**3GPP TSG-WG SA2 Meeting #164S2-2407555r1**

**Maastricht, NL, Aug 19 – Aug 23, 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.502** | **CR** | **4841** | **rev** |  | **Current version:** | **19.0.0** |  |
|  | | | | | | | | |
| *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:*** | Adding the NAT and packet inspection functionaility in the UPF NF profile | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Rakuten Mobile, CMCC?, Nokia?, ZTE?, SKT? | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPEAS\_Ph2 | | | | |  | ***Date:*** | | | 2024-07-17 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The following UPF functionalities are added in the N4 capabilities and UPF NF profile stored in NRF:  - The functionality of NAT information exposure.  - Packet Inspection functionality (to differentiate between IP or MAC filter based packet detection, and the packet detection based on other means, e.g. layer 7 DPI).  Based on conclusions of TR 23.700-62, 3GPP TS 23.502 should be updated to support the above new requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added text to clause 4.17.6 SMF Provisioning of available UPFs using the NRF, Nnrf\_NFManagement\_NFRegister service operation and Nnrf\_NFDiscovery\_Request service operation | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Support for UPF supporitng NAT and packet inspection feature will be missing in NF Profile section | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.17.6.1, 5.2.7.2.2, 5.2.7.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \*

##### 4.3.2.2.1 Non-roaming and Roaming with Local Breakout

Clause 4.3.2.2.1 specifies PDU Session establishment in the non-roaming and roaming with local breakout cases. The procedure is used to:

- Establish a new PDU Session;

- Handover a PDN Connection in EPS to PDU Session in 5GS without N26 interface;

- Switching an existing PDU Session between non-3GPP access and 3GPP access. The specific system behaviour in this case is further defined in clauses 4.9.2 and 4.9.3; or

- Request a PDU Session for Emergency services.

In the case of roaming, the AMF determines if a PDU Session is to be established in LBO or Home Routing. In the case of LBO, the procedure is as in the case of non-roaming with the difference that the AMF, the SMF, the UPF and the PCF are located in the visited network. PDU Sessions for Emergency services are never established in Home Routed mode. If Control Plane CIoT 5GS Optimisation is enabled for the PDU session with LBO, the NEF is not used as the anchor of this PDU Session.

NOTE 1: UE provides both the S-NSSAIs of the Home PLMN and Visited PLMN to the network as described in clause 5.15.5.3 of TS 23.501 [2].



Figure 4.3.2.2.1-1: UE-requested PDU Session Establishment for non-roaming and roaming with local breakout

The procedure assumes that the UE has already registered on the AMF thus unless the UE is Emergency Registered the AMF has already retrieved the user subscription data from the UDM.

1. From UE to AMF: NAS Message (S-NSSAI(s), [Alternative S-NSSAI], UE Requested DNN, PDU Session ID, Request type, Old PDU Session ID, N1 SM container (PDU Session Establishment Request, [Port Management Information Container])).

In order to establish a new PDU Session, the UE generates a new PDU Session ID.

The UE initiates the UE Requested PDU Session Establishment procedure by the transmission of a NAS message containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID, Requested PDU Session Type, a Requested SSC mode, 5GSM Capability, PCO, SM PDU DN Request Container, [Number Of Packet Filters], [Header Compression Configuration], UE Integrity Protection Maximum Data Rate, [Always-on PDU Session Requested], [RSN], [URSP rule enforcement reports] and [PDU Session Pair ID].

The Request Type indicates "Initial request" if the PDU Session Establishment is a request to establish a new PDU Session and indicates "Existing PDU Session" if the request refers to an existing PDU Session switching between 3GPP access and non-3GPP access or to a PDU Session handover from an existing PDN connection in EPC. If the request refers to an existing PDN connection in EPC, the S-NSSAI is set as described in clause 5.15.7.2 of TS 23.501 [2]

When Emergency service is required and an Emergency PDU Session is not already established, a UE shall initiate the UE Requested PDU Session Establishment procedure with a Request Type indicating "Emergency Request".

The Request Type indicates "Emergency Request" if the PDU Session Establishment is a request to establish a PDU Session for Emergency services. The Request Type indicates "Existing Emergency PDU Session" if the request refers to an existing PDU Session for Emergency services switching between 3GPP access and non-3GPP access or to a PDU Session handover from an existing PDN connection for Emergency services in EPC.

The 5GSM Core Network Capability is provided by the UE and handled by SMF as defined in clause 5.4.4b of TS 23.501 [2].

The Number Of Packet Filters indicates the number of supported packet filters for signalled QoS rules for the PDU Session that is being established. The number of packet filters indicated by the UE is valid for the lifetime of the PDU Session. For presence condition, see TS 24.501 [25].

The UE Integrity Protection Maximum Data Rate indicates the maximum data rate up to which the UE can support UP integrity protection. The UE shall provide the UE Integrity Protection Data Rate capability independently of the Access Type over which the UE sends the PDU Session Establishment Request.

If the use of header compression for Control Plane CIoT 5GS optimisation was negotiated successfully between the UE and the network in the previous registration procedure, the UE shall include the Header Compression Configuration, unless "Unstructured" PDU Session Type is indicated. The Header Compression Configuration includes the information necessary for the header compression channel setup. Optionally, the Header Compression Configuration may include additional header compression context parameters.

The NAS message sent by the UE is encapsulated by the AN in a N2 message towards the AMF that should include User location information and Access Type Information.

The PDU Session Establishment Request message may contain SM PDU DN Request Container containing information for the PDU Session authorization by the external DN.

The UE includes the S-NSSAI from the Allowed NSSAI of the current access type or Partially Allowed NSSAI. If the UE is provided with the mapping of an S-NSSAI that is replaced by an Alternative S-NSSAI, the UE shall provide both the Alternative S-NSSAI and the S-NSSAI that is replaced by it. If the Mapping of Allowed NSSAI or Mapping Of Partially Allowed NSSAI was provided to the UE, the UE shall provide both the S-NSSAI of the VPLMN from the Allowed NSSAI or Partially Allowed NSSAI and the corresponding S-NSSAI of the HPLMN from the Mapping Of Allowed NSSAI or Mapping Of Partially Allowed NSSAI. If the UE is provided with the mapping of the VPLMN S-NSSAI to a VPLMN Alternative S-NSSAI, the UE provides both the VPLMN Alternative S-NSSAI and the VPLMN S-NSSAI in the PDU Session Establishment message. If the UE is provided with the mapping of the HPLMN S-NSSAI to a HPLMN Alternative S-NSSAI, the UE provides both the HPLMN Alternative S-NSSAI and the HPLMN S-NSSAI in the PDU Session Establishment message. The AMF verifies whether the Alternative S-NSSAI and the S-NSSAI provided in the PDU Session Establishment Request message is valid based on the UE context as described in clause 5.15.19 of TS 23.501 [2].

If the procedure is triggered for SSC mode 3 operation, the UE shall also include the Old PDU Session ID which indicates the PDU Session ID of the on-going PDU Session to be released, in NAS message. The Old PDU Session ID is included only in this case.

The AMF receives from the AN the NAS SM message (built in step 1) together with User Location Information (e.g. Cell Id in the case of the NG-RAN).

The UE shall not trigger a PDU Session establishment for a PDU Session corresponding to a LADN when the UE is outside the area of availability of the LADN.

The UE shall not trigger a PDU Session establishment for a PDU Session associated to an S-NSSAI if the S-NSSAI is not valid as per the S-NSSAI location availability information.

If the UE is establishing a PDU session for IMS and the UE is configured to discover the P-CSCF address during connectivity establishment, the UE shall include an indicator that it requests a P‑CSCF IP address(es) within the SM container.

The PS Data Off status is included in the PCO in the PDU Session Establishment Request message.

The UE capability to support Reliable Data Service is included in the PCO in the PDU Session Establishment Request message.

If the UE has indicated that it supports transfer of Port Management Information Containers as per UE 5GSM Core Network Capability and if the PDU session type is Ethernet, then the UE shall include the MAC address of the DS-TT Ethernet port used for this Ethernet PDU session. If the UE is aware of the UE-DS-TT Residence Time, then the UE shall additionally include the UE-DS-TT Residence Time.

If the UE requests to establish always-on PDU session, the UE includes an Always-on PDU Session Requested indication in the PDU Session Establishment Request message.

As described in TS 23.548 [74], a UE that hosts EEC(s) may indicate in the PCO that it supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s).

A UE that hosts the EDC functionality shall indicate in the PCO its capability to support the EDC functionality (see clause 5.2.1 of TS 23.548 [74]).

The UE may also include PDU Session Pair ID and/or RSN in PDU Session Establishment Request message as described in clause 5.33.2.1 of TS 23.501 [2].

A UE that supports EAS re-discovery as described in clause 6.2.3.3 of TS 23.548 [74], may indicate so in the PCO.

Port Management Information Container may be received from DS-TT and includes port management capabilities, i.e. information indicating which standardized and deployment-specific port management information is supported by DS-TT as defined in clause 5.28.3 of TS 23.501 [2].

If UE supports to report URSP rule enforcement to network and the URSP rule that triggered this PDU Session Establishment Request included the Indication for reporting URSP rule enforcement, the UE may provide URSP rule enforcement report as described in clause 6.6.2.4 of TS 23.503 [20].

2. For NR satellite access, the AMF may decide to verify the UE location as described in clause 5.4.11.4 of TS 23.501 [2].

The AMF determines that the message corresponds to a request for a new PDU Session based on that Request Type indicates "initial request" and that the PDU Session ID is not used for any existing PDU Session of the UE. If the NAS message does not contain an S-NSSAI, the AMF determines an S-NSSAI of the Serving PLMN for the requested PDU Session from the current Allowed NSSAI for the UE. If there is only one S-NSSAI in the Allowed NSSAI, this S-NSSAI shall be used. If there is more than one S-NSSAI in the Allowed NSSAI, the S-NSSAI selected is either according to the UE subscription, if the subscription contains only one default S-NSSAI and the corresponding mapped HPLMN S-NSSAI of the Serving PLMN is included in the Allowed NSSAI, or based on operator policy (e.g. also ensures any UE Requested DNN is allowed for the selected S-NSSAI)). When the NAS Message does not contain a DNN, the AMF determines the DNN for the requested PDU Session by selecting the default DNN for the S-NSSAI (irrespective of whether the S-NSSAI is included in the NAS message or determined by the AMF) if the default DNN is present in the UE's Subscription Information (or for the corresponding S-NSSAI of the HPLMN, in the case of LBO); otherwise the serving AMF selects a locally configured DNN for this S-NSSAI of the Serving PLMN. If the AMF cannot select an SMF (e.g. the UE requested DNN is not supported by the network, or the UE requested DNN is not in the Subscribed DNN List for the S-NSSAI (or its mapped value for the HPLMN in the case of LBO) and wildcard DNN is not included in the Subscribed DNN list), the AMF shall, based on operator policies received from PCF, either reject the NAS Message containing PDU Session Establishment Request from the UE with an appropriate cause or request PCF to replace the UE requested DNN by a selected DNN. If the DNN requested by the UE is present in the UE subscription information but indicated for replacement in the operator policies received from PCF, the AMF shall request the PCF to perform a DNN replacement to a selected DNN. AMF requests DNN replacement as specified in clause 4.16.2.1.1. If the DNN requested by the UE is present in the UE subscription information but not supported by the network and not indicated for replacement in the operator policies received from PCF, the AMF shall reject the NAS Message containing PDU Session Establishment Request from the UE with an appropriate cause value.

The AMF selects an SMF as described in clause 6.3.2 of TS 23.501 [2] and clause 4.3.2.2.3. If the Request Type indicates "Initial request" or the request is due to handover from EPS or from non-3GPP access serving by a different AMF, the AMF stores an association of the S-NSSAI(s), the DNN, the PDU Session ID, the SMF ID as well as the Access Type of the PDU Session. If the AMF determines to replace the S-NSSAI received from the UE with the Alternative S-NSSAI or the AMF receives the Alternative S-NSSAI and the S-NSSAI is by the UE, the AMF selects the SMF based on the Alternative S-NSSAI.

During registration procedures, the AMF determines the use of the Control Plane CIoT 5GS Optimisation or User Plane CIoT 5GS Optimisation based on UEs indications in the 5G Preferred Network Behaviour, the serving operator policies and the network support of CIoT 5GS optimisations. The AMF selects an SMF that supports Control Plane CIoT 5GS optimisation or User Plane CIoT 5GS Optimisation as described in clause 6.3.2 of TS 23.501 [2].

If the Request Type is "initial request" and if the Old PDU Session ID indicating the existing PDU Session is also contained in the message, the AMF selects an SMF as described in clause 4.3.5.2 and stores an association of the new PDU Session ID, the S-NSSAI(s), the selected SMF ID as well as Access Type of the PDU Session.

If the Request Type indicates "Existing PDU Session", the AMF selects the SMF based on SMF-ID received from UDM. The case where the Request Type indicates "Existing PDU Session" and either the AMF does not recognize the PDU Session ID or the subscription context that the AMF received from UDM during the Registration or Subscription Profile Update Notification procedure does not contain an SMF ID corresponding to the PDU Session ID constitutes an error case. The AMF updates the Access Type stored for the PDU Session.

