacement of UE requested DNNs not supported by the network, and/or indicate a list of UE requested DNNs per S-NSSAI valid for the serving network, that are subject for replacement (details are described in TS 23.503 [45]).

If the DNN provided by the UE is not supported by the network and AMF cannot select an SMF by querying NRF, the AMF shall reject the NAS Message containing PDU Session Establishment Request from the UE with a cause indicating that the DNN is not supported unless the PCF provided the policy to perform a DNN replacement of unsupported DNNs.

If the DNN requested by the UE is indicated for replacement or the DNN provided by the UE is not supported by the network and the PCF provided the policy to perform DNN replacement of UE requested DNNs not supported by the network, the AMF shall interact with the PCF to perform a DNN replacement. During PDU Session Establishment procedure and as a result of DNN replacement, the PCF provides the selected DNN that is applicable for the S-NSSAI requested by the UE at the PDU Session Establishment. The AMF uses the selected DNN in the query towards the NRF for the SMF selection, as specified in clause 6.3.2, and provides both requested and selected DNN to the selected SMF. For PDU Session with Home-routed Roaming whether to perform DNN replacement is based on operator agreements.

NOTE 1: The selected DNN is determined based on operator preferences and can differ from subscribed DNNs. The matching of selected DNN to S-NSSAI is assumed to be based on network configuration.

Each PDU Session supports a single PDU Session type i.e. supports the exchange of a single type of PDU requested by the UE at the establishment of the PDU Session. The following PDU Session types are defined: IPv4, IPv6, IPv4v6, Ethernet, Unstructured.

PDU Sessions are established (upon UE request), modified (upon UE and 5GC request) and released (upon UE and 5GC request) using NAS SM signalling exchanged over N1 between the UE and the SMF. Upon request from an Application Server, the 5GC is able to trigger a specific application in the UE. When receiving that trigger message, the UE shall pass it to the identified application in the UE. The identified application in the UE may establish a PDU Session to a specific DNN, see clause 4.4.5.

SMF may support PDU Sessions for LADN where the access to a DN is only available in a specific LADN service area. This is further defined in clause 5.6.5.

SMF may support PDU Sessions for a 5G VN group which offers a virtual data network capable of supporting 5G LAN-type service over the 5G system. This is further defined in clause 5.8.2.13.

The SMF is responsible of checking whether the UE requests are compliant with the user subscription. For this purpose, it retrieves and requests to receive update notifications on SMF level subscription data from the UDM. Such data may indicate per DNN and per S-NSSAI of the HPLMN:

- The allowed PDU Session Types and the default PDU Session Type.

- The allowed SSC modes and the default SSC mode.

- QoS Information (refer to clause 5.7): the subscribed Session-AMBR, Default 5QI and Default ARP.

- The IP Index information.

- The static IP address/prefix.

- The subscribed User Plane Security Policy.

- the Charging Characteristics to be associated with the PDU Session. Whether this information is provided by the UDM to a SMF in another PLMN (for PDU Sessions in LBO mode) is defined by operator policies in the UDM/UDR.

NOTE 2: The content of the Charging Characteristics as well as the usage of the Charging Characteristics by the SMF are defined in TS 32.255 [68].

A PDU Session may support:

(a) a single-access PDU Connectivity Service, in which case the PDU Session is associated with a single access type at a given time, i.e. either 3GPP access or non-3GPP access; or

(b) a multi-access PDU Connectivity Service, in which case the PDU Session is simultaneously associated with both 3GPP access and non-3GPP access and simultaneously associated with two independent N3/N9 tunnels between the PSA and RAN/AN.

A PDU Session supporting a single-access PDU Connectivity Service is also referred to as single-access PDU Session, while a PDU Session supporting a multi-access PDU Connectivity Service is referred to as Multi-Access PDU (MA PDU) Session and it is used to support the ATSSS feature (see clause 5.32 for details).

A UE that is registered over multiple accesses chooses over which access to establish a PDU Session. As defined in TS 23.503 [45], the HPLMN may send policies to the UE to guide the UE selection of the access over which to establish a PDU Session.

