**SA WG2 Meeting #S2-143E  *S2-200xxxx***

**24 February – 9 March, 2021, Elbonia**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** |  | **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 |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | KI #1-1, I-SMF selection |
|  |  |
| ***Source to WG:*** | CATT, ZTE, Nokia?, Huawei? |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** |  eEDGE\_5GC  |  | ***Date:*** | 2021-02-24 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Per TR 23.748 clause 9.3, it is concluded to support SMF sending the target DNAI(s) to the AMF to assistant the I-SMF selection. |
|  |  |
| ***Summary of change:*** | SMF sending the target DNAI(s) to the AMF to assistant the I-SMF selection. |
|  |  |
| ***Consequences if not approved:*** |  5.6.7.1, 5.34.1, 5.34.3, 6.2.6.2, 6.3.2 |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **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:*** |  |

\* \* \* \* 1st change \* \* \* \*

#### 5.6.7.1 General

The content of this clause applies to non-roaming and to LBO deployments i.e. to cases where the involved entities (AF, PCF, SMF, UPF) belong to the Serving PLMN or AF belongs to a third party with which the Serving PLMN has an agreement. AF influence on traffic routing does not apply in the case of Home Routed deployments. PCF shall not apply AF requests to influence traffic routing to PDU Sessions established in Home Routed mode.

An AF may send requests to influence SMF routeing decisions for traffic of PDU Session. The AF requests may influence UPF (re)selection and (I-)SMF (re)selection and allow routeing user traffic to a local access to a Data Network (identified by a DNAI).

The AF may issue requests on behalf of applications not owned by the PLMN serving the UE.

If the operator does not allow an AF to access the network directly, the AF shall use the NEF to interact with the 5GC, as described in clause 6.2.10.

The AF may be in charge of the (re)selection or relocation of the applications within the local DN. Such functionality is not defined. For this purpose, the AF may request to get notified about events related with PDU Sessions.

The AF requests are sent to the PCF via N5 (in the case of requests targeting specific on-going PDU Sessions of individual UE(s), for an AF allowed to interact directly with the 5GC NFs) or via the NEF. The AF requests that target existing or future PDU Sessions of multiple UE(s) or of any UE are sent via the NEF and may target multiple PCF(s), as described in clause 6.3.7.2. The PCF(s) transform(s) the AF requests into policies that apply to PDU Sessions. When the AF has subscribed to UP path management event notifications from SMF(s) (including notifications on how to reach a GPSI over N6), such notifications are sent either directly to the AF or via an NEF (without involving the PCF). For AF interacting with PCF directly or via NEF, the AF requests may contain the information as described in the Table 5.6.7-1:

Table 5.6.7-1: Information element contained in AF request

|  |  |  |  |
| --- | --- | --- | --- |
| Information Name | Applicable for PCF or NEF (NOTE 1) | Applicable for NEF only | Category |
| Traffic Description | Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.  | The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.  | Mandatory |
| Potential Locations of Applications | Indicates potential locations of applications, represented by a list of DNAI(s). | The potential locations of applications can be represented by AF-Service-Identifier. | Conditional(NOTE 2) |
| Target UE Identifier(s) | Indicates the UE(s) that the request is targeting, i.e. an individual UE, a group of UE represented by Internal Group Identifier (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s). | GPSI can be applied to identify the individual UE, or External Group Identifier can be applied to identify a group of UE. | Mandatory |
| Spatial Validity Condition | Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity. | The specified location can be represented by a list of geographic zone identifier(s).  | Optional |
| AF transaction identifier | The AF transaction identifier refers to the AF request. | N/A | Mandatory |
| N6 Traffic Routing requirements | Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation. | N/A | Optional(NOTE 2) |
| Application Relocation Possibility | Indicates whether an application can be relocated once a location of the application is selected by the 5GC. | N/A | Optional |
| UE IP address preservation indication | Indicates UE IP address should be preserved. | N/A | Optional |
| Temporal Validity Condition | Time interval(s) or duration(s). | N/A | Optional |
| Information on AF subscription to corresponding SMF events | Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription. | N/A | Optional |
| NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR.NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only.NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. |

For each information element mentioned above in the AF request, the detailed description is as follows:

1) Information to identify the traffic. The traffic can be identified in the AF request by

- Either a DNN and possibly slicing information (S-NSSAI) or an AF-Service-Identifier

- When the AF provides an AF-Service-Identifier i.e. an identifier of the service on behalf of which the AF is issuing the request, the 5G Core maps this identifier into a target DNN and slicing information (S-NSSAI)

- When the NEF processes the AF request the AF-Service-Identifier may be used to authorize the AF request.