If the Request Type indicates "Existing PDU Session" referring to an existing PDU Session moved between 3GPP access and non-3GPP access, then if the Serving PLMN S-NSSAI of the PDU Session is present in the Allowed NSSAI of the target access type or Partially Allowed NSSAI, the PDU Session Establishment procedure can be performed in the following cases:

- the SMF ID corresponding to the PDU Session ID and the AMF belong to the same PLMN;

- the SMF ID corresponding to the PDU Session ID belongs to the HPLMN;

Otherwise the AMF shall reject the PDU Session Establishment Request with an appropriate reject cause.

NOTE 2: The SMF ID includes the PLMN ID that the SMF belongs to.

The AMF shall reject a request coming from an Emergency Registered UE and the Request Type indicates neither "Emergency Request" nor "Existing Emergency PDU Session". When the Request Type indicates "Emergency Request", the AMF is not expecting any S-NSSAI and DNN value provided by the UE and uses locally configured values instead. The AMF stores the Access Type of the PDU Session.

If the Request Type indicates "Emergency Request" or "Existing Emergency PDU Session", the AMF selects the SMF as described in clause 5.16.4 of TS 23.501 [2].

If the AMF is running a slice deregistration inactivity timer for the S-NSSAI of the PDU Session and the timer is associated with the Access Type over which the PDU Session Establishment Request was received, the AMF stops the timer.

3. From AMF to SMF: Either Nsmf\_PDUSession\_CreateSMContext Request (SUPI, selected DNN, UE requested DNN, S-NSSAI(s), [Alternative S-NSSAI], [Slice Area Restriction indication], PDU Session ID, AMF ID, Request Type, [PCF ID, Same PCF Selection Indication], Priority Access, [Small Data Rate Control Status], N1 SM container (PDU Session Establishment Request), User location information, Access Type, RAT Type, PEI, GPSI, UE presence in LADN service area, Subscription For PDU Session Status Notification, DNN Selection Mode, Trace Requirements, Control Plane CIoT 5GS Optimisation indication, Control Plane Only indicator, Satellite backhaul category, GEO Satellite ID, [PVS FQDN(s) and/or PVS IP address(es), Onboarding Indication], Disaster Roaming service indication) or Nsmf\_PDUSession\_UpdateSMContext Request (SUPI, DNN, S-NSSAI(s), SM Context ID, AMF ID, Request Type, N1 SM container (PDU Session Establishment Request), User location information, Access Type, RAT type, PEI, Serving Network (PLMN ID, or PLMN ID and NID, see clause 5.18 of TS 23.501 [2]), Satellite backhaul category, GEO Satellite ID), [PCF binding information, notification of SM Policy Association establishment Indication].

If the AMF does not have an association with an SMF for the PDU Session ID provided by the UE (e.g. when Request Type indicates "initial request"), the AMF invokes the Nsmf\_PDUSession\_CreateSMContext Request, but if the AMF already has an association with an SMF for the PDU Session ID provided by the UE (e.g. when Request Type indicates "existing PDU Session"), the AMF invokes the Nsmf\_PDUSession\_UpdateSMContext Request.

The AMF sends the S-NSSAI of the Serving PLMN from the Allowed NSSAI or Partially Allowed NSSAI to the SMF. If the AMF determined to replace the S-NSSAI received from the UE with an Alternative S-NSSAI and the AMF selected the SMF based on the Alternative S-NSSAI in step 2, the AMF sends both the S-NSSAI value of the Alternative S-NSSAI and the S-NSSAI value of the S-NSSAI received from the UE to the SMF. If the Alternative S-NSSAI and the S-NSSAI is provided by the UE and the AMF selected the SMF based on the Alternative S-NSSAI in step 2, the AMF sends both the S-NSSAI value of the Alternative S-NSSAI and the S-NSSAI value of the S-NSSAI received from the UE to the SMF. For roaming scenario in local breakout (LBO), the AMF also sends the corresponding S-NSSAI of the HPLMN from the Mapping Of Allowed NSSAI or Mapping Of Partially Allowed NSSAI to the SMF. If the AMF determines to replace the HPLMN S-NSSAI received from the UE with the HPLMN Alternative S-NSSAI or the AMF receives the HPLMN Alternative S-NSSAI and the HPLMN S-NSSAI provided by the UE, the AMF sends both HPLMN S-NSSAI and HPLMN Alternative S-NSSAI to the SMF.

When the AMF determines that the S-NSSAI is subject to area restriction, i.e. the S-NSSAI is configured with an NS-AoS, or the S-NSSAI is present in the Partially Allowed NSSAI, the AMF sends Slice Area Restriction indication to SMF indicating that the PDU Session is subject to area restriction for the S-NSSAI. If the S-NSSAI is replaced with the Alternative S-NSSAI, the AMF checks the area restriction only for the Replaced S-NSSAI.

The AMF ID is the UE's GUAMI which uniquely identifies the AMF serving the UE. The AMF forwards the PDU Session ID together with the N1 SM container containing the PDU Session Establishment Request received from the UE. The GPSI shall be included if available at AMF.

The AMF determines Access Type and RAT Type, see clause 4.2.2.2.1.

The AMF provides the PEI instead of the SUPI when the UE in limited service state has registered for Emergency services (i.e. Emergency Registered) without providing a SUPI. The PEI is defined in clause 5.9.3 of TS 23.501 [2]. If the UE in limited service state has registered for Emergency services (i.e. Emergency Registered) with a SUPI but has not been authenticated the AMF indicates that the SUPI has not been authenticated. The SMF determines that the UE has not been authenticated when it does not receive a SUPI for the UE or when the AMF indicates that the SUPI has not been authenticated.

If the AMF determines that the selected DNN corresponds to an LADN then the AMF provides the "UE presence in LADN service area" that indicates if the UE is IN or OUT of the LADN service area. If the AMF enforces the LADN Service Area per LADN DNN and S-NSSAI, then the AMF also provides an indication that "the PDU Session is subject to LADN per LADN DNN and S-NSSAI".

If the Old PDU Session ID is included in step 1 and if the SMF is not to be reallocated, the AMF also includes Old PDU Session ID in the Nsmf\_PDUSession\_CreateSMContext Request.

DNN Selection Mode is determined by the AMF. It indicates whether an explicitly subscribed DNN has been provided by the UE in its PDU Session Establishment Request.

The SMF may use DNN Selection Mode when deciding whether to accept or reject the UE request.

When the Establishment cause received as part of AN parameters during the Registration procedure or Service Request procedure is associated with priority services (e.g. MPS, MCX), or when the AMF determines the UE has priority subscription (e.g. MPS, MCX) in the UDM, the AMF includes a Message Priority header to indicate priority information. The SMF uses the Message Priority header to determine if the UE request is subject to exemption from NAS level congestion control. Other NFs relay the priority information by including the Message Priority header in service-based interfaces, as specified in TS 29.500 [17].

In the local breakout case, if the SMF (in the VPLMN) is not able to process some part of the N1 SM information that Home Routed Roaming is required and the SMF responds to the AMF that it is not the right SMF to handle the N1 SM message by invoking Nsmf\_PDUSession\_CreateSMContext Response service operation. The SMF includes a proper N11 cause code triggering the AMF to proceed with home routed case. The procedure starts again at step 2 of clause 4.3.2.2.2.

In the non-roaming case, for PDU Session with Request Type "initial request", the AMF checks if the PCF Selection Assistance info from the UDM indicates that the same PCF is required for the requested DNN and S-NSSAI and if required, the AMF includes in Nsmf\_PDUSession\_CreateSMContext Request both the Same PCF Selection Indication and the PCF ID selected by the AMF, this PCF ID identifies the H-PCF,

If PCF Selection Assistance info is not received from the UDM, the AMF may include a PCF ID in the Nsmf\_PDUSession\_CreateSMContext Request based on operator policies. This PCF ID identifies the H-PCF in the non-roaming case and the V-PCF in the local breakout roaming case.

The AMF includes Trace Requirements if Trace Requirements have been received in subscription data.

If the AMF decides to use the Control Plane CIoT 5GS Optimisation or User Plane CIoT 5GS Optimisation as specified in step 2 or to only use Control Plane CIoT 5GS Optimisation for the PDU session as described in clause 5.31.4 of TS 23.501 [2], the AMF sends the Control Plane CIoT 5GS Optimisation indication or Control Plane Only indicator to the SMF.

If the AMF determines that the RAT type is NB-IoT and the number of PDU Sessions with user plane resources activated for the UE has reached the maximum number of supported user plane resources (0, 1 or 2) based on whether the UE supports UP data transfer and the UE's 5GMM Core Network Capability as described in clause 5.31.19 of TS 23.501 [2], the AMF may either reject the PDU Session Establishment Request or continue with the PDU Session establishment and include the Control Plane CIoT 5GS Optimisation indication or Control Plane Only indicator to the SMF.

The AMF includes the latest Small Data Rate Control Status if it has stored it for the PDU Session.

If the RAT type was included in the message, then the SMF stores the RAT type in SM Context.

If the UE supports CE mode B and use of CE mode B is not restricted according to the Enhanced Coverage Restriction information in the UE context in the AMF, then the AMF shall include the extended NAS-SM timer indication. Based on the extended NAS-SM timer indication, the SMF shall use the extended NAS-SM timer setting for the UE as specified in TS 24.501 [25].

If the identity of an NWDAF is available to the AMF, the AMF informs the SMF of the NWDAF ID(s) used for UE related Analytics and corresponding Analytics ID(s).

If the AMF, based on configuration, is aware that the UE is accessing over a gNB using satellite backhaul as defined in clause 5.43.4 of TS 23.501 [2], the AMF determines the type of satellite backhaul category and includes Satellite backhaul category to the SMF.

If the AMF, based on configuration, is aware that the UE is accessing over a gNB using GEO satellite backhaul, the AMF may, based on configuration, include the GEO satellite ID as described in clause 5.43.2 of TS 23.501 [2].

The AMF may provide the Disaster Roaming service indication as specified in TS 23.501 [2].

4. If Session Management Subscription data for corresponding SUPI, DNN and S-NSSAI of the HPLMN is not available, then SMF retrieves the Session Management Subscription data using Nudm\_SDM\_Get (SUPI, Session Management Subscription data, selected DNN, S-NSSAI of the HPLMN, Serving PLMN ID, [NID]) and subscribes to be notified when this subscription data is modified using Nudm\_SDM\_Subscribe (SUPI, Session Management Subscription data, selected DNN, S-NSSAI of the HPLMN, Serving PLMN ID, [NID]). The UDM may get this information from UDR by Nudr\_DM\_Query (SUPI, Subscription Data, Session Management Subscription data, selected DNN, S-NSSAI of the HPLMN, Serving PLMN ID, [NID]) and may subscribe to notifications from UDR for the same data by Nudr\_DM\_subscribe. If a S-NSSAI is subject to network slice usage control and the S-NSSAI is dedicated to a single AF, for a PDU Session for non-roaming subscribers, the UDM may provide a Slice Usage Policy information including whether a network slice is on demand and a PDU Session inactivity timer value as described in clause 5.15.15 of TS 23.501 [2]. If the SMF received Alternative S-NSSAI (for the HPLMN in roaming case) in step 3, the SMF retrieves subscription data as specified in clause 5.15.19 of TS 23.501 [2].

The SMF may use DNN Selection Mode when deciding whether to retrieve the Session Management Subscription data e.g. if the (selected DNN, S-NSSAI of the HPLMN) is not explicitly subscribed, the SMF may use local configuration instead of Session Management Subscription data.

If the Request Type in step 3 indicates "Existing PDU Session" or "Existing Emergency PDU Session" the SMF determines that the request is due to switching between 3GPP access and non-3GPP access or due to handover from EPS. The SMF identifies the existing PDU Session based on the PDU Session ID. In such a case, the SMF does not create a new SM context but instead updates the existing SM context and provides the representation of the updated SM context to the AMF in the response.

If the Request Type is "Initial request" and if the Old PDU Session ID is included in Nsmf\_PDUSession\_CreateSMContext Request, the SMF identifies the existing PDU Session to be released based on the Old PDU Session ID.

The Subscription data includes the Allowed PDU Session Type(s), Allowed SSC mode(s), default 5QI and ARP, subscribed Session-AMBR, SMF-Associated external parameters.

IP Index or Static IP address/prefix may be included in the subscription data if the UE has subscribed to it.

The required UPF functionalities and/or preferred UPF functionalities for the PDU Session may be included in the subscription data.

The SMF checks the validity of the UE request: it checks:

- Whether the UE request is compliant with the user subscription and with local policies;

- (If the selected DNN corresponds to an LADN), whether the UE is located within the LADN service area based on the "UE presence in LADN service area" indication from the AMF. If the AMF does not provide the "UE presence in LADN service area" indication and the SMF determines that the selected DNN corresponds to a LADN, then the SMF considers that the UE is OUT of the LADN service area.

The SMF determines whether the PDU Session requires redundancy and the SMF determines the RSN as described in clause 5.33.2.1 of TS 23.501 [2]. If the SMF determines that redundant handling is not allowed or not possible for the given PDU Session, the SMF shall either reject the establishment of the PDU Session or accept the establishment of a PDU session without redundancy handling based on local policy.