NOTE 3: In this Release of the specification, at any given time, a PDU Session is routed over only a single access network, unless it is an MA PDU Session in which case it can be routed over one 3GPP access network and one Non 3GPP access network concurrently.

A UE may request to move a single-access PDU Session between 3GPP and Non 3GPP accesses. The decision to move single-access PDU Sessions between 3GPP access and Non 3GPP access is made on a per PDU Session basis, i.e. the UE may, at a given time, have some PDU Sessions using 3GPP access while other PDU Sessions are using Non 3GPP access.

If the UE is attempting to move a single-access PDU session from 3GPP access to non-3GPP access and the PDU session is associated with control plane only indication, then the AMF shall reject the PDU Session Establishment request as related CIoT 5GS optimisation features are not supported over non-3GPP access as described in clause 5.4.5.2.5 of TS 24.501 [47]. If the UE is attempting to move a single-access PDU session from non-3GPP access to NB-N1 mode of 3GPP access, the PDU Session Establishment request would also be rejected by AMF when the UP resources for the UE exceed the maximum number of supported UP resources as described in clause 5.4.5.2.4 of TS 24.501 [47].

In a PDU Session Establishment Request message sent to the network, the UE shall provide a PDU Session ID. The PDU Session ID is unique per UE and is the identifier used to uniquely identify one of a UE's PDU Sessions. The PDU Session ID shall be stored in the UDM to support handover between 3GPP and non-3GPP access when different PLMNs are used for the two accesses. The UE also provides as described in TS 24.501 [47]:

(a) PDU Session Type.

(b) S-NSSAI of the HPLMN that matches the application (that is triggering the PDU Session Request) within the NSSP in the URSP rules or within the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45].

NOTE 4: If the UE cannot determine any S-NSSAI after performing the association of the application to a PDU Session, then it does not indicate any S-NSSAI in the PDU Session Establishment procedure as defined in clause 5.15.5.3.

(c) S-NSSAI of the Serving PLMN from the Allowed NSSAI, corresponding to the S-NSSAI of the HPLMN (b).

NOTE 5: In non-roaming scenario the mapping of the Allowed NSSAI to HPLMN S-NSSAIs is not provided to the UE (because the S-NSSAI of the Serving PLMN (c) has the same value of the S-NSSAI of the HPLMN (b)), therefore the UE provides in the PDU Session Request only the S-NSSAI of the Serving PLMN (c).

NOTE 6: In roaming scenarios the UE provides in the PDU Session Request both the S-NSSAI of the HPLMN (b) and the S-NSSAI of the VPLMN from the Allowed NSSAI (c) that maps to the S-NSSAI of the HPLMN.

(d) DNN (Data Network Name).

(e) SSC mode (Service and Session Continuity mode defined in clause 5.6.9.2).

Additionally, if the UE supports ATSSS and wants to activate a MA PDU Session, the UE shall provide Request Type as "MA PDU Request" and shall indicate the supported ATSSS capabilities (see clause 5.32 for details).

Table 5.6.1-1: Attributes of a PDU Session

|  |  |  |
| --- | --- | --- |
| PDU Session attribute | May be modified later during the lifetime of the PDU Session | Notes |
| S-NSSAI of the HPLMN | No | (Note 1) (Note 2) |
| S-NSSAI of the Serving PLMN | Yes | (Note 1) (Note 2) (Note 4) |
| DNN (Data Network Name) | No | (Note 1) (Note 2) |
| PDU Session Type | No | (Note 1) |
| SSC mode | No | (Note 2)  The semantics of Service and Session Continuity mode is defined in clause 5.6.9.2 |
| PDU Session Id | No |  |
| User Plane Security Enforcement information | No | (Note 3) |
| Multi-access PDU Connectivity Service | No | Indicates if the PDU Session provides multi-access PDU Connectivity Service or not. |
| NOTE 1: If it is not provided by the UE, the network determines the parameter based on default information received in user subscription. Subscription to different DNN(s) and S-NSSAI(s) may correspond to different default SSC modes and different default PDU Session Types  NOTE 2: S-NSSAI(s) and DNN are used by AMF to select the SMF(s) to handle a new session. Refer to clause 6.3.2. The DNN may include both the Network Identifier and the Operator Identifier, see TS 29.502 [36]. See more details of the DNN usage and applicability, e.g. when full DNN or only Network Identifier is applied, in relevant stage 3 specifications.  NOTE 3: User Plane Security Enforcement information is defined in clause 5.10.3.  NOTE 4: The S-NSSAI value of the Serving PLMN associated to a PDU Session can change whenever the UE moves to a different PLMN, while keeping that PDU Session. | | |