- An application identifier or traffic filtering information (e.g. 5 Tuple). The application identifier refers to an application handling UP traffic and is used by the UPF to detect the traffic of the application

 When the AF request is for influencing SMF routing decisions, the information is to identify the traffic to be routed.

 When the AF request is for subscription to notifications about UP path management events, the information is to identify the traffic that the events relate to.

2) Information about the N6 traffic routing requirements for traffic identified as defined in 1). This includes:

- Information about the N6 traffic routing requirements that is provided per DNAI: for each DNAI, the N6 traffic routing requirements may contain a routing profile ID and/or N6 traffic routing information.

- An optional indication of traffic correlation, when the information in 4) identifies a group of UEs. This implies the targeted PDU Sessions should be correlated by a common DNAI in the user plane for the traffic identified in 1). If this indication is provided by the AF, the 5GC should select a common DNAI for the target PDU Sessions from the list of DNAI(s) specified in 3).

NOTE 1: The N6 traffic routing requirements are related to the mechanism enabling traffic steering in the local access to the DN. The routing profile ID refers to a pre-agreed policy between the AF and the 5GC. This policy may refer to different steering policy ID(s) sent to SMF and e.g. based on time of the day etc.

NOTE 2: The mechanisms enabling traffic steering in the local access to the DN are not defined.

3) Potential locations of applications towards which the traffic routing should apply. The potential location of application is expressed as a list of DNAI(s). If the AF interacts with the PCF via the NEF, the NEF may map the AF-Service-Identifier information to a list of DNAI(s). The DNAI(s) may be used for UPF (re)selection and (I-)SMF (re)selection.

4) Information on the UE(s). This may correspond to:

- Individual UEs identified using GPSI, or an IP address/Prefix or a MAC address.

- Groups of UEs identified by an External Group Identifier as defined in TS 23.682 [36] when the AF interacts via the NEF, or Internal-Group Identifier (see clause 5.9.7) when the AF interacts directly with the PCF.

- Any UE accessing the combination of DNN, S-NSSAI and DNAI(s).

 When the PDU Session type is IPv4 or IPv6 or IPv4v6, and the AF provides an IP address and/or an IP Prefix, or when the PDU Session type is Ethernet and the AF provides a MAC address, this allows the PCF to identify the PDU Session for which this request applies and the AF request applies only to that specific PDU Session of the UE. In this case, additional information such as the UE identity may also be provided to help the PCF to identify the correct PDU Session.

 Otherwise the request targets multiple UE(s) and shall apply to any existing or future PDU Sessions that match the parameters in the AF request.

 When the AF request targets an individual UE and GPSI is provided within the AF request, the GPSI is mapped to SUPI according to the subscription information received from UDM.

 When the AF request targets any UE or a group of UE, the AF request is likely to influence multiple PDU Sessions possibly served by multiple SMFs and PCFs.

 When the AF request targets a group of UE it provides one or several group identifiers in its request. The group identifiers provided by the AF are mapped to Internal-Group identifiers. Members of the group have this Group Identifier in their subscription. The Internal-Group Identifier is stored in UDM, retrieved by SMF from UDM and passed by SMF to PCF at PDU Session set-up. The PCF can then map the AF requests with user subscription and determine whether an AF request targeting a Group of users applies to a PDU Session.

 When the AF request is for influencing SMF routing decisions, the information is to identify UE(s) whose traffic is to be routed.

 When the AF request is for subscription to notifications about UP path management events, the information is to identify UE(s) whose traffic the events relate to.

 When the AF request is for traffic forwarding in a PDU Session serving for TSC, the MAC address used by the PDU Session is determined by the AF to identify UE whose traffic is to be routed according to the previously stored binding relationship of the 5GS Bridge and the port number of the traffic forwarding information received from TSN network.