If the UE request is considered as not valid, the SMF decides to not accept to establish the PDU Session.

NOTE 3: The SMF can, instead of the Nudm\_SDM\_Get service operation, use the Nudm\_SDM\_Subscribe service operation with an Immediate Report Indication that triggers the UDM to immediately return the subscribed data if the corresponding feature is supported by both the SMF and the UDM.

For a Disaster Roaming service, the UDM provides the Session Management Subscription data to the SMF based on the local policy and/or the local configuration as specified in clause 5.40.4 of TS 23.501 [2].

For an S-NSSAI subject to NSAC and if LBO applies, the SMF in supporting VPLMN stores the applicable NSAC admission mode.

5. From SMF to AMF: Either Nsmf\_PDUSession\_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause))) or an Nsmf\_PDUSession\_UpdateSMContext Response depending on the request received in step 3.

If the SMF received Nsmf\_PDUSession\_CreateSMContext Request in step 3 and the SMF is able to process the PDU Session establishment request, the SMF creates an SM context and responds to the AMF by providing an SM Context ID.

If the UP Security Policy for the PDU Session is determined to have Integrity Protection set to "Required", the SMF may, based on local configuration, decide whether to accept or reject the PDU Session request based on the UE Integrity Protection Maximum Data Rate.

NOTE 4: The SMF can e.g. be configured to reject a PDU Session if the UE Integrity Protection Maximum Data Rate has a very low value, if the services provided by the DN would require higher bitrates.

When the SMF decides to not accept to establish a PDU Session, the SMF rejects the UE request via NAS SM signalling including a relevant SM rejection cause by responding to the AMF with Nsmf\_PDUSession\_CreateSMContext Response. The SMF also indicates to the AMF that the PDU Session ID is to be considered as released, the SMF proceeds to step 20 and the PDU Session Establishment procedure is stopped.

6. Optional Secondary authentication/authorization.

If the Request Type in step 3 indicates "Existing PDU Session", the SMF does not perform secondary authentication/authorization.

If the Request Type received in step 3 indicates "Emergency Request" or "Existing Emergency PDU Session", the SMF shall not perform secondary authentication\authorization.

If the SMF needs to perform secondary authentication/authorization during the establishment of the PDU Session by a DN-AAA Server as described in clause 5.6.6 of TS 23.501 [2], the SMF triggers the PDU Session establishment authentication/authorization as described in clause 4.3.2.3.

7a. If dynamic PCC is to be used for the PDU Session, the SMF performs PCF selection as described in clause 6.3.7.1 of TS 23.501 [2]. If the Request Type indicates "Existing PDU Session" or "Existing Emergency PDU Session", the SMF shall use the PCF already selected for the PDU Session.

Otherwise, the SMF may apply local policy.

7b. The SMF may perform an SM Policy Association Establishment procedure as defined in clause 4.16.4 to establish an SM Policy Association with the PCF and get the default PCC Rules for the PDU Session. The SMF shall include the 3GPP Data Off status if received in step 1. The GPSI, PVS FQDN(s) and/or PVS IP address(es) and the Onboarding Indication shall be included if available at SMF in the case of ON-SNPN. The SMF shall include both the S-NSSAI and the Alternative S-NSSAI, if received in step 3. If the Request Type in step 3 indicates "Existing PDU Session", the SMF provides information on the Policy Control Request Trigger condition(s) that have been met by an SMF initiated SM Policy Association Modification procedure as defined in clause 4.16.5.1. The PCF may provide policy information defined in clause 5.2.5.4 (and in TS 23.503 [20]) to SMF.

The PCF for the UE subscribes to notifications of event "UE reporting Connection Capabilities from associated URSP rule" as defined in clause 6.1.3.18 in TS 23.503 [20], using Npcf\_PolicyAuthorization\_Subscribe (EventId set to "UE reporting Connection Capabilities from associated URSP rule", EventFilter set to at least "list of Connection Capabilities") to the PCF for the PDU Session. The PCF for session may notify the PCF for UE about the URSP rule enforcement together with the PDU session parameters that this application associated with by Npcf\_PolicyAuthorization\_Notify.

During the SM Policy Association Establishment procedure, if the PCF detects the request relates to SM Policy Association enabling integration with TSN or TSC or Deterministic Networking (as defined in TS 23.501 [2] clause 5.28) based on local configuration, the PCF may provide policy control request trigger for 5GS Bridge/Router Information as defined in clause 6.1.3.5 of TS 23.503 [20].

The PCF, based on the Emergency DNN, sets the ARP of the PCC rules to a value that is reserved for Emergency services as described in TS 23.503 [20].

NOTE 5: The purpose of step 7 is to receive PCC rules before selecting UPF. If PCC rules are not needed as input for UPF selection, step 7 can be performed after step 8.

- During the SM Policy Association Establishment procedure for PDU Sessions for non-roaming UEs, if a S-NSSAI is subject to network slice usage control, the PCF may provide a Slice Usage Policy information including whether a network slice is on demand and a PDU Session inactivity timer value as described in clause 5.15.15 of TS 23.501 [2].

8. If the Request Type in step 3 indicates "Initial request", the SMF selects an SSC mode for the PDU Session as described in clause 5.6.9.3 of TS 23.501 [2]. The SMF also selects one or more UPFs as needed as described in clause 6.3.3 of TS 23.501 [2]. In the case of PDU Session Type IPv4 or IPv6 or IPv4v6, the SMF allocates an IP address/prefix for the PDU Session (unless configured otherwise) as described in clause 5.8.2 of TS 23.501 [2]. In the case of PDU Session Type IPv6 or IPv4v6, the SMF also allocates an interface identifier to the UE for the UE to build its link-local address. For Unstructured PDU Session Type the SMF may allocate an IPv6 prefix for the PDU Session and N6 point-to-point tunnelling (based on UDP/IPv6) as described in clause 5.6.10.3 of TS 23.501 [2]. For Ethernet PDU Session Type, neither a MAC nor an IP address is allocated by the SMF to the UE for this PDU Session.

If the AMF indicated Control Plane CIoT 5GS Optimisation in step 3 for this PDU session, then,

1) For Unstructured PDU Session Type, the SMF checks whether UE's subscription include a "NEF Identity for NIDD" for the DNN/S-NSSAI combination. When the "NEF Identity for NIDD" is present in the UE's subscription data, the SMF will select the NEF identified for the S-NSSAI and selected DNN in the "NEF Identity for NIDD" as the anchor of this PDU Session. Otherwise, the SMF will select a UPF as the anchor of this PDU Session.

2) For other PDU Session Types, the SMF will perform UPF selection to select a UPF as the anchor of this PDU Session.

If the Request Type in Step 3 is "Existing PDU Session", the SMF maintains the same IP address/prefix that has already been allocated to the UE in the source network.

If the Request Type in step 3 indicates "Existing PDU Session" referring to an existing PDU Session moved between 3GPP access and non-3GPP access the SMF maintains the SSC mode of the PDU Session, the current PDU Session Anchor and IP address.

NOTE 6: The SMF may decide to trigger e.g. new intermediate UPF insertion or allocation of a new UPF as described in step 5 in clause 4.2.3.2.

If the Request Type indicates "Emergency Request", the SMF selects the UPF as described in clause 5.16.4 of TS 23.501 [2] and selects SSC mode 1.

SMF may select a UPF (e.g. based on requested DNN/S-NSSAI) that supports NW-TT functionality.

SMF may select a PSA UPF that supports PDU Set identification and marking for a QoS flow with PDU Set based handling capability.

SMF may select a PSA UPF based on subscription information (i.e., the required UPF functionalities and/or priority of preferred UPF functionalities) from UDM. For example, the SMF may select the best UPF supporting all the required functionalities and the set of preferred functionalities with higher priority.

9. SMF may perform an SMF initiated SM Policy Association Modification procedure as defined in clause 4.16.5.1 to provide information on the Policy Control Request Trigger condition(s) that have been met. If Request Type is "initial request" and dynamic PCC is deployed and PDU Session Type is IPv4 or IPv6 or IPv4v6, SMF notifies the PCF (if the Policy Control Request Trigger condition is met) with the allocated UE IP address/prefix(es).

NOTE 7: If an IP address/prefix has been allocated before step 7 (e.g. subscribed static IP address/prefix in UDM/UDR) or the step 7 is performed after step 8, the IP address/prefix can be provided to PCF in step 7 and the IP address/prefix notification in this step can be skipped.

If the PCF has subscribed to Policy Control Request Trigger for "UE reporting Connection Capabilities from associated URSP rule" and if SMF received the URSP rule enforcement report (i.e. connection capabilities information) from the UE at step 1, then the SMF may include the URSP rule enforcement report as described in clause 6.1.3.5 of TS 23.503 [20] and clause 6.6.2.4 of TS 23.503 [20].

The PCF may provide updated policies to the SMF. The PCF may provide policy information defined in clause 5.2.5.4 (and in TS 23.503 [20]) to SMF.

The PCF may generate SDF Templates in PCC rules based on the reported Connection Capabilities as described in clause 6.1.6 in TS 23.503 [20].

NOTE 8: The mapping between Connection Capability and SDF templates in the PCC rule is implementation specific.

10. If Request Type indicates "initial request", the SMF initiates an N4 Session Establishment procedure with the selected UPF(s), otherwise it initiates an N4 Session Modification procedure with the selected UPF(s):

10a. The SMF sends an N4 Session Establishment/Modification Request to the UPF and provides Packet detection, enforcement and reporting rules to be installed on the UPF for this PDU Session. If the SMF is configured to request IP address allocation from UPF as described in clause 5.8.2 of TS 23.501 [2] then the SMF indicates to the UPF to perform the IP address/prefix allocation and includes the information required for the UPF to perform the allocation. If the selective User Plane deactivation is required for this PDU Session, the SMF determines the inactivity timer and provides it to the UPF. For a PDU Session for non-roaming subscribers, if the S-NSSAI of the PDU Session is subject to network slice usage control, the SMF obtains the PDU Session inactivity timer value for the PDU Session as described in step 4 or step 7 or uses preconfigured value and configures the UPF to run the PDU Session inactivity timer. The SMF provides Trace Requirements to the UPF if it has received Trace Requirements. If the Reliable Data Service is enabled for the PDU Session by the SMF as specified in TS 23.501 [2], the RDS Configuration information is provided to the UPF in this step. The SMF provides Small Data Rate Control parameters to the UPF for the PDU Session, if required. The SMF provides the Small Data Rate Control Status to the UPF, if received from the AMF. If the Serving PLMN intends to enforce Serving PLMN Rate Control (see clause 5.31.14.2 of TS 23.501 [2]) for this PDU session then the SMF shall provide Serving PLMN Rate Control parameters to UPF for limiting the rate of downlink control plane data packets.

For a PDU Session of type Ethernet or IP, the SMF (e.g. for a certain requested DNN/S-NSSAI for which Time Sensitive Networking, Time Sensitive Communications, Time Synchronization and/or Deterministic Networking is applicable) may include an indication to request UPF to provide a port number.

If SMF decides to perform redundant transmission for one or more QoS Flows of the PDU session as described in clause 5.33.1.2 of TS 23.501 [2], two CN Tunnel Info are requested by the SMF from the UPF. The SMF also indicates the UPF to eliminate the duplicated packet for the QoS Flow in uplink direction. The SMF indicates the UPF that one CN Tunnel Info is used as the redundancy tunnel of the PDU session described in clause 5.33.2.2 of TS 23.501 [2].

If SMF decides to insert two I-UPFs between the PSA UPF and the NG-RAN for redundant transmission as described in clause 5.33.1.2 of TS 23.501 [2], the SMF requests the corresponding CN Tunnel Info and provides them to the I-UPFs and PSA UPF respectively. The SMF also indicates the PSA UPF to eliminate the duplicated packet for the QoS Flow in uplink direction. The SMF indicates the PSA UPF that one CN Tunnel Info is used as the redundancy tunnel of the PDU session described in clause 5.33.2.2 of TS 23.501 [2].

NOTE 9: The method to perform elimination and reordering on RAN/UPF based on the packets received from the two GTP-U tunnels is up to RAN/UPF implementation. The two GTP-U tunnels are terminated at the same RAN node and UPF.

If Control Plane CIoT 5GS Optimisation is enabled for this PDU session and the SMF selects the NEF as the anchor of this PDU Session in step 8, the SMF performs SMF-NEF Connection Establishment Procedure as described in clause 4.25.2.

If interworking with TSN deployed in the transport network is supported (see clause 4.4.8 of TS 23.501 [2]) and the UPF supports CN-TL, the SMF includes a TL-Container with a get-request to the N4 Session Establishment/Modification request that is sent to the UPF, as described in clause 5.28a.2 of TS 23.501 [2].

If SMF decides to enable ECN marking for L4S by PSA UPF, a QoS Flow level ECN marking for L4S indicator shall be sent by SMF to PSA UPF over N4 as described in clause 5.37.3.3 of TS 23.501 [2].

If selected PSA UPF supports Nupf\_EventExposure service, the SMF should include DNN and S-NSSAI in the N4 Session Establishment procedure.