Subscription Information may include a wildcard DNN per subscribed S-NSSAI: when a wildcard DNN is associated with a subscribed S-NSSAI, the subscription allows, for this S-NSSAI, the UE to establish a PDU Session using any DNN value.

NOTE 7: The SMF is made aware whether the DNN of a PDU Session being established corresponds to an explicitly subscribed DNN or corresponds to a wildcard DNN. Thus, the SMF can reject a PDU Session establishment if the DNN of the PDU Session is not part of explicitly subscribed DNN(s) and local policies in the SMF require UE to have a subscription to this DNN.

A UE may establish multiple PDU Sessions, to the same data network or to different data networks, via 3GPP and via and Non-3GPP access networks at the same time.

A UE may establish multiple PDU Sessions to the same Data Network and served by different UPF terminating N6.

A UE with multiple established PDU Sessions may be served by different SMF.

The SMF shall be registered and deregistered on a per PDU Session granularity in the UDM.

The user plane paths of different PDU Sessions (to the same or to different DNN) belonging to the same UE may be completely disjoint between the AN and the UPF interfacing with the DN.

When the SMF cannot control the UPF terminating the N3 interface used by a PDU Session and SSC mode 2/3 procedures are not applied to the PDU Session, an I-SMF is inserted between the SMF and the AMF and handling of PDU Session(s) is described in clause 5.34.

NOTE 8: User Plane resources for PDU Sessions of a UE, except for regulatory prioritized service like Emergency Services and MPS, can be deactivated by the SMF if the UE is only reachable for regulatory prioritized services.

The SMF serving a PDU session (i.e. Anchor) can be changed during lifetime of the PDU session either within the same SMF set or, if the Context Transfer Procedures as specified in clause 4.26 of TS 23.502 [3] are supported, between SMFs in different SMF sets.

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

#### 6.2.6.1 General

The Network Repository Function (NRF) supports the following functionality:

- Supports service discovery of NRF services and their endpoint addresses by the NRF bootstrapping service.

- Supports service discovery function. Receive NF Discovery Request from NF instance or SCP, and provides the information of the discovered NF instances (be discovered) to the NF instance or SCP, including the scenario of NF instances residing in a target PLMN that the serving PLMN can use for certain UEs as specified by clause 6.44 of TS 22.261 [2].

- Supports P-CSCF discovery (specialized case of AF discovery by SMF).

- Maintains the NF profile of available NF instances and their supported services.

- Maintains SCP profile of available SCP instances.

- Supports SCP discovery by SCP instances.

- Notifies about newly registered/updated/ deregistered NF and SCP instances along with its potential NF services to the subscribed NF service consumer or SCP.

- Maintains the health status of NFs and SCP.

In the context of Network Slicing, based on network implementation, multiple NRFs can be deployed at different levels (see clause 5.15.5):

- PLMN level (the NRF is configured with information for the whole PLMN),

- shared-slice level (the NRF is configured with information belonging to a set of Network Slices),

- slice-specific level (the NRF is configured with information belonging to an S-NSSAI).

In the context of roaming, multiple NRFs may be deployed in the different networks (see clause 4.2.4):

- the NRF(s) in the Visited PLMN (known as the vNRF) configured with information for the visited PLMN.