5) Indication of application relocation possibility. This indicates whether an application can be relocated once a location of the application is selected by the 5GC. If application relocation is not possible, the 5GC shall ensure that for the traffic related with an application, no DNAI change takes place once selected for this application.

6) Temporal validity condition. This is provided in the form of time interval(s) or duration(s) during which the AF request is to be applied.

 When the AF request is for influencing SMF routing decisions, the temporal validity condition indicates when the traffic routing is to apply.

 When the AF request is for subscription to notifications about UP path management events, the temporal validity condition indicates when the notifications are to be generated.

7) Spatial validity condition on the UE(s) location. This is provided in the form of validity area(s). If the AF interacts with the PCF via the NEF, it may provide a list of geographic zone identifier(s) and the NEF maps the information to areas of validity based on pre-configuration. The PCF in turn determines area(s) of interest based on validity area(s).

 When the AF request is for influencing SMF routing decisions, the spatial validity condition indicates that the request applies only to the traffic of UE(s) located in the specified location.

 When the AF request is for subscription to notifications about UP path management events, the spatial validity condition indicates that the subscription applies only to the traffic of UE(s) located in the specified location.

8) Information on AF subscription to corresponding SMF events.

 The AF may request to be subscribed to change of UP path associated with traffic identified in the bullet 1) above. The AF request contains:

- A type of subscription (subscription for Early and/or Late notifications).

 The AF subscription can be for Early notifications and/or Late notifications. In the case of a subscription for Early notifications, the SMF sends the notifications before the (new) UP path is configured. In the case of a subscription for Late notifications, the SMF sends the notification after the (new) UP path has been configured.

- Optionally, an indication of "AF acknowledgment to be expected".

 The indication implies that the AF will provide a response to the notifications of UP path management events to the 5GC. The SMF may, according to this indication, determine to wait for a response from the AF before the SMF configures in the case of early notification, or activates in the case of late notification, the new UP path as described in clause 5.6.7.2.

 The AF subscription can also request to receive information associating the GPSI of the UE with the IP address(es) of the UE and/or with actual N6 traffic routing to be used to reach the UE on the PDU Session; in this case the corresponding information is sent by the SMF regardless of whether a DNAI applies to the PDU Session.

9) An AF transaction identifier referring to the AF request. This allows the AF to update or remove the AF request and to identify corresponding UP path management event notifications. The AF transaction identifier is generated by the AF.

 When the AF interacts with the PCF via the NEF, the NEF maps the AF transaction identifier to an AF transaction internal identifier, which is generated by the NEF and used within the 5GC to identify the information associated to the AF request. The NEF maintains the mapping between the AF transaction identifier and the AF transaction internal identifier. The relation between the two identifiers is implementation specific.

 When the AF interacts with the PCF directly, the AF transaction identifier provided by the AF is used as AF transaction internal identifier within the 5GC.

10) Indication of UE IP address preservation. This indicates UE IP address related to the traffic identified in bullet 1) should be preserved. If this indication is provided by the AF, the 5GC should preserve the UE IP address by preventing reselection of PSA UPF for the identified traffic once the PSA UPF is selected.

An AF may send requests to influence SMF routeing decisions, for event subscription or for both.

The AF may request to be subscribed to notifications about UP path management events, i.e. a UP path change occurs for the PDU Session. The corresponding notification about a UP path change sent by the SMF to the AF may indicate the DNAI and /or the N6 traffic routing information that has changed as described in clause 4.3.6.3 of TS 23.502 [3]. It may include the AF transaction internal identifier, the type of notification (i.e. early notification or late notification), the Identity of the source and/or target DNAI, the IP address/prefix of the UE or the MAC address used by the UE, the GPSI and the N6 traffic routing information related to the 5GC UP.

NOTE 3: The change from the UP path status where no DNAI applies to a status where a DNAI applies indicates the activation of this AF request; the change from the UP path status where a DNAI applies to a status where no DNAI applies indicates the de-activation of this AF request.

 In the case of IP PDU Session Type, the IP address/prefix of the UE together with N6 traffic routing information indicates to the AF how to reach over the User Plane the UE identified by its GPSI. N6 traffic routing information indicates any tunnelling that may be used over N6. The nature of this information depends on the deployment.