NOTE 10: If SMF does not provide DNN and S-NSSAI to UPF it could result in rejections for the Nupf\_EventExposure\_Subscribe service operations, unless UPF is configured with a DNN and S-NSSAI for a specific IP address range.

10b. The UPF acknowledges by sending an N4 Session Establishment/Modification Response.

If the SMF indicates in step 10a that IP address/prefix allocation is to be performed by the UPF then this response contains the requested IP address/prefix. The requested CN Tunnel Info is provided to SMF in this step. If SMF indicated the UPF to perform packet duplication and elimination for the QoS Flow in step 10a, two CN Tunnel Info are allocated by the UPF and provided to the SMF. If SMF decides to insert two I-UPFs between the PSA UPF and the NG-RAN for redundant transmission as described in clause 5.33.1.2 of TS 23.501 [2], CN Tunnel Info of two I-UPFs and the UPF (PSA) are allocated by the UPFs and provided to the SMF. The UPF indicates the SMF that one CN Tunnel Info is used as the redundancy tunnel of the PDU session as described in clause 5.33.2.2 of TS 23.501 [2].

If SMF requested UPF to provide a port number then UPF includes the port number and user-plane Node ID in the response according to TS 23.501 [2]. To support integration with IEEE TSN, the user-plane node ID is Bridge ID. To support integration with IETF DetNet, the user-plane node ID can be Router ID. Besides the network instance, the SMF may also provide DNN/S-NSSAI for the UPF to respond with user-plane Node ID based on pre-configuration information.

If multiple UPFs are selected for the PDU Session, the SMF initiate N4 Session Establishment/Modification procedure with each UPF of the PDU Session in this step.

NOTE 10: If the PCF has subscribed to the UE IP address change Policy Control Trigger (as specified in clause 6.1.3.5 of TS 23.503 [20]) then the SMF notifies the PCF about the IP address/prefix allocated by the UPF. This is not shown in figure 4.3.2.2.1-1.

If interworking with TSN deployed in the transport network is supported and the UPF supports CN-TL and received a TL-Container with a get-request from the SMF/CUC in step 10a (see clause 4.4.8 of TS 23.501 [2]), the UPF/CN-TL includes a TL-Container with a get-response in the N4 Session Establishment/Modification response, as described in clause 5.28a.2 of TS 23.501 [2]. The SMF/CUC stores the information provided in the get-response.

11. SMF to AMF: Namf\_Communication\_N1N2MessageTransfer (PDU Session ID, N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), CN Tunnel Info, S-NSSAI from the Allowed NSSAI or Partially Allowed NSSAI, Session-AMBR, PDU Session Type, User Plane Security Enforcement information, UE Integrity Protection Maximum Data Rate, RSN, PDU Session Pair ID, TL-Container), N1 SM container (PDU Session Establishment Accept ([QoS Rule(s) and associated UL Protocol Description(s) (if available), QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s)], selected SSC mode, S-NSSAI(s), UE Requested DNN, allocated IPv4 address, interface identifier, Session-AMBR, selected PDU Session Type, [Reflective QoS Timer] (if available), [P-CSCF address(es)], [Control Plane Only indicator], [Header Compression Configuration], [Always-on PDU Session Granted], [Small Data Rate Control parameters], [Small Data Rate Control Status], [Serving PLMN Rate Control], [PVS FQDN(s) and/or PVS IP address(es)], [Non-3GPP QoS Assistance Information Container]))). If multiple UPFs are used for the PDU Session, the CN Tunnel Info contains tunnel information related with the UPFs that terminate N3.

The SMF may provide the SMF derived CN assisted RAN parameters tuning to the AMF by invoking Nsmf\_PDUSession\_SMContextStatusNotify (SMF derived CN assisted RAN parameters tuning) service. The AMF stores the SMF derived CN assisted RAN parameters tuning in the associated PDU Session context for this UE.

The N2 SM information carries information that the AMF shall forward to the (R)AN which includes:

- The CN Tunnel Info corresponds to the Core Network address(es) of the N3 tunnel corresponding to the PDU Session. If two CN Tunnel Info are included for the PDU session for redundant transmission, the SMF also indicates the NG-RAN that one of the CN Tunnel Info used as the redundancy tunnel of the PDU session as described in clause 5.33.2.2 of TS 23.501 [2].

- One or multiple QoS profiles and the corresponding QFIs can be provided to the (R)AN. This is further described in clause 5.7 of TS 23.501 [2]. The SMF may indicate for each QoS Flow whether redundant transmission shall be performed by a corresponding redundant transmission indicator.

- The PDU Session ID may be used by AN signalling with the UE to indicate to the UE the association between (R)AN resources and a PDU Session for the UE.

- A PDU Session is associated to an S-NSSAI of the HPLMN and if applicable, to an S-NSSAI of the VPLMN and a DNN. The S-NSSAI provided to the (R)AN, is the S-NSSAI with the value for the Serving PLMN (i.e. the HPLMN S-NSSAI or, in LBO roaming case, the VPLMN S-NSSAI). When Alternative S-NSSAI is received from AMF in step 3, the S-NSSAI provided to the (R)AN is the Alternative S-NSSAI.

- User Plane Security Enforcement information is determined by the SMF as described in clause 5.10.3 of TS 23.501 [2].

- If the User Plane Security Enforcement information indicates that Integrity Protection is "Preferred" or "Required", the SMF also includes the UE Integrity Protection Maximum Data Rate as received in the PDU Session Establishment Request.

- The use of the RSN parameter and the PDU Session Pair ID by NG-RAN are described in clause 5.33.2.1 of TS 23.501 [2].

- For each QoS Flow, the SMF may at most request one of the following to the NG-RAN:

- ECN marking for L4S at NG-RAN in the case of ECN marking for L4S in RAN as described in clause 5.37.3 of TS 23.501 [2]; or

- Congestion information monitoring as described in clauses 5.45.3 and 5.37.4 of TS 23.501 [2]; or

- provide information for ECN marking for L4S at UPF in the case of ECN marking for L4S by PSA UPF as described in clause 5.37.3 of TS 23.501 [2].

- TL-Container as described in clause 5.28a.2 of TS 23.501 [2]. If interworking with TSN deployed in the transport network is supported and the NG-RAN supports AN-TL (see clause 4.4.8 of TS 23.501 [2]), the SMF includes a TL-Container with a get-request to the N2 SM information, as described in clause 5.28a.2 of TS 23.501 [2].

The N1 SM container contains the PDU Session Establishment Accept that the AMF shall provide to the UE. If the UE requested P-CSCF discovery then the message shall also include the P-CSCF IP address(es) as determined by the SMF and as described in clause 5.16.3.4 of TS 23.501 [2]. The PDU Session Establishment Accept includes S-NSSAI from the Allowed NSSAI or Partially Allowed NSSAI. The S-NSSAI value of the Alternative S-NSSAI is included in the PDU session Establishment Accept if the SMF has received the Alternative S-NSSAI from the AMF. For LBO roaming scenario, the PDU Session Establishment Accept includes the S-NSSAI from the Allowed NSSAI or Partially Allowed NSSAI for the VPLMN and also it includes the corresponding S-NSSAI of the HPLMN from the Mapping Of Allowed NSSAI or Mapping Of Partially Allowed NSSAI that SMF received in step 3. If the SMF has received the VPLMN Alternative S-NSSAI from the AMF, the PDU Session Establishment Accept includes the VPLMN Alternative S-NSSAI. If the SMF has received the HPLMN Alternative S-NSSAI from the AMF, the PDU Session Establishment Accept includes the HPLMN Alternative S-NSSAI. If the PCF, based on the local configuration, provides the PCC rules with Protocol Descriptions for UL in step 7b or step 9, the SMF may additionally provide the Protocol Description for UL with the associated QoS rule as described in clause 5.37.5.1 of TS 23.501 [2].

If the PDU Session being established was requested to be an always-on PDU Session, the SMF shall indicate whether the request is accepted by including an Always-on PDU Session Granted indication in the PDU Session Establishment Accept message. If the PDU Session being established was not requested to be an always-on PDU Session but the SMF determines that the PDU Session needs to be established as an always-on PDU Session, the SMF shall include an Always-on PDU Session Granted indication in the PDU Session Establishment Accept message indicating that the PDU session is an always-on PDU Session.

If Control Plane CIoT 5GS Optimisation is enabled for this PDU session, the N2 SM information is not included in this step. If Control Plane CIoT 5GS optimisation is enabled for this PDU session and the UE has sent the Header Compression Configuration in the PDU Session Establishment Request and the SMF supports the header compression parameters, the SMF shall include the Header Compression Configuration in the PDU Session Establishment Accept message. If the UE has included Header Compression context parameters in Header Compression Configuration in the PDU Session Establishment Request, the SMF shall establish the header compression context and may acknowledge the Header Compression context parameters. If the header compression context is not established during the PDU Session Establishment procedure, before using the compressed format for sending the data, the UE and the SMF need to establish the header compression context based on the Header Compression Configuration. If the SMF has received the Control Plane Only Indicator in step 3, the SMF shall include the Control Plane Only Indicator in the PDU Session Establishment Accept message. The SMF shall indicate the use of Control Plane only on its CDR. If the Small Data Rate Control is configured in the SMF, the SMF shall also include Small Data Rate Control parameters and the Small Data Rate Control Status (if received from the AMF) in the PDU Session Establishment Accept message as described in clause 5.31.14.3 of TS 23.501 [2]. If the Serving PLMN intends to enforce Serving PLMN Rate Control (see clause 5.31.14.2 of TS 23.501 [2]) for this PDU session then the SMF shall include the Serving PLMN Rate Control parameters in the PDU Session Establishment Accept message. The UE shall store and use Serving PLMN Rate Control parameters as the maximum allowed limit of uplink control plane user data.

If the UE indicates the support of RDS in the PCO in the PDU Session Establishment Request and RDS is enabled for the PDU Session, the SMF shall inform the UE that RDS is enabled in the PCO in the PDU Session Establishment Accept (see clause 5.31.6 of TS 23.501 [2]).

If the NIDD parameters (e.g. maximum packet size) were received from NEF during the SMF-NEF Connection Establishment procedure in step 10, the SMF shall inform the UE of the NIDD parameters in the PCO in the PDU Session Establishment Accept (see clause 5.31.5 of TS 23.501 [2]).

If the UE indicated in the PCO that it supports the ability to receive ECS address(es) via NAS, the SMF may provide the ECS Address Configuration Information (as described in clause 6.5.2 of TS 23.548 [74]) to the UE in the PCO. The SMF may derive the ECS Address Configuration Information based on local configuration and/or UE subscription information. In non-roaming scenarios, the SMF may also derive the ECS Address Configuration Information based on the UE's location.

If the UE indicated in the PCO that it supports the EDC functionality, the SMF may indicate to the UE either that the use of the EDC functionality is allowed for the PDU Session or that the use of the EDC functionality is required for the PDU Session (see clause 5.2.1 of TS 23.548 [74]).

Multiple QoS Rules, QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with those QoS rule(s) and QoS Profiles may be included in the PDU Session Establishment Accept within the N1 SM and in the N2 SM information.

The Namf\_Communication\_N1N2MessageTransfer contains the PDU Session ID allowing the AMF to know which access towards the UE to use.

If the PDU session establishment failed anywhere between step 5 and step 11, then the Namf\_Communication\_N1N2MessageTransfer request shall include the N1 SM container with a PDU Session Establishment Reject message (see clause 8.3.3 of TS 24.501 [25]) and shall not include any N2 SM container. The (R)AN sends the NAS message containing the PDU Session Establishment Reject to the UE. In this case, steps 12-17 are skipped.

Based on the S-NSSAI and DNN for PIN, the SMF may provide the UE with per QoS-flow Non-3GPP QoS Assistance Information in the N1 SM container as specified in clause 5.44.3.3 of TS 23.501 [2].

12. AMF to (R)AN: N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)), [CN assisted RAN parameters tuning]). If the N2 SM information is not included in the step 11, an N2 Downlink NAS Transport message is used instead.

The AMF sends the NAS message containing PDU Session ID and PDU Session Establishment Accept targeted to the UE and the N2 SM information received from the SMF within the N2 PDU Session Request to the (R)AN.

If the SMF derived CN assisted RAN parameters tuning are stored for the activated PDU Session(s), the AMF may derive updated CN assisted RAN parameters tuning and provide them the (R)AN.

13. (R)AN to UE: The (R)AN may issue AN specific signalling exchange with the UE that is related with the information received from SMF. For example, in the case of a NG-RAN, an RRC Connection Reconfiguration may take place with the UE establishing the necessary NG-RAN resources related to the QoS Rules for the PDU Session request received in step 12.

(R)AN also allocates (R)AN Tunnel Info for the PDU Session. In the case of Dual Connectivity, the Master RAN node may assign some (zero or more) QFIs to be setup to a Master RAN node and others to the Secondary RAN node. The AN Tunnel Info includes a tunnel endpoint for each involved (R)AN node and the QFIs assigned to each tunnel endpoint. A QFI can be assigned to either the Master RAN node or the Secondary RAN node and not to both.