- the NRF(s) in the Home PLMN (known as the hNRF) configured with information for the home PLMN and optionally target PLMN(s) which includes NF instances that HPLMN can use for certain UEs as specified by clause 6.44 of TS 22.261 [2], referenced by the vNRF via the N27 interface. The hNRF may also query a NRF in another target PLMN as specified in clause 4.17.5 of TS 23.502 [3].

NOTE : The NRF in HPLMN interacts with NRF in target PLMN for certain UEs based on SUPI, Routing Indicator if these parameters are included in the query.

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

### 6.3.1 General

The NF discovery and NF service discovery enable Core Network entities (NFs or Service Communication Proxy (SCP)) to discover a set of NF instance(s) and NF service instance(s) for a specific NF service or an NF type. NF service discovery is enabled via the NF discovery procedure, as specified in clauses 4.17.4, 4.17.5, 4.17.9 and 4.17.10 of TS 23.502 [3].

Unless the expected NF and NF service information is locally configured on the requester NF, e.g. when the expected NF service or NF is in the same PLMN as the requester NF, the NF and NF service discovery is implemented via the Network Repository Function (NRF). NRF is the logical function that is used to support the functionality of NF and NF service discovery and status notification as specified in clause 6.2.6.

NOTE 1: NRF can be colocated together with SCP e.g. for communication option D, depicted in Annex E.

In order for the requested NF type or NF service to be discovered via the NRF, the NF instance need to be registered in the NRF. This is done by sending a Nnrf\_NFManagement\_NFRegister containing the NF profile. The NF profile contains information related to the NF instance, such as NF instance ID, supported NF service instances (see clause 6.2.6 for more details regarding the NF profile). The registration may take place e.g. when the producer NF instance and its NF service instance(s) become operative for the first time. The NF service registration procedure is specified in clause 4.17.1 of TS 23.502 [3].

In order for the requester NF or SCP to obtain information about the NF and/or NF service(s) registered or configured in a PLMN/slice, based on local configuration the requester NF or SCP may initiate a discovery procedure with the NRF by providing the type of the NF and optionally a list of the specific service(s) it is attempting to discover. The requester NF or SCP may also provide other service parameters e.g. slicing related information. For the detailed service parameter(s) used for specific NF and NF service discovery refer to clause 5.2.7.3.2 of TS 23.502 [3]. The requester NF may also provide NF Set related information to enable reselection of NF instances within the NF set. The requester NF may also provide the required supported features of the NF.

For some Network Functions which have access to the subscription data (e.g. HSS, UDM) the NRF may need to resolve the NF Group ID corresponding to a subscriber identifier. If the NRF has no stored configuration mapping identity sets/ranges to NF Group ID locally, the NRF may retrieve the NF Group ID corresponding to a specific subscriber identifier from the UDR using the Nudr\_GroupIDmap\_Query service operation.

In the case of Indirect Communication, a NF Service Consumer employs an SCP which routes the request to the intended target of the request.

If the requester NF is configured to delegate discovery, the requester NF may omit the discovery procedure with the NRF and instead delegate the discovery to the SCP; the SCP will then act on behalf of the requester NF. In this case, the requester NF adds any necessary discovery and selection parameters to the request in order for the SCP to be able to do discovery and associated selection. The SCP may interact with the NRF to perform discovery and obtain discovery result and it may interact with the NRF or UDR to obtain NF Group ID corresponding to subscriber identifier.

NOTE 2: For delegated discovery of the HSS or the UDM, the SCP can rely on the NRF to discover the group of HSS/UDM instance(s) serving the provided user identity, or in some deployments the SCP can first query the UDR for the HSS/UDM Group ID for the provided user identity. It is expected that the stage 3 defines a single encoding for the user identity provided by the service consumer that can be used for both variants of delegated discovery to avoid that the service consumer needs to be aware of the SCP behaviour.