NOTE 4: N6 traffic routing information can e.g. correspond to the identifier of a VPN or to explicit tunnelling information such as a tunnelling protocol identifier together with a Tunnel identifier.

NOTE 5: In the case of Unstructured PDU Session type the nature of the N6 traffic routing information related to the 5GC UP is described in clause 5.6.10.3.

 In the case of Ethernet PDU Session Type, the MAC address of the UE together with N6 traffic routing information indicates to the AF how to reach over the User Plane the UE identified by its GPSI. The UE MAC address (es) is reported by the UPF as described in clause 5.8.2.12. The N6 traffic routing information can be, e.g. a VLAN ID or the identifier of a VPN or a tunnel identifier at the UPF.

 In the case of PDU Session serving for TSC, the SMF informs AF of the 5GS Bridge user plane information as defined in clause 5.28.1, as well as the association between the MAC address used by the PDU Session, 5GS Bridge ID and DS-TT port number.

When notifications about UP path management events are sent to the AF via the NEF, if required, the NEF maps the UE identify information, e.g. SUPI, to the GPSI and the AF transaction internal identifier to the AF transaction identifier before sending the notifications to the AF.

The PCF authorizes the request received from the AF based on information received from the AF, operator's policy, etc. and determines for each DNAI, a traffic steering policy ID (derived from the routing profile ID provided by the AF) and/or the N6 traffic routing information (as provided by the AF) to be sent to the SMF as part of the PCC rules. The traffic steering policy IDs are configured in the SMF or in the UPF. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN.

The DNAIs are related to the information considered by the SMF for UPF selection and (I-)SMF (re)selection, e.g. for diverting (locally) some traffic matching traffic filters provided by the PCF.

The PCF acknowledges a request targeting an individual PDU Session to the AF or to the NEF.

For PDU Session that corresponds to the AF request, the PCF provides the SMF with a PCC rule that is generated based on the AF request, Local routing indication from the PDU Session policy control subscription information and taking into account UE location presence in area of interest (i.e. Presence Reporting Area). The PCC rule contains the information to identify the traffic, information about the DNAI(s) towards which the traffic routing should apply and optionally, an indication of traffic correlation and/or an indication of application relocation possibility and/or indication of UE IP address preservation. The PCC rule also contains per DNAI a traffic steering policy ID and/or N6 traffic routing information, if the N6 traffic routing information is explicitly provided in the AF request. The PCF may also provide in the PCC rule information to subscribe the AF (or the NEF) to SMF events (UP path changes) corresponding to the AF request in which case it provides the information on AF subscription to corresponding SMF events received in the AF request. This is done by providing policies at PDU Session set-up or by initiating a PDU Session Modification procedure. When initiating a PDU Session set-up or PDU Session Modification procedure, the PCF considers the latest known UE location to determine the PCC rules provided to the SMF. The PCF evaluates the temporal validity condition of the AF request and informs the SMF to activate or deactivate the corresponding PCC rules according to the evaluation result. When policies specific to the PDU Session and policies general to multiple PDU Sessions exist, the PCF gives precedence to the PDU Session specific policies over the general policies.

The spatial validity condition is resolved at the PCF. In order to do that, the PCF subscribes to the SMF to receive notifications about change of UE location in an area of interest (i.e. Presence Reporting Area). The subscribed area of interest may be the same as spatial validity condition, or may be a subset of the spatial validity condition (e.g. a list of TAs) based on the latest known UE location. When the SMF detects that UE entered the area of interest subscribed by the PCF, the SMF notifies the PCF and the PCF provides to the SMF the PCC rules described above by triggering a PDU Session Modification. When the SMF becomes aware that the UE left the area subscribed by the PCF, the SMF notifies the PCF and the PCF provides updated PCC rules by triggering a PDU Session Modification. SMF notifications to the PCF about UE location in or out of the subscribed area of interest are triggered by UE location change notifications received from the AMF or by UE location information received during a Service Request or Handover procedure.