If the (R)AN receives two CN Tunnel Info for a PDU session in step 12 for redundant transmission, (R)AN also allocates two AN Tunnel Info correspondingly and indicate to SMF one of the AN Tunnel Info is used as the redundancy tunnel of the PDU session as described in clause 5.33.2.2 of TS 23.501 [2].

(R)AN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) provided in step 12 to the UE. (R)AN shall only provide the NAS message to the UE if the AN specific signalling exchange with the UE includes the (R)AN resource additions associated to the received N2 command.

If MICO mode is active and the NAS message Request Type in step 1 indicated "Emergency Request", then the UE and the AMF shall locally deactivate MICO mode.

If the N2 SM information is not included in the step 11, then the following steps 14 to 16b and step 17 are omitted.

If the UE is running a slice deregistration inactivity timer for the S-NSSAI of the established PDU Session and the timer is associated with the Access Type over which the PDU Session Establishment Request was received, the UE stops the timer as described in clause 5.15.15 of TS 23.501 [2].

14. (R)AN to AMF: N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification, TL-Container, established QoS Flows status (active/not active) (for one of the following: congestion information monitoring, ECN marking for L4S at PSA UPF, ECN marking for L4S at NG-RAN), PDU Set Based Handling Support Indication)).

The AN Tunnel Info corresponds to the Access Network address of the N3 tunnel corresponding to the PDU Session.

The (R)AN may reject the addition or modification of a QoS Flow, e.g. due to handling of the UE-Slice-MBR as described in clause 5.7.1.10 of TS 23.501 [2]. If the (R)AN rejects QFI(s) the SMF is responsible of updating the QoS rules and QoS Flow level QoS parameters associated to the rejected QoS Flow(s) in the UE accordingly.

The NG-RAN rejects the establishment of UP resources for the PDU Session when it cannot fulfil User Plane Security Enforcement information with a value of Required. The NG-RAN notifies the SMF when it cannot fulfil a User Plane Security Enforcement with a value of Preferred.

If the NG-RAN cannot establish redundant user plane for the PDU Session as indicated by the RSN parameter and PDU Session Pair ID, the NG-RAN takes the decision on whether to reject the establishment of RAN resources for the PDU Session based on local policies as described in TS 23.501 [2].

If interworking with TSN deployed in the transport network is supported and the NG-RAN supports AN-TL and received a TL-Container with a get-request from the SMF/CUC in step 12 (see clause 4.4.8 of TS 23.501 [2]), the NG-RAN/AN-TL includes a TL-Container with a get-response to the N2 SM information, as described in clause 5.28a.2 of TS 23.501 [2].

NG-RAN includes the PDU Set Based Handling Support Indication in N2 SM information as defined in clause 5.37.5.3 of TS 23.501 [2].

15. AMF to SMF: Nsmf\_PDUSession\_UpdateSMContext Request (SM Context ID, N2 SM information, Request Type).

The AMF forwards the N2 SM information received from (R)AN to the SMF.

If the list of rejected QFI(s) is included in N2 SM information, the SMF shall release the rejected QFI(s) associated QoS profiles.

If the N2 SM information indicates failure of user plane resource setup, the SMF shall reject the PDU session establishment by including a N1 SM container with a PDU Session Establishment Reject message (see clause 8.3.3 of TS 24.501 [25]) in the Nsmf\_PDUSession\_UpdateSMContext Response in step 17. Step 16 is skipped in this case and instead the SMF releases the N4 Session with UPF.

If the User Plane Enforcement Policy Notification in the N2 SM information indicates that no user plane resources could be established and the User Plane Enforcement Policy indicated "required" as described in clause 5.10.3 of TS 23.501 [2], the SMF shall reject the PDU session establishment by including a N1 SM container with a PDU Session Establishment Reject message (see clause 8.3.3 of TS 24.501 [25]) in the Nsmf\_PDUSession\_UpdateSMContext Response in step 17. Step 16 is skipped in this case.

If the N2 SM information includes a TL-Container with a get-response as described in clause 5.28a.2 of TS 23.501 [2], the SMF/CUC stores the information provided in the get-response.

16a. The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Info to the UPF as well as the corresponding forwarding rules.

If SMF decides to perform redundant transmission for one or more QoS Flows of the PDU, the SMF also indicates the UPF to perform packet duplication for the QoS Flow(s) in downlink direction by forwarding rules.

In the case of redundant transmission with two I-UPFs for one or more QoS Flows of the PDU, the SMF provides AN Tunnel Info to two I-UPFs and also indicates the UPF (PSA) to perform packet duplication for the QoS Flow(s) in downlink direction by forwarding rules. The SMF also provides the UL Tunnel Info of the UPF (PSA) to the two I-UPFs and the DL Tunnel Info of the two I-UPFs to the UPF (PSA).

If the N2 SM information includes the PDU Set Based Handling Support Indication, SMF configures PSA UPF to perform PDU Set information marking for the QoS flow as defined in clause 5.37.5.3 of TS 23.501 [2].

NOTE 11: If the PDU Session Establishment Request was due to mobility between 3GPP and non-3GPP access or mobility from EPC, the downlink data path is switched towards the target access in this step.

16b. The UPF provides an N4 Session Modification Response to the SMF.

If multiple UPFs are used in the PDU Session, the UPF in step 16 refers to the UPF terminating N3.

After this step, the UPF delivers any down-link packets to the UE that may have been buffered for this PDU Session.

16c. If Request Type in step 3 indicates neither "Emergency Request" nor "Existing Emergency PDU Session" and if the SMF has not yet registered for this PDU Session, then the SMF registers with the UDM using Nudm\_UECM\_Registration (SUPI, DNN, S-NSSAI of HPLMN, PDU Session ID, SMF Identity, Serving Node PLMN ID, [NID], PCF ID) for a given PDU Session. As a result, the UDM stores following information: SUPI, SMF identity and the associated DNN, S-NSSAI of HPLMN, PDU Session ID, PCF ID and Serving Network (PLMN ID, [NID], see clause 5.18 of TS 23.501 [2]). The UDM may further store this information in UDR by Nudr\_DM\_Update (SUPI, Subscription Data, UE context in SMF data). If the UDM has existing applicable event exposure subscriptions for events detected in SMF for this UE or any of the groups this UE belongs to (possibly retrieved from UDR), UDM invokes the Nsmf\_EventExposure\_Subscribe service for creating the event exposure subscriptions. If the SMF received Alternative S-NSSAI in step 3, the S-NSSAI provided to the UDM is the replaced S-NSSAI.

If the Request Type received in step 3 indicates "Emergency Request":

- For an authenticated non-roaming UE, based on operator configuration (e.g. related with whether the operator uses a fixed SMF for Emergency calls, etc.), the SMF may register in the UDM using Nudm\_UECM\_Registration (SUPI, PDU Session ID, SMF identity, Indication of Emergency Services) for a given PDU Session that is applicable for emergency services. As a result, the UDM shall store the applicable PDU Session for Emergency services.

- For an unauthenticated UE or a roaming UE, the SMF shall not register in the UDM for a given PDU Session.

17. SMF to AMF: Nsmf\_PDUSession\_UpdateSMContext Response (Cause).

The SMF may subscribe to the UE mobility event notification from the AMF (e.g. location reporting, UE moving into or out of Area Of Interest), after this step by invoking Namf\_EventExposure\_Subscribe service operation as specified in clause 5.2.2.3.2. For LADN, the SMF subscribes to the UE moving into or out of LADN service area event notification by providing the LADN DNN as an indicator for the Area Of Interest (see clause 5.6.5 and 5.6.11 of TS 23.501 [2]).

If SMF receives the indication in step 3 that "the PDU Session is subject to LADN per LADN DNN and S-NSSAI", the SMF subscribes to the UE moving into or out of LADN service area event notification by providing the LADN DNN and S-NSSAI as an indicator for the Area Of Interest.

If SMF receives the indication in step 3 that the PDU Session is subject to area restriction for the S-NSSAI, the SMF subscribe to "UE mobility event notification" event for reporting UE presence in Area of Interest by providing the S-NSSAI as an indicator for the Area Of Interest (see clauses 5.6.11 and 5.3.4.4 of TS 23.501 [2]).

After this step, the AMF forwards relevant events subscribed by the SMF.

For those scenarios where the PCFs serving the AMF and the SMF are different, the SMF informs the AMF of the NWDAF ID(s) used for UE related Analytics and corresponding Analytics ID(s).

18. [Conditional] SMF to AMF: Nsmf\_PDUSession\_SMContextStatusNotify (Release)

If during the procedure, any time after step 5, the PDU Session establishment is not successful, the SMF informs the AMF by invoking Nsmf\_PDUSession\_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU Session address if allocated (e.g. IP address) and releases the association with PCF, if any. In this case, step 19 is skipped.

For a PDU Session for non-roaming subscribers, if the S-NSSAI of the PDU Session is subject to network slice usage control and there is no other PDU Session using the S-NSSAI over the same Access Type, the AMF starts the slice deregistration inactivity timer for the S-NSSAI over this Access Type as described in clause 5.15.15.3 of TS 23.501 [2].

19. SMF to UE: In the case of PDU Session Type IPv6 or IPv4v6, the SMF generates an IPv6 Router Advertisement and sends it to the UE. If Control Plane CIoT 5GS Optimisation is enabled for this PDU Session the SMF sends the IPv6 Router Advertisement via the AMF for transmission to the UE using the Mobile Terminated Data Transport in Control Plane CIoT 5GS Optimisation procedures (see clause 4.24.2), otherwise the SMF sends the IPv6 Router Advertisement via N4 and the UPF.

20. When the trigger for 5GS Bridge/Router information available is armed, then the SMF may initiate the SM Policy Association Modification as described in clause 4.16.5.1.

If the UE has indicated support of transferring Port Management Information Containers, then SMF informs PCF that 5GS Bridge/Router information is available. SMF provides the 5GS Bridge/Router information (e.g. 5GS user-plane Node ID, port number for the PDU session, MAC address of the DS-TT Ethernet port for Ethernet PDU Session type, UE IP address for IP PDU Session type and UE-DS-TT Residence Time (if available) as provided by the UE) to PCF. In the case of Deterministic Networking, the SMF may also provide the MTU size for IPv4 or the MTU size for IPv6. If the SMF received a Port Management Information Container from either the UE or the UPF, then the SMF provides the Port Management Information Container and port number of the related port to the PCF as described in clause 5.28.3.2 of TS 23.501 [2].

If the SMF has received User Plane Node Management Information from the UPF, then the SMF provides the User Plane Node Management Information Container to the PCF as part of 5GS Bridge/Router information and as described in clause 5.28.3.2 of TS 23.501 [2].

To support IEEE TSN, the TSN AF calculates the bridge delay for each port pair, i.e. composed of DS-TT Ethernet port and NW-TT Ethernet port, using the UE-DS-TT Residence Time for all NW-TT Ethernet port(s) serving the 5GS Bridge indicated by the 5GS user-plane Node ID. Additionally, the TSN AF determines the 5GS bridge delay for port pair composed of two DS-TT ports connecting to the same 5GS Bridge as sum of bridge delays related to PDU Sessions of the two DS-TT ports.

21. If the PDU Session establishment failed after step 4, the SMF shall perform the following:

The SMF unsubscribes to the modifications of Session Management Subscription data for the corresponding (SUPI, DNN, S-NSSAI of the HPLMN), using Nudm\_SDM\_Unsubscribe (SUPI, Session Management Subscription data, DNN, S-NSSAI of the HPLMN), if the SMF is no more handling a PDU Session of the UE for this (DNN, S-NSSAI of the HPLMN). The UDM may unsubscribe to the modification notification from UDR by Nudr\_DM\_Unsubscribe (SUPI, Subscription Data, Session Management Subscription data, S-NSSAI of the HPLMN, DNN).

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

#### 4.17.6.1 General

This clause describes the provisioning of available UPFs in SMF using the NRF as documented in clause 6.3.3 of TS 23.501 [2].

This optional node-level step takes place prior to selecting the UPF for PDU Sessions and may be followed by N4 Node Level procedures defined in clause 4.4.3 where the UPF and the SMF exchange information such as the support of optional functionalities and capabilities.

As an option, UPF(s) may register in the NRF. This registration phase uses the Nnrf\_NFManagement\_NFRegister operation and hence does not use N4.

For the purpose of SMF provisioning of available UPFs, the SMF uses the Nnrf\_NFManagement\_NFStatusSubscribe, Nnrf\_NFManagement\_NFStatusNotify and Nnrf\_NFDiscovery services to learn about available UPFs.

NOTE 1: The protocol used by UPF to interact with NRF is described in TS 29.510 [37]

UPFs may be associated with UPF Provisioning Information in the NRF. The UPF Provisioning Information consists of:

- a list of (S-NSSAI, DNN);

- UE IPv4 Address Ranges and/or IPv6 Prefix Range(s) per (S-NSSAI, DNN); and

NOTE 2: The above information can be used by the SMF for UPF selection when static IP address/prefix allocation is required for a UE.

- a SMF Area Identity the UPF can serve. The SMF Area Identity allows limiting the SMF provisioning of UPF(s) using NRF to those UPF(s) associated with a certain SMF Area Identity. This can e.g. be used if an SMF is only allowed to control UPF(s) configured in NRF as belonging to a certain SMF Area Identity.