The NRF provides a list of NF instances and NF service instances relevant for the discovery criteria. The NRF may provide the IP address or the FQDN of NF instance(s) and/or the Endpoint Address(es) of relevant NF service instance(s) to the NF Consumer or SCP. The NRF may also provide NF Set ID and/or NF Service Set ID to the NF Consumer or SCP. The response contains a validity period during which the discovery result is considered valid and can be cached. The result of the NF and NF service discovery procedure is applicable to any subscriber that fulfils the same discovery criteria. The entity that does the discovery may cache the NF profile(s) received from the NF/NF service discovery procedure. During the validity period, the cached NF profile(s) may be used for NF selection for any subscriber matching the discovery criteria.

NOTE 3: Refer to TS 29.510 [58] for details on using the validity period.

In the case of Direct Communication, the requester NF uses the discovery result to select NF instance and a NF service instance that is able to provide a requested NF Service (e.g. a service instance of the PCF that can provide Policy Authorization).

In the case of Indirect Communication without Delegated Discovery, the requester NF uses the discovery result to select a NF instance while the associated NF service instance selection may be done by the requester NF and/or an SCP on behalf of the requester NF.

In both the cases above, the requester NF may use the information from a valid cached discovery result for subsequent selections (i.e. the requester NF does not need to trigger a new NF discovery procedure to perform the selection).

In the case of Indirect Communication with Delegated Discovery, the SCP will discover and select a suitable NF instance and NF service instance based on discovery and selection parameters provided by the requester NF and optional interaction with the NRF. The NRF to be used may be provided by the NF consumer as part of the discovery parameters, e.g. as a result of a NSSF query. The SCP may use the information from a valid cached discovery result for subsequent selections (i.e. the SCP does not need to trigger a new NF discovery procedure to perform the selection).

NOTE 4: In a given PLMN, Direct Communication, Indirect Communication, or both may apply.

The requester NF or SCP may subscribe to receive notifications from the NRF of a newly updated NF profile of an NF (e.g. NF service instances taken in or out of service), or newly registered de-registered NF instances. The NF/NF service status subscribe/notify procedure is defined in clauses 4.17.7 and 4.17.8 of TS 23.502 [3].

For NF and NF service discovery across PLMNs, the NRF in the local PLMN interacts with the NRF in the remote PLMN to retrieve the NF profile(s) of the NF instance(s) in the remote PLMN that matches the discovery criteria. The NRF in the local PLMN reaches the NRF in the remote PLMN by forming a target PLMN specific query using the PLMN ID provided by the requester NF. The remote PLMN NRF (i.e. HPLMN NRF) may further interact with the target PLMN NRF as specified in clause 6.2.6.1. The NF/NF service discovery procedure across PLMNs is specified in clause 4.17.5 of TS 23.502 [3].

NOTE 5: See TS 29.510 [58] for details on using the target PLMN ID specific query to reach the NRF in the remote PLMN.

For topology hiding, see clause 6.2.17.

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

### 6.3.2 SMF discovery and selection

The SMF selection functionality is supported by the AMF and SCP and is used to allocate an SMF that shall manage the PDU Session. The SMF selection procedures are described in clause 4.3.2.2.3 of TS 23.502 [3].

The SMF discovery and selection functionality follows the principles stated in clause 6.3.1.

If the AMF does discovery, the AMF shall utilize the NRF to discover SMF instance(s) unless SMF information is available by other means, e.g. locally configured on AMF. The AMF provides UE location information to the NRF when trying to discover SMF instance(s). The NRF provides NF profile(s) of SMF instance(s) to the AMF. In addition, the NRF also provides the SMF service area of SMF instance(s) to the AMF. The SMF selection functionality in the AMF selects an SMF instance and an SMF service instance based on the available SMF instances obtained from NRF or on the configured SMF information in the AMF.

NOTE 1: Protocol aspects of the access to NRF are specified in TS 29.510 [58].

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

The SMF selection for Emergency services is described in clause 5.16.4.5.

The following factors may be considered during the SMF selection:

a) Selected Data Network Name (DNN). The formulation of the DNN considers the information provided in f) below. In the case of the home routed roaming, the DNN is not applied for the V-SMF selection.

b) S-NSSAI of the HPLMN (for non-roaming and home-routed roaming scenarios), and S-NSSAI of the VPLMN (for roaming with local breakout and home-routed roaming scenarios).

c) NSI-ID.