When the PCC rules are activated, the SMF may, based on local policies, take the information in the PCC rules into account to:

- (re)select UP paths (including DNAI(s)) for PDU Sessions. The SMF is responsible for handling the mapping between the UE location (TAI / Cell-Id) and DNAI(s) associated with UPF and applications and the selection of the UPF(s) that serve a PDU Session. This is described in clause 6.3.3. If the PDU Session is of IP type and if Indication of UE IP address preservation is included in the PCC rules, the SMF should preserve the UE IP address, by not reselecting the related PSA UPF once the PSA UPF is selected, for the traffic identified in the PCC rule. If the PCC rules are related to a 5G VN group served by the SMF and if the Information about the N6 traffic routing requirements includes an indication of traffic correlation, the SMF should select a common DNAI for the PDU Sessions of the 5G VN group.

- configure traffic steering at UPF, including activating mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL). Such mechanisms are defined in clause 5.6.4. This may include that the SMF is providing the UPF with packet handling instructions (i.e. PDRs and FARs) for steering traffic to the local access to the DN. The packet handling instructions are generated by the SMF using the traffic steering policy ID and/or the N6 traffic routing information in the PCC rules corresponding to the applied DNAI. In the case of UP path reselection, the SMF may configure the source UPF to forward traffic to the UL CL/BP so that the traffic is steered towards the target UPF.

- if Information on AF subscription to corresponding SMF events has been provided in the PCC rule, inform the AF of the (re)selection of the UP path (UP path change). If the information includes an indication of "AF acknowledgment to be expected", the SMF may decide to wait for a response from the AF before it activates the new UP path, as described in clause 5.6.7.2.

When an I-SMF is inserted for a PDU Session, the I-SMF insertion, relocation or removal to a PDU session shall be transparent (i.e. not aware) to the PCF and to the AF. The processing of the AF influence on traffic routing is described in clause 5.34 and detail procedure is described in clause 4.23.6 of TS 23.502 [3].

\* \* \* \* End of 1st change \* \* \* \*

\* \* \* \* 2nd change \* \* \* \*

### 5.34.1 General

When the UE is outside of the SMF Service Area, or current SMF cannot serve the target DNAI(s) for the traffic routing towards Local DN, an I-SMF is inserted between the SMF and the AMF. The I-SMF has a N11 interface with the AMF and a N16a interface with the SMF and is responsible of controlling the UPF(s) that the SMF cannot directly control. The exchange of the SM context and forwarding of tunnel information if needed are done between two SMFs directly without involvement of AMF.

Depending on scenario, a PDU Session in non-roaming case or local breakout is either served by a single SMF or served by an SMF and an I-SMF. When a PDU Session is served by both an SMF and an I-SMF, the SMF is the NF instance that has the interfaces towards the PCF and CHF.

In this Release of the specification, deployments topologies with specific SMF Service Areas apply only for 3GPP access.

The SMF shall release or reject the PDU Session if the DNN of the PDU Session corresponds to a LADN and the I-SMF is inserted to the PDU Session.

NOTE 1: This implies that operators need to plan the LADN deployment in such a way that the LADN Service area needs to be within the SMF Service Area, but not across SMFs' Service Areas.

NOTE 2: This is to cover the case where the UE is not in or moves out of SMF Service Area and an I-SMF is inserted to the PDU Session e.g. during PDU Session Establishment, Service Request. If the PDU Session is maintained with I-SMF, the SMF is not be able to enforce the LADN Service control, e.g. SMF is not notified in the case of Service Request.

Independent of whether deployments topologies with specific SMF Service Areas apply, the SMF may trigger the PDU Session re-establishment to the same DN, if the PDU Session is associated with the SSC mode 2 or SSC mode 3.

NOTE 3: SSC mode 2 or SSC mode 3 can be used to optimize SMF location for a PDU Session and/or, depending on deployment, ensure that the UE is always within the service area of the SMF controlling the PDU Session. In this case (when PDU Session continuity over the PLMN is not required) procedures described in this clause are not needed.

In this Release, how TSC (as defined in clauses 5.27 and 5.28) is supported for PDU Sessions involving an I-SMF is not specified.

In this Release, Redundant User Plane Paths as defined in clause 5.33.2.2 is not supported for PDU Sessions involving an I-SMF.