- the supported ATSSS steering functionality, i.e. whether MPTCP functionality or ATSSS-LL functionality or MPQUIC functionality, or any combination of them is supported.

- the supported UPF event exposure service and supported Event IDs, e.g. local notification of QoS Monitoring to AF or e.g. events for data collection to NWDAF by Nupf\_EventExposure\_Notify.

- the supported functionality associated with high data rate low latency services, eXtended Reality (XR) and interactive media services, specified in clause 5.37 (for example, ECN marking for L4S, specified in clause 5.37.3, PDU Set Marking, specified in clause 5.37.5, UE power saving management, specified in clause 5.37.8).

- additional supported functionalities, e.g. NAT information exposure functionality and the packet inspection functionality, see clause 6.2.3 of TS 23.501 [2].

The SMF Area Identity and UE IPv4 Address Ranges and/or IPv6 Prefix Range(s) are optional in the UPF Provisioning Information.

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

##### 5.2.3.3.1 General

Subscription data types used in the Nudm\_SubscriberDataManagement Service are defined in Table 5.2.3.3.1-1 below.

Table 5.2.3.3.1-1: UE Subscription data types

| Subscription data type | Field | Description |
| --- | --- | --- |
| Access and Mobility Subscription data (data needed for UE | GPSI List | List of the GPSI (Generic Public Subscription Identifier) used both inside and outside of the 3GPP system to address a 3GPP subscription (see NOTE 9). |
| Registration and Mobility Management) | Internal Group ID-list | List of the subscribed internal group(s) that the UE belongs to. |
|  | Subscribed UE-AMBR | The maximum aggregated uplink and downlink MBRs to be shared across all Non-GBR QoS Flows according to the subscription of the user. |
|  | Subscribed UE-Slice-MBR(s) | List of maximum aggregated uplink and downlink MBRs to be shared across all GBR and Non-GBR QoS Flows related to the same S-NSSAI according to the subscription of the user. There is a single uplink and a single downlink value per S-NSSAI. |
|  | Subscribed S-NSSAIs | The Network Slices that the UE subscribes to. In the roaming case, it indicates the subscribed Network Slices applicable to the Serving PLMN (NOTE 11).  For a subscribed S-NSSAI subject to NSAC for the registered number of UE, the applicable NSAC admission mode is included as described in clause 4.2.11.5.2. |
|  | Default S-NSSAIs | The Subscribed S-NSSAIs marked as default S-NSSAI. In the roaming case, only those applicable to the Serving PLMN (NOTE 12). |
|  | Slice Usage Policy information | Includes:  - indication the S-NSSAI is on demand; and  - slice deregistration inactivity timer value.  The AMF uses this information as described in clause 5.15.15 of TS 23.501 [2].  (NOTE 22) |
|  | S-NSSAIs subject to Network Slice-Specific Authentication and Authorization | The Subscribed S-NSSAIs marked as subject to NSSAA. When present, the GPSI list shall include at least one GPSI. |
|  | Network Slice Simultaneous Registration Group Information | Optionally, for each S-NSSAI in the Subscribed S-NSSAIs, one or more value of Network Slice Simultaneous Registration Group(s) (NOTE 11) associated with the S-NSSAI. |
|  | Network Slice validity time information | Optionally, if the Subscribed S-NSSAI is temporarily available network slice, one validity time is associated with this S-NSSAI. |
|  | UE Usage Type | As defined in clause 5.15.7.2 of TS 23.501 [2]. |
|  | RAT restriction | 3GPP and non-3GPP Radio Access Technology(ies) not allowed the UE to access. |
|  | Forbidden area | Defines areas in which the UE is not permitted to initiate any communication with the network. |
|  | Service Area Restriction | Indicates Allowed Areas in which the UE is permitted to initiate communication with the network and Non-allowed areas in which the UE and the network are not allowed to initiate Service Request or SM signalling to obtain user services. |
|  | Core Network type restriction | Defines whether UE is allowed to connect to 5GC and/or EPC for this PLMN. |
|  | CAG information | The CAG information includes Allowed CAG list and optionally an indication whether the UE is only allowed to access 5GS via CAG cells and each entry in the Allowed CAG list may also be associated with time validity information as defined in clause 5.30.3 of TS 23.501 [2]. |
|  | CAG information Subscription Change Indication | When present, indicates to the serving AMF that the CAG information in the subscription data changed and the UE must be updated. |
|  | RFSP Index | An index to specific RRM configuration in the NG-RAN. |
|  | Subscribed Periodic Registration Timer | Indicates a subscribed Periodic Registration Timer value, which may be influenced by e.g. network configuration parameter as specified in clause 4.15.6.3a. |
|  | Subscribed Active Time | Indicates a subscribed active time value, which may be influenced by e.g. network configuration parameter as specified in clause 4.15.6.3a. |
|  | MPS priority | Indicates the user is subscribed to MPS as indicated in clause 5.16.5 of TS 23.501 [2]. |
|  | MCX priority | Indicates the user is subscribed to MCX as indicated in clause 5.16.6 of TS 23.501 [2]. |
|  | AMF-Associated Expected UE Behaviour parameters | Information on expected UE movement and communication characteristics. See clause 4.15.6.3 |
|  | Steering of Roaming | List of preferred PLMN/access technology combinations and/or Credentials Holder controlled prioritized lists of preferred SNPNs and GINs and/or Credentials Holder controlled prioritized lists of preferred SNPNs and GINs for accessing Localized Services (see NOTE 21) or HPLMN/Credentials Holder indication that no change of the above list(s) stored in the UE is needed (see NOTE 3).  Optionally includes an indication that the UDM requests an acknowledgement of the reception of this information from the UE. |
|  | SoR Update Indicator for Initial Registration | An indication whether the UDM requests the AMF to retrieve SoR information when the UE performs Registration with NAS Registration Type "Initial Registration". |
|  | SoR Update Indicator for Emergency Registration | An indication whether the UDM requests the AMF to retrieve SoR information when the UE performs Registration with NAS Registration Type "Emergency Registration". |
|  | Network Slicing Subscription Change Indicator | When present, indicates to the serving AMF that the subscription data for network slicing changed and the UE configuration must be updated. |
|  | Provide the UE with the full set of subscribed S-NSSAIs | Indicates the AMF to provide the UE with the full set of subscribed S-NSSAIs even if they do not share a common NSSRG. |
|  | Tracing Requirements | Trace requirements about a UE (e.g. trace reference, address of the Trace Collection Entity, etc.) is defined in TS 32.421 [39]. |
|  | Inclusion of NSSAI in RRC Connection Establishment Allowed | When present, it is used to indicate that the UE is allowed to include NSSAI in the RRC connection Establishment in clear text for 3GPP access. |
|  | Service Gap Time | Used to set the Service Gap timer for Service Gap Control (see clause 5.31.16 of TS 23.501 [2]). |
|  | Subscribed DNN list | List of the subscribed DNNs for the UE (NOTE 1). Used to determine the list of LADN available to the UE as defined in clause 5.6.5 of TS 23.501 [2]. |
|  | LADN Service Area | List of Tracking Areas configured per DNN and S-NSSAI within which UE is permitted to initiate Service Request or SM signalling. |
|  | UDM Update Data | Includes a set of parameters see clause 4.20.1 for parameters possible to deliver) to be delivered from UDM to the UE via NAS signalling as defined in clause 4.20 (NOTE 3).  Optionally includes an indication that the UDM requests an acknowledgement of the reception of this information from the UE and an indication for the UE to re-register. |
|  | NB-IoT UE priority | Numerical value used by the NG-RAN to prioritise between UEs accessing via NB-IoT. |
|  | Enhanced Coverage Restriction | Specifies whether CE mode B is restricted for the UE, or both CE mode A and CE mode B are restricted for the UE, or both CE mode A and CE mode B are not restricted for the UE. |
|  | NB-IoT Enhanced Coverage Restriction | Indicates whether Enhanced Coverage for NB-IoT UEs is restricted or not. |
|  | IAB-Operation allowed | Indicates that the subscriber is allowed for IAB-operation as specified in clause 5.35.2 of TS 23.501 [2]. |
|  | MBSR Operation allowed | Indicates the subscriber is allowed for MBSR operation as specified in clause 5.35A.4 of TS 23.501 [2]. If present, additional location information (i.e. a list of TAIs or Area Codes that can be interpreted by AMF into TAIs ) and/or time information (including one or more time windows, and/or one or more recurring time periods) may also be present to restrict the MBSR operation to be within the location and time provided. |
|  | Charging Characteristics | It contains the Charging Characteristics as defined in Annex A of TS 32.256 [71].  This information, when provided, shall override any corresponding predefined information at the AMF. |
|  | Extended idle mode DRX cycle length | Indicates a subscribed extended idle mode DRX cycle length value. |
|  | PCF Selection Assistance info | list of combination of DNN and S-NSSAI that indicates that the same PCF needs to be selected for AM Policy Control and SM Policy Control (NOTE 10). |
|  | AerialUESubscriptionInfo | Aerial UE Subscription Information. It contains an Indication on whether Aerial service for the UE is allowed or not. |
|  | 5G Access Stratum-based Time Synchronization Service Data | Includes the Access Stratum Time Synchronization Service Authorization to indicate whether the UE should be provisioned with 5G system internal clock timing information over access stratum.  Optionally includes an Uu time synchronization error budget.  Optionally includes one or more periods of start and stop times defining the times when the UE should be provisioned with 5G system internal clock timing information.  Optionally includes a Time Synchronization Coverage Area comprising a list of TAs where the UE shall be provisioned with 5G system internal clock timing information (NOTE 19).  Optionally includes a clock quality detail level to indicate whether and which clock quality information to provide to the UE. It comprises one of the following values: clock quality metrics or acceptable/not acceptable indication.  Optionally includes the clock quality acceptance criteria for the UE. It may be defined based on one or more of the following attributes: time source, traceability to UTC and to GNSS, synchronization state, clock accuracy, frequency stability. |
|  | Routing Indicator | Routing Indicator assigned to the SUPI. |
|  | ODB for Packet services | Operator Determined Barring for Packet Oriented Services. See TS 23.015 [90] and TS 29.503 [52] for the handling of ODB for Packet service parameter. |
|  | QMC Configuration information | The content of QMC Configuration information (e.g. QoE reference, QoE collection entity address, etc.) is defined in TS 28.405 [92]. |
|  | NCR-Operation allowed | Indicates that the subscriber is allowed for NCR-operation as specified in clause 5.xx of TS 23.501 [2]. |
|  | AM Policy Association indicator | Indicates whether the AM Policy Association is "enabled", "disabled". |
|  | UE Policy Association indicator | Indicates whether the UE Policy Association is "enabled" or "disabled". |
| Slice Selection Subscription data (data needed for | Subscribed S-NSSAIs | The Network Slices that the UE subscribes to. In roaming case, it indicates the subscribed network slices applicable to the serving PLMN (NOTE 11). |
| Slice Selection as described in clause 4.2.2.2.3 and | Default S-NSSAIs | The Subscribed S-NSSAIs marked as default S-NSSAI. In the roaming case, only those applicable to the Serving PLMN (NOTE 12). |
| in clause 4.11.0a.5) | S-NSSAIs subject to Network Slice-Specific Authentication and Authorization | The Subscribed S-NSSAIs marked as subject to NSSAA. |
|  | Network Slice Simultaneous Registration Group (NSSRG) Information | Optionally, for each S-NSSAI in the Subscribed S-NSSAIs, the one or more value of Network Slice Simultaneous Registration Group(s) (NOTE 11) associated with the S-NSSAI. |
|  | Network Slice validity time information | Optionally, if the Subscribed S-NSSAI is temporarily available network slice, one validity time is associated with this S-NSSAI. |
| SMF Selection | SUPI | Key |
| Subscription data (data needed for SMF | **SMF Selection Subscription data contains one or more S-NSSAI level subscription data:** | |
| Selection as described | S-NSSAI | Indicates the value of the S-NSSAI. |
| in clause 6.3.2 of | Subscribed DNN list | List of the subscribed DNNs for the UE (NOTE 1). |
| TS 23.501 [2]) | Default DNN | The default DNN if the UE does not provide a DNN (NOTE 2). |
|  | DNN(s) subject to aerial services | List of DNNs that are used for aerial services (e.g. UAS operations or C2, etc.) as described in TS 23.256 [80]. (see NOTE 13). |
|  | LBO Roaming Information | Indicates whether LBO roaming is allowed per DNN, or per (S-NSSAI, subscribed DNN). (NOTE 16) |
|  | HR-SBO allowed indication | Indicates whether Session Breakout for HR Session in VPLMN is allowed per DNN, or per (S-NSSAI, subscribed DNN).  (NOTE 17) |
|  | Interworking with EPS indication list | Indicates whether EPS interworking is supported per (S-NSSAI, subscribed DNN). |
|  | Same SMF for Multiple PDU Sessions to the same DNN and S-NSSAI | Indication whether the same SMF for multiple PDU Sessions to the same DNN and S-NSSAI is required. |
|  | Invoke NEF indication | When present, indicates, per S-NSSAI and per DNN, that NEF based infrequent small data transfer shall be used for the PDU Session (see NOTE 8). |
|  | SMF information for static IP address/prefix | When static IP address/prefix is used, this may be used to indicate the associated SMF information per (S-NSSAI, DNN). |
|  | Additional parameters for SMF selection in target PLMN | Indicates the target PLMN identifier where SMF resource resides. |
| UE context in SMF | SUPI | Key. |
| data | PDU Session ID(s) | List of PDU Session ID(s) for the UE. |
|  | **For emergency PDU Session ID:** | |
|  | Emergency Information | The SMF+PGW-C FQDN for emergency session used for interworking with EPC. |
|  | **For each non-emergency PDU Session ID:** | |
|  | DNN | DNN for the PDU Session. |
|  | SMF | Allocated SMF for the PDU Session. Includes SMF IP Address and SMF NF Id. |
|  | SMF+PGW-C FQDN | The S5/S8 SMF+PGW-C FQDN used for interworking with EPS (see NOTE 5). |
|  | PCF ID | The PCF ID serving the PDU Session/PDN Connection. |
| SMS Management Subscription data (data needed by | SMS parameters | Indicates SMS parameters subscribed for SMS service such as SMS teleservice, SMS barring list |
| SMSF for SMSF Registration) | Trace Requirements | Trace requirements about a UE (e.g. trace reference, address of the Trace Collection Entity, etc.) is defined in TS 32.421 [39].  This information is only sent to a SMSF in HPLMN. |
|  | Routing Indicator | Routing Indicator assigned to the SUPI. |
| SMS Subscription data | SMS Subscription | Indicates subscription to any SMS delivery service over NAS irrespective of access type. |
| (data needed in AMF) |  |  |
| UE Context in SMSF data | SMSF Information | Indicates SMSF allocated for the UE, including SMSF address and SMSF NF ID. |
|  | Access Type | 3GPP or non-3GPP access through this SMSF |
| Session Management Subscription data (data needed for PDU | GPSI List | List of the GPSI (Generic Public Subscription Identifier) used both inside and outside of the 3GPP system to address a 3GPP subscription. |
| Session Establishment) | Internal Group ID-list | List of the subscribed internal group(s) that the UE belongs to. |
|  | Trace Requirements | Trace requirements about a UE (e.g. trace reference, address of the Trace Collection Entity, etc…) is defined in TS 32.421 [39].  This information is only sent to a SMF in the HPLMN or one of its equivalent PLMN(s). |
|  | Routing Indicator | Routing Indicator assigned to the SUPI. |
|  | **Session Management Subscription data contains one or more S-NSSAI level subscription data:** | |