NOTE 2: The use of NSI -ID in the network is optional and depends on the deployment choices of the operator. If used, the NSI ID is associated with S-NSSAI.

d) Access technology being used by the UE.

e) Support for Control Plane CIoT 5GS Optimisation.

f) Subscription information from UDM, e.g.

- per DNN: whether LBO roaming is allowed.

- per DNN: whether HR-SBO roaming is allowed.

- per S-NSSAI: the subscribed DNN(s).

- per (S-NSSAI, subscribed DNN): whether LBO roaming is allowed.

- per (S-NSSAI, subscribed DNN): whether HR-SBO roaming is allowed.

- per (S-NSSAI, subscribed DNN): whether EPC interworking is supported.

- per (S-NSSAI, subscribed DNN): whether selecting the same SMF for all PDU sessions to the same S-NSSAI and DNN is required.

- per (S-NSSAI, DNN) associated with 5G VN group: Service Area (LADN service area) for the 5G VN group. In the case of SMF selection for a PDU Session targeting 5G VN group, the AMF may prefer candidate SMF(s) that have an intersection with the LADN service area of the 5G VN group.

- per (S-NSSAI, subscribed DNN): Additional Parameters for SMF selection in target PLMN as defined in TS 23.502 [3] and may include the target network identifier (i.e. PLMN ID preferred by the operator), locality and optionally with spatial validity condition and time validity information.

NOTE 2: When AMF formulates the NRF query for SMF selection, the target network identifier (i.e. PLMN ID) in subscription data can be used as the Operator Identifier of the DNN parameter and/or as part of the target PLMN list (see more details in TS 29.510 [58]).

g) Void.

h) Local operator policies.

NOTE 3: These policies can take into account whether the SMF to be selected is an I-SMF or a V-SMF or a SMF.

i) Load conditions of the candidate SMFs.

j) Analytics (i.e. statistics or predictions) for candidate SMFs' load as received from NWDAF (see TS 23.288 [86]), if NWDAF is deployed.

k) UE location (i.e. TA).

l) Service Area of the candidate SMFs. In case of SMF seletion in another target PLMN, the formulation of the target PLMN considers the information provided in f) above.

m) Capability of the SMF to support a MA PDU Session.

n) If interworking with EPS is required.

o) Preference of V-SMF support. This is applicable only for V-SMF selection in the case of home routed roaming.

p) Target DNAI.

q) Capability of the SMF to support User Plane Remote Provisioning (see clause 5.30.2.10.4.3).

r) Supported DNAI list.

s) HR-SBO support (according to clause 6.7 of TS 23.548 [130]).

t) Capability of the SMF (V-SMF and H-SMF) to support non-3GPP access path switching.

To support the allocation of a static IPv4 address and/or a static IPv6 prefix as specified in clause 5.8.2.2.1, a dedicated SMF may be deployed for the indicated combination of DNN and S-NSSAI and registered to the NRF, or provided by the UDM as part of the subscription data.

In the case of delegated discovery, the AMF, shall send all the available factors a)-d), k) and n) to the SCP.

In addition, the AMF may indicate to the SCP which NRF to use (in the case of NRF dedicated to the target slice).

If there is an existing PDU Session and the UE requests to establish another PDU Session to the same DNN and S-NSSAI of the HPLMN, and the UE subscription data indicates the support for interworking with EPS for this DNN and S-NSSAI of the HPLMN or UE subscription data indicates the same SMF shall be selected for all PDU sessions to the same S-NSSAI, DNN, the same SMF in non roaming and LBO case or the same H-SMF in home routed roaming case, shall be selected. In addition, if the UE Context in the AMF provides a SMF ID for an existing PDU session to the same DNN, S-NSSAI, the AMF uses the stored SMF ID for the additional PDU Session. In any such a case where the AMF can determine which SMF should be selected, if delegated discovery is used, the AMF shall indicate a desired NF Instance ID so that the SCP is able to route the message to the relevant SMF. Otherwise, if UE subscription data does not indicate the support for interworking with EPS for this DNN and S-NSSAI, a different SMF in non roaming and LBO case or a different H-SMF in home routed roaming case, may be selected. For example, to support a SMF load balancing or to support a graceful SMF shutdown (e.g. a SMF starts to no more take new PDU Sessions).