Redundant PDU sessions support as defined in clause 5.33.2.1 is supported for PDU Sessions involving an I-SMF, when different S-NSSAIs are used for the redundant PDU sessions.

Redundant User Plane Paths as defined in clause 5.33.2.3 is supported for PDU Sessions involving an I-SMF only if this PDU session is established for a S-NSSAI referring to network instances requiring redundant transmission at transport layer.

QoS monitoring (as defined in clause 5.33.3) is supported as long as SMF and not I-SMF initiates the QoS monitoring function.

Dynamic CN PDB provisioning (as defined in clause 5.7.3.4) is supported for PDU Sessions involving an I-SMF.

In this Release, no dedicated functionality is specified for I-SMF and N16a in order to support NPN.

\* \* \* \* End of 2nd change \* \* \* \*

\* \* \* \* 3rd change \* \* \* \*

### 5.34.3 I-SMF selection, V-SMF reselection

The AMF is responsible of detecting when to add or to remove an I-SMF or a V-SMF for a PDU Session. For this purpose, the AMF gets from NRF information about the Service Area and supported DNAI(s) of SMF(s).

During mobility events such as Hand-Over or AMF change, if the service area of the SMF does not include the new UE location, then the AMF selects and inserts an I-SMF which can serve the UE location and the S-NSSAI. Conversely if the AMF detects that an I-SMF is no more needed (as the service area of the SMF includes the new UE location) it removes the I-SMF and interfaces directly with the SMF of the PDU Session. If the AMF detects that the SMF cannot serve the UE location (e.g. due to mobility), then the AMF selects a new I-SMF serving the UE location. If the existing I-SMF (or V-SMF) cannot serve the UE location (e.g. due to mobility) and the service area of the SMF does not include the new UE location (or the PDU Session is Home Routed), then the AMF initiates an I-SMF (or V-SMF) change.

Due to the AF uses AF influence traffic mechanism to request target DNAI(s) towards Local DN when the PDU Session has been established, the SMF receives the target DNAI(s) and decides whether it is required to send the target DNAI to the AMF for triggering I-SMF selection, e.g. the SMF determines the target DNAI(s) which are applicable to the current UE location. If current (I-)SMF cannot serve the target DNAI, the AMF performs I-SMF (re)selection based on target DNAI.

At PDU Session Establishment in non-roaming and roaming with LBO scenarios, if the AMF or SCP cannot select an SMF with a Service Area supporting the current UE location for the selected (DNN, S-NSSAI) and required SMF capabilities, the AMF selects an SMF for the selected (DNN, S-NSSAI) and required capabilities and in addition selects an I-SMF serving the UE location and the S-NSSAI.

Compared to the SMF selection function defined in clause 6.3.2, the following parameters are not applicable for I-SMF/V-SMF selection:

- Data Network Name (DNN).

- Subscription information from UDM.

NOTE 1: All SMF(s) and I-SMF are assumed to be able to control the UPF mapping between EPC bearers and 5GC QoS flows.

If delegated SMF discovery is used at PDU Session establishment:

1. The AMF sends Nsmf\_PDUSession\_CreateSMContext Request to SCP and includes the parameters as defined in clause 6.3.2 (e.g. the DNN, required SMF capabilities, UE location) as discovery and selection parameters. If the SCP successfully selects an SMF matching all discovery and selection parameters, the SCP forwards the Nsmf\_PDUSessionCreateSMContext Request to the selected SMF.

2. If the SCP cannot select an SMF matching all discovery and selection parameters, the SCP returns a dedicated error to AMF. In this case the I-SMF also need be discovered.

3. Upon reception of the error from the SCP that an SMF matching all discovery and selection parameters cannot be found, the AMF performs the discovery and selection of the SMF from NRF (thus not providing the UE location as a discovery parameter). The AMF may indicate the maximum number of SMF instances to be returned from NRF, i.e. SMF selection at NRF.

4. The AMF sends Nsmf\_PDUSession\_CreateSMContext Request to SCP, which includes the endpoint (e.g. URI) of the selected SMF and the discovery and selection parameters as defined in clause 6.3.2 except the DNN and the required SMF capabilities, i.e. parameter for I-SMF selection. The SCP performs discovery and selection of the I-SMF and forwards the Nsmf\_PDUSession\_CreateSMContext Request to the selected I-SMF.