|  | S-NSSAI | Indicates the value of the S-NSSAI.  For a subscribed S-NSSAI subject to NSAC for the established PDU session number, the applicable NSAC admission mode is included as described in clause 4.2.11.5.2. |
|  | Subscribed DNN list | List of the subscribed DNNs for the S-NSSAI (NOTE 1). |
|  | Slice Usage Policy information | Includes:  - indication the S-NSSAI is on demand; and  - PDU Session inactivity timer value.  The SMF uses this information as described in clause 5.15.15 of TS 23.501 [2].  (NOTE 22). |
|  | ODB for Packet services | Operator Determined Barring for Packet Oriented Services. See TS 23.015 [90] and TS 29.503 [52] for the handling of ODB for Packet service parameter. |
|  | **For each DNN in S-NSSAI level subscription data:** | |
|  | DNN | DNN for the PDU Session. |
|  | Aerial service indication | Indicates whether the DNN is used for aerial services (e.g. UAS operations or C2, etc.) as described in TS 23.256 [80]. |
|  | Framed Route information | Set of Framed Routes. A Framed Route refers to a range of IPv4 addresses / IPv6 Prefixes to associate with a PDU Session established on this (DNN, S-NSSAI).  See NOTE 4. |
|  | IP Index information | Information used for selecting how the UE IP address is to be allocated (see clause 5.8.2.2.1 of TS 23.501 [2]). |
|  | Allowed PDU Session Types | Indicates the allowed PDU Session Types (IPv4, IPv6, IPv4v6, Ethernet and Unstructured) for the DNN, S-NSSAI. See NOTE 6. |
|  | Default PDU Session Type | Indicates the default PDU Session Type for the DNN, S-NSSAI. |
|  | Allowed SSC modes | Indicates the allowed SSC modes for the DNN, S-NSSAI. |
|  | Default SSC mode | Indicate the default SSC mode for the DNN, S-NSSAI. |
|  | Interworking with EPS indication | Indicates whether interworking with EPS is supported for this DNN and S-NSSAI. |
|  | 5GS Subscribed QoS profile | The QoS Flow level QoS parameter values (5QI and ARP) for the DNN, S-NSSAI (see clause 5.7.2.7 of TS 23.501 [2]). |
|  | Charging Characteristics | It contains Charging Characteristics as defined in Annex A clause A.1 of TS 32.255 [45]. This information, when provided, shall override any corresponding predefined information at the SMF. |
|  | Subscribed-Session-AMBR | The maximum aggregated uplink and downlink MBRs to be shared across all Non-GBR QoS Flows in each PDU Session, which are established for the DNN, S-NSSAI. |
|  | Static IP address/prefix | Indicate the static IP address/prefix for the DNN, S-NSSAI. |
|  | User Plane Security Policy | Indicates the security policy for integrity protection and encryption for the user plane. |
|  | PDU Session continuity at inter RAT mobility | Provides for this DDN, S-NSSAI how to handle a PDU Session when UE the moves to or from NB-IoT. Possible values are: maintain the PDU session; disconnect the PDU session with a reactivation request; disconnect PDU session without reactivation request; or to leave it to local VPLMN policy. |
|  | NEF Identity for NIDD | When present, indicates, per S-NSSAI and per DNN, the identity of the NEF to anchor Unstructured PDU Session. When not present for the S-NSSAI and DNN, the PDU session terminates in UPF (see NOTE 8). |
|  | NIDD information | Information such as External Group Identifier, External Identifier, MSISDN, or AF Identifier used for SMF-NEF Connection. |
|  | SMF-Associated Expected UE Behaviour parameters | Parameters on expected characteristics of a PDU Session their corresponding validity times as specified in clause 4.15.6.3. |
|  | SMF-Associated Application-Specific Expected UE Behaviours parameters | Parameters characterise the foreseen behaviour of a UE for a specific application as specified in clause 4.15.6.3f. |
|  | Suggested number of downlink packets | Parameters on expected PDU session characteristics as specified in clauses 4.15.3.2.3b and 4.15.6.3a. |
|  | ATSSS information | Indicates whether MA PDU session establishment is allowed. |
|  | Secondary authentication indication | Indicates that whether the Secondary authentication/authorization (as defined in clause 5.6 of TS 23.501 [2]) is required for PDU Session Establishment or PDN Connection Establishment as specified in clause 4.3.2.3 and clause H.2. (see NOTE 14) |
|  | DN-AAA Server UE IP address allocation indication | Indicates that whether the SMF is required to request the UE IP address from the DN-AAA Server (as defined in clause 5.6 of TS 23.501 [2]) for PDU Session Establishment or PDN Connection Establishment as specified in clause 4.3.2.3 and clause H.2. |
|  | DN-AAA Server addressing information | If at least one of secondary DN-AAA authentication, DN-AAA authorization or DN-AAA UE IP address allocation is required by subscription data, the subscription data may also contain DN-AAA Server addressing information. |
|  | Edge Configuration Server Address Configuration Information | Consists of one or more ECS Configuration Information as defined in clause 8.3.2.1 of TS 23.558 [83]. The ECS Configuration Information sent by UDM to SMF is associated with the PLMN ID where the UE is roaming on. (see NOTE 20) |
|  | API based secondary authentication indication | Indicates that whether the API based Secondary authentication/authorization (as defined in clause 5.2.3 of TS 23.256 [80]) is required for PDU Session Establishment or PDN Connection Establishment as specified in clause 4.3.2.3 and clause H.2 (see NOTE 14). |
|  | UE authorization for EAS discovery via EASDF | Indicates whether the UE is authorized to use 5GC assisted EAS discovery via EASDF (as defined in TS 23.548 [74]). |
|  | HR-SBO authorization indication | Indicates whether the VPLMN is authorized for Home Routed Session Breakout (HR-SBO) (see NOTE 17 and NOTE 18). |
| Required UPF functionalities | Indicates the required UPF functionalities for the DNN, S-NSSAI. |
|  | Preferred UPF functionalities | Indicate the priority of preferred UPF functionalities for the DNN, S-NSSAI. |
| Identifier translation | SUPI | Corresponding SUPI for input GPSI. |
|  | (Optional) MSISDN | Corresponding GPSI (MSISDN) for input GPSI (External Identifier). This is optionally provided for legacy SMS infrastructure not supporting MSISDN-less SMS. The presence of an MSISDN should be interpreted as an indication to the NEF that MSISDN shall be used to identify the UE when sending the SMS to the SMS-SC via T4. |
|  | GPSI | Corresponding GPSI for input SUPI and associated application information (e.g. Application Port ID) (NOTE 15). |
| Intersystem continuity Context | (DNN, PGW FQDN) list | For each DNN, indicates the SMF+PGW-C which support interworking with EPC. |
| LCS privacy  (data needed by GMLC) | LCS privacy profile data | Provides information for LCS privacy classes and Location Privacy Indication (LPI) as defined in clause 5.4.2 of TS 23.273 [51] |
| Ranging/Sidelink Positioning privacy (data needed by GMLC) | UE Ranging/SL Positioning privacy profile data | Provides information for Ranging/Sidelink Positioning privacy classes and Ranging/SL Positioning Privacy Indication (RSPI) as defined in Annex B of TS 33.533 [94]. |
| LCS mobile origination  (data needed by AMF) | LCS Mobile Originated Data | When present, indicates to the serving AMF which LCS mobile originated services are subscribed as defined in clause 7.1 of TS 23.273 [51]. |
| User consent (see TS 23.288 [50]) | User consent for UE data collection | Indicates whether the user has given consent for collecting, distributing and analysing UE related data. User consent is provided per purpose (e.g. analytics, model training). |
| UE reachability | UE reachability information | Provides, per PLMN, the list of NF IDs or the list of NF sets or the list of NF types authorized to request notification for UE's reachability (NOTE 7). |
| V2X Subscription data (see TS 23.287 [73]) | NR V2X Services Authorization | Indicates whether the UE is authorized to use the NR sidelink for V2X services as Vehicle UE, Pedestrian UE, or both. |
|  | LTE V2X Services Authorization | Indicates whether the UE is authorized to use the LTE sidelink for V2X services as Vehicle UE, Pedestrian UE, or both. |
|  | NR UE-PC5-AMBR | AMBR of UE's NR sidelink (i.e. PC5) communication for V2X services. |
|  | LTE UE-PC5-AMBR | AMBR of UE's LTE sidelink (i.e. PC5) communication for V2X services. |
| A2X Subscription data (see TS 23.256 [80]) | NR A2X Services Authorization | Indicates whether the UE is authorized to use the NR sidelink for A2X services. |
|  | LTE A2X Services Authorization | Indicates whether the UE is authorized to use the LTE sidelink for A2X services. |
|  | NR UE-PC5-AMBR for A2X | AMBR of UE's NR sidelink (i.e. PC5) communication for A2X services. |
|  | LTE UE-PC5-AMBR for A2X | AMBR of UE's LTE sidelink (i.e. PC5) communication for A2X services. |
| ProSe Subscription data (see TS 23.304 [77]) | ProSe Service Authorization | Indications for whether the UE is authorised to use the 5G ProSe service(s), including:  - use 5G ProSe Direct Discovery;  - use 5G ProSe Direct Communication;  - act as a 5G ProSe Remote UE;  - serve as a 5G ProSe UE-to-Network Relay;  - use multi-path communication via direct Uu path and via 5G ProSe Layer-2 UE-to-Network Relay as a 5G ProSe Layer-2 Remote UE;  - act as a 5G ProSe End UE; and  - serve as a 5G ProSe UE-to-UE Relay. |
|  | ProSe NR UE-PC5-AMBR | AMBR of UE's NR sidelink (i.e. PC5) communication for ProSe services. |
| MBS Subscription data (see TS 23.247 [78]) | MBS Service Authorization | Indicates whether the UE is authorized to use Multicast MBS service. May also indicate the multicast MBS Session which the UE is allowed to join if the UE is authorized to use multicast MBS Service. |
|  | MBS Assistance Information | Include MBS assistance information for a UE that joins a multicast group. |
| Time Synchronization Subscription data (see clause 5.27.1.11 of TS 23.501 [2]) | AF Request Authorization Information | Includes the AF Request Authorization to indicate whether the UE is authorized for an AF-requested 5G access stratum-based time distribution and (g)PTP-based time distribution services (per DNN/S-NSSAI). The indication is provided separately for each service.  Optionally includes a list of TA(s) which specifies the Authorized Time Synchronization Coverage Area in which an AF may request time synchronization services (NOTE 19).  Optionally, one or more periods of authorized start and stop times, which indicates the allowed time period during which an AF may request time synchronization services.  Optionally, authorized Uu time synchronization error budget, which indicates the limit the AF may request.  Optionally includes information to determine whether the AF may request  - to provide clock quality metric information to the UE;  - to provide an acceptable/not acceptable indication to the UE.  Optionally includes one or more sets of the clock quality acceptance criteria for the UE that the AF may request. Clock quality acceptance criteria may be defined using TSS attributes from Table 5.27.1.12-1 of TS 23.501 [2]. |
|  | Subscribed Time Synchronization Service ID(s) | Each containing the DNN/S-NSSAI and a reference to a PTP instance configuration pre-configured at the TSCTSF.  Optionally, for each PTP instance configuration, one or more periods of start and stop times defining active times of time synchronization service for the PTP instance.  Optionally, for each PTP instance configuration, a Time Synchronization Coverage Area defining a list of TAs where the (g)PTP-based time synchronization is available for the UEs in the PTP instance (NOTE 19).  Optionally, for each PTP instance configuration, Uu time synchronization error budget. |
| Ranging/Sidelink Positioning Subscription data (see TS 23.586 [88]) | Ranging/SL Positioning Service Authorization | Indicates whether the UE is authorized to use Ranging/SL Positioning Service. |
| NOTE 1: The Subscribed DNN list can include a wildcard DNN.  NOTE 2: The default DNN shall not be a wildcard DNN.  NOTE 3: The Steering of Roaming information and UDM Update Data are protected using the mechanisms defined in TS 33.501 [15].  NOTE 4: Framed Route information and Framed Route(s) are defined in TS 23.501 [2].  NOTE 5: Depending on the scenario PGW-C FQDN may be for S5/S8, or for S2b (ePDG case).  NOTE 6: The Allowed PDU Session Types configured for a DNN which supports interworking with EPC should contain only the PDU Session Type corresponding to the PDN Type configured in the APN that corresponds to the DNN.  NOTE 7: Providing a list of NF types or a list of NF sets may be more appropriate for some deployments, e.g. in highly dynamic NF lifecycle management deployments.  NOTE 8: For a S-NSSAI and a DNN, the "Invoke NEF Indication" shall be present in the SMF selection subscription data if and only if the "NEF Identity for NIDD" Session Management Subscription Data includes a NEF Identity. When the "NEF Identity for NIDD" Session Management Subscription Data includes a NEF Identity for a S-NSSAI and DNN, the "Control Plane Only Indicator" will always be set for PDU Sessions to this S-NSSAI and DNN (see clause 5.31.4.1 of TS 23.501 [2]).  NOTE 9: When multiple GPSIs are included in the GPSI list, any GPSI in the list can be used in NSSAA procedures.  NOTE 10: The same PCF can be selected to serve the UE and to serve one or multiple PDU sessions, each of them is indicated in the list of S-NSSAI, DNN combinations in the PCF Selection Assistance Info. Providing one combination of DNN and S-NSSAI in the PCF Selection Assistance Info is assumed if interworking with EPS is needed. In case multiple PDU sessions to one DNN, S-NSSAI are established in EPS, it is appropriate to select same PCF by configuration or by using existing method, e.g. same PCF selection in usage monitoring.  NOTE 11: If Network Slice Simultaneous Registration Group information is present and the VPLMN does not support the subscription-based restrictions to simultaneous registration of network slices, the subset of the Subscribed S-NSSAIs defined in clause 5.15.12 of TS 23.501 [2], are included, without providing the NSSRG information.  NOTE 12: The Default S-NSSAIs (if more than one is present) are associated with common NSSRG values if NSSRG information is present. At least one Default S-NSSAI shall be present in a subscription including NSSRG information.  NOTE 13: When UUAA is performed in the AMF (as in clause 5.2.2 of TS 23.256 [80]) and UUAA-MM status is FAILED or PENDING, the AMF shall reject PDU session establishment requests from the UE for a DNN that is subject to aerial services.  NOTE 14: For a DNN in S-NSSAI either a DN-AAA based secondary authentication, or an API based secondary authentication can be configured. When API based authentication of the PDU session is required, Secondary authentication indication shall not be present.  NOTE 15: A GPSI may be associated with Application Port ID, MTC Provider Information and/or AF Identifier.  NOTE 16: For non-roaming UE (e.g. accessing SNPN with CH credentials), LBO roaming information does not apply.  NOTE 17: This information applies only for HR PDU Session.  NOTE 18: This information is only valid for the current serving network. When Session Breakout for HR Session is authorized, usage of corresponding EAS Deployment Information and AF traffic influence in VPLMN is also authorized.  NOTE 19: The subscribed Time Synchronization Coverage Area shall be inside of the Allowed Areas as per UE's service area restriction.  NOTE 20: For roaming UE in a visited PLMN, the corresponding PLMN ID is provided with Edge Configuration Server (ECS) Address Configuration Information.  NOTE 21: The entries in the Credentials Holder controlled prioritized lists of preferred SNPNs and GINs for accessing Localized Services are associated with a time validity information and optionally a location validity information indicating the conditions allowing the UE to access to localized services in the SNPN or/and location assistance information used to aid the UE where to search for the SNPN as specified in clause 5.30.2.3 of TS 23.501 [2].  NOTE 22: Only for an S-NSSAI dedicated to a single AF is associated with Slice Usage Policy information. For roaming UE, Slice Usage Policy information does not apply. | | |