In the home-routed roaming case, the SMF selection functionality selects an SMF in VPLMN based on the S-NSSAI of the VPLMN, as well as an SMF in HPLMN based on the S-NSSAI of the HPLMN. This is specified in clause 4.3.2.2.3.3 of TS 23.502 [3].

If the HR-SBO roaming is allowed for the PDU Session, the DNN is also considered for V-SMF selection.

When the UE requests to establish a PDU Session to a DNN and an S-NSSAI of the HPLMN, if the UE MM Core Network Capability indicates the UE supports EPC NAS and optionally, if the UE subscription indicates the support for interworking with EPS for this DNN and S-NSSAI of the HPLMN, the selection functionality (in AMF or SCP) selects a combined SMF+PGW-C. Otherwise, a standalone SMF may be selected.

If the UDM provides a subscription context that allows for handling the PDU Session in the VPLMN (i.e. using LBO) for this DNN and S-NSSAI of the HPLMN and, optionally, the AMF is configured to know that the VPLMN has a suitable roaming agreement with the HPLMN of the UE, the following applies:

- If the AMF does discovery, the SMF selection functionality in AMF selects an SMF from the VPLMN.

- If delegated discovery is used, the SCP selects an SMF from the VPLMN.

If an SMF in the VPLMN cannot be derived for the DNN and S-NSSAI of the VPLMN, or if the subscription does not allow for handling the PDU Session in the VPLMN using LBO, then the following applies:

- If the AMF does discovery, both an SMF in VPLMN and an SMF in HPLMN are selected, and the DNN and S-NSSAI of the HPLMN is used to derive an SMF identifier from the HPLMN.

- If delegated discovery is used:

- The AMF performs discovery and selection of H-SMF from NRF. The AMF may indicate the maximum number of H-SMF instances to be returned from NRF, i.e. SMF selection at NRF.

- The AMF sends Nsmf\_PDUSession\_CreateSMContext Request to SCP, which includes the endpoint (e.g. URI) of the selected H-SMF, and the discovery and selection parameters as defined in this clause, i.e. parameter for V-SMF selection. The SCP performs discovery and selection of the V-SMF and forwards the request to the selected V-SMF.

- The V-SMF sends the Nsmf\_PDUSession\_Create Request towards the H-SMF via the SCP; the V-SMF uses the received endpoint (e.g. URI) of the selected H-SMF to construct the target destination to be addressed. The SCP forwards the request to the H-SMF.

- Upon reception of a response from V-SMF, based on the received V-SMF ID the AMF obtains the Service Area of the V-SMF from NRF. The AMF uses the Service Area of the V-SMF to determine the need for V-SMF relocation upon subsequent UE mobility.

If the initially selected SMF in VPLMN (for roaming with LBO) detects it does not understand information in the UE request, it may reject the N11 message (related with a PDU Session Establishment Request message) with a proper N11 cause triggering the AMF to select both a new SMF in the VPLMN and a SMF in the HPLMN (for home routed roaming).

The AMF selects SMF(s) considering support for CIoT 5GS optimisations (e.g. Control Plane CIoT 5GS Optimisation).

In the case of onboarding of UEs for SNPNs, when the UE is registered for SNPN onboarding the AMF selects SMF(s) of Onboarding Network considering the Capability of SMF to support User Plane Remote Provisioning.

Additional details of AMF selection of an I-SMF are described in clause 5.34.

In the case of home routed scenario, the AMF selects a new V-SMF if it determines that the current V-SMF cannot serve the UE location. The selection/relocation is same as an I-SMF selection/relocation as described in clause 5.34.

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