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

6. The SMF answers to the I-SMF that answers to the AMF; in this answer the AMF receives the I-SMF ID.

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

If delegated I-SMF discovery is used once the PDU Session establishment has been established, the procedure starts at step 4 above and is further detailed in the messages flows of TS 23.502 [3] clause 23.

If delegated V-SMF discovery is used for V-SMF reselection, clause 6.3.2 applies, but there is no need for discovery and selection of the H-SMF. This is further detailed in the messages flows of TS 23.502 [3] clause 23.

\* \* \* \* End of 3rd change \* \* \* \*

\* \* \* \* 4th change \* \* \* \*

#### 6.2.6.2 NF profile

NF profile of NF instance maintained in an NRF includes the following information:

- NF instance ID.

- NF type.

- PLMN ID.

- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID.

- FQDN or IP address of NF.

- NF capacity information.

- NF priority information.

NOTE 1: This parameter is used for AMF selection, if applicable, as specified in clause 6.3.5. See clause 6.1.6.2.2 of TS 29.510 [58] for its detailed use.

- NF Set ID.

- NF Service Set ID of the NF service instance.

- NF Specific Service authorization information.

- if applicable, Names of supported services.

- Endpoint Address(es) of instance(s) of each supported service.

- Identification of stored data/information.

NOTE 2: This is only applicable for a UDR profile. See applicable input parameters for Nnrf\_NFManagement\_NFRegister service operation in TS 23.502 [3] clause 5.2.7.2.2. This information applicability to other NF profiles is implementation specific.

- Other service parameter, e.g., DNN or DNN list, notification endpoint for each type of notification that the NF service is interested in receiving.

- Location information for the NF instance.

NOTE 3: This information is operator specific. Examples of such information can be geographical location, data center.

- TAI(s).

- NF load information.

- Routing Indicator, for UDM and AUSF.

- One or more GUAMI(s), in the case of AMF.

- SMF area identity(ies) in the case of UPF.

- UDM Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of internal group identifiers, range(s) of external group identifiers for UDM.

- UDR Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of external group identifiers for UDR.

- AUSF Group ID, range(s) of SUPIs for AUSF.

- PCF Group ID, range(s) of SUPIs for PCF.

- HSS Group ID, set(s) of IMPIs, set(s) of IMPU, set(s) of IMSIs, set(s) of PSIs, set(s) of MSISDN for HSS.

- Supported Analytics ID(s), NWDAF Serving Area information (i.e. list of TAIs for which the NWDAF can provide analytics) if available in the case of NWDAF.

NOTE 4: The NWDAF's Serving Area information is common to all its supported Analytics IDs.

- Event ID(s) supported by AFs, in the case of NEF.

- Application Identifier(s) supported by AFs, in the case of NEF.

- Range(s) of External Identifiers, or range(s) of External Group Identifiers, or the domain names served by the NEF, in the case of NEF.

NOTE 5: This is applicable when NEF exposes AF information for analytics purpose as detailed in TS 23.288 [86].

NOTE 6: It is expected service authorization information is usually provided by OA&M system, and it can also be included in the NF profile in the case that e.g. an NF instance has an exceptional service authorization information.

NOTE 7: The NRF may store a mapping between UDM Group ID and SUPI(s), UDR Group ID and SUPI(s), AUSF Group ID and SUPI(s) and PCF Group ID and SUPI(s), to enable discovery of UDM, UDR, AUSF and PCF using SUPI, SUPI ranges as specified in clause 6.3 or interact with UDR to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID based on UE identity, e.g. SUPI (see clause 6.3.1 for details).

- IP domain list as described in clause 6.1.6.2.21 of TS 29.510 [58], Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes, in the case of BSF.

- SCP Domain the NF belongs to.

- Supported DNAI list, in the case of SMF.

\* \* \* \* End of 4th change \* \* \* \*

\* \* \* \* 5th 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). 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 S-NSSAI: the subscribed DNN(s).

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

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.

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.

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].

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).

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 \* \* \* \*