Table 5.2.3.3.1-2: Group Subscription data types

| Subscription data type | Field | Description |
| --- | --- | --- |
| Group Identifier translation | External Group Identifier | Identifies external group of UEs that the UE belongs to as defined in TS 23.682 [23]. |
|  | Internal Group Identifier | Identifies internal group of UEs that the UE belongs to as defined in TS 23.501 [2]. |
|  | SUPI list | Corresponding SUPI list for input External Group Identifier. |
| Group Data  (NOTE 1) | Internal Group Identifier | Internal identifiers of the group of UEs that the Group Data belongs to. |
|  | Group data | In the case of 5G VN related groups the content of this information contains parameters defined in clause 4.15.6.3b.  In the case of DNN and S-NSSAI specific parameters in the Groups, the content of this information contains parameters defined in clause 4.15.6.3e. |
| NOTE 1: Group Data within Group Subscription Data can be managed using the Shared Data feature defined in TS 29.503 [52]. In that case, Shared Data is identified using Shared Data identifier and can contain additional information than the one defined in this table. | | |

At least a mandatory key is required for each Subscription Data Type to identify the corresponding data. Depending on the use case, for some Subscription Data Types it is possible to use one or multiple sub keys to further identify the corresponding data, as defined in Tables 5.2.3.3.1-3 and 5.2.3.3.1-4 below.

Table 5.2.3.3.1-3: UE Subscription data types keys

|  |  |  |
| --- | --- | --- |
| Subscription Data Types | Data Key | Data Sub Key |
| Access and Mobility Subscription data | SUPI | Serving PLMN ID and optionally NID |
| SMF Selection Subscription data | SUPI | Serving PLMN ID and optionally NID |
| UE context in SMF data | SUPI | S-NSSAI |
| SMS Management Subscription data | SUPI | Serving PLMN ID and optionally NID |
| SMS Subscription data | SUPI | Serving PLMN ID and optionally NID |
| UE Context in SMSF data | SUPI | - |
| Session Management Subscription data | SUPI | S-NSSAI |
|  |  | DNN |
|  |  | Serving PLMN ID and optionally NID |
| Identifier translation | GPSI | - |
|  | SUPI | Application Port ID, MTC Provider Information, AF Identifier |
| Slice Selection Subscription data | SUPI | Serving PLMN ID and optionally NID |
| Intersystem continuity Context | SUPI | DNN |
| LCS privacy | SUPI | - |
| Ranging/Sidelink Positioning privacy | SUPI | - |
| LCS mobile origination | SUPI | - |
| User consent | SUPI | Purpose |
| UE reachability | SUPI | - |
| V2X Subscription data | SUPI | - |
| ProSe Subscription data | SUPI | - |
| MBS Subscription data | SUPI | - |
| A2X Subscription data | SUPI | - |
| Ranging/Sidelink Positioning Subscription data | SUPI | - |

Table 5.2.3.3.1-4: Group Subscription data types keys

|  |  |  |
| --- | --- | --- |
| Subscription Data Types | Data Key | Data Sub Key |
| Group Identifier translation | External Group Identifier | - |
|  | Internal Group Identifier | - |
| Group Data | Internal Group Identifier | - |

Wireline access specific subscription data parameters are specified in TS 23.316 [53].

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

#### 5.2.7.2 Nnrf\_NFManagement service

##### 5.2.7.2.1 General

**Service description:** This service enables one NF to manage its NF profile in NRF (i.e. register, update, deregister). This service also allows a consumer NF or SCP to subscribe in NRF to receive notifications regarding changes in the NF profile of other NFs.

##### 5.2.7.2.2 Nnrf\_NFManagement\_NFRegister service operation

**Service Operation name:** Nnrf\_NFManagement\_NFRegister.

**Description:** Registers the consumer NF in the NRF by providing the NF profile of the consumer NF to NRF and NRF marks the consumer NF available.

**Inputs, Required:** NF type, NF instance ID, FQDN or IP address of NF, Names of supported NF services (if applicable) and PLMN ID e.g. if NF needs to be discovered by other PLMNs/SNPNs.

NOTE 1: for the UPF, the addressing information within the NF profile corresponds to the N4 interface.

NOTE 2: For the purpose of the Nnrf\_NFManagement service, the SCP is treated by the NRF in the same way as NFs. Specifically, the SCP is designated with a specific NF type and NF instance ID. However, the SCP does not support services and related NF profile parameters do not apply (e.g. NF Set ID, NF service set ID, Endpoint Address(es) of instance(s) of supported service(s)), see clause 6.2.6.3 of TS 23.501 [2].

**Inputs, Optional:**

- If the consumer NF stores Data Set(s) (e.g. UDR): Range(s) of SUPIs, range(s) of GPSIs, range(s) of external group identifiers, Data Set Identifier(s).

- If the consumer is BSF: Range(s) of SUPIs, range(s) of GPSIs, Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes, IP domain list as described in clause 6.1.6.2.21 of TS 29.510 [37], Range(s) of SUPIs, range(s) of GPSIs.

NOTE 3: Range of SUPI(s) is limited in this release to a SUPI type of IMSI as defined in TS 23.003 [33].

- If the consumer is UDM, UDR, PCF, BSF or AUSF, they can include UDM Group ID, UDR Group ID, PCF Group ID, BSF Group ID, AUSF Group ID respectively.

- For UDM and AUSF, Routing Indicator, or Routing Indicator and Home Network Public Key identifier; Home Network Identifier: PLMN ID in the case of PLMN, PLMN ID + NID in the case of SNPN. Optionally, some NFs may additionally include a Home Network Identifier (including the identification of the CH with AAA Server or DCS with AAA Server) in the form of a realm e.g. in the case of access to an SNPN using credentials owned by CH with AAA Server or in the case of SNPN Onboarding using a DCS with AAA Server.

- For NSSAAF, Home Network Identifier in the form of a realm e.g. in the case of access to an SNPN using credentials owned by CH with AAA Server or in the case of SNPN Onboarding using credentials from a DCS with AAA Server.

- If the consumer is AMF, it includes list of GUAMI(s). In addition, AMF may include list of GUAMI(s) for which it can serve as backup for failure/maintenance.

- If the consumer is CHF, it may include Range(s) of SUPIs, Range(s) of GPSIs, or Range(s) of PLMNs as defined in TS 32.290 [42].

- If the consumer is CHF, primary CHF instance and the secondary CHF instance pair. If the CHF does not provide NF set ID or NF Service Set ID, it shall provide a primary CHF instance and the secondary CHF instance pair and otherwise it may do so.

- If the consumer is P-CSCF, the P-CSCF IP address(es) to be provided to the UE by SMF.

- If the consumer is HSS, IMPI range, IMPU range, HSS Group ID (as defined in TS 23.228 [55]) can be used as optional input parameters.

- For the UPF Management: UPF Provisioning Information as defined in clause 4.17.6.

- S-NSSAI(s) and the associated NSI ID(s) (if available).

- DNN(s) if the consumer is PCF or BSF. DNN(s) per S-NSSAI if the consumer is SMF, UPF or TSCTSF.

- If the consumer is a trusted AF it may include one or multiple combination(s) of S-NSSAI and DNN corresponding to the AF. In addition, it may include supported Application Id(s), Event ID(s) and Internal-Group Identifier. It may include an indication whether it supports mapping between UE IP address (IPv4 address or IPv6 prefix) and UE ID (i.e. SUPI).

- Information about the location or serving scope of the NF consumer (operator specific information, e.g. geographical location, data centre).

- TAI(s).

- NF Set ID.

- NF Service Set ID.

- If the consumer is PCF or SMF, it includes the MA PDU Session capability to indicate if the NF instance supports MA PDU session or not.

- If the consumer is PCF, it includes the DNN replacement capability to indicate if the NF instance supports DNN replacement or not.

- If the consumer is PCF or SMF, it includes the slice replacement capability to indicate if the NF instance supports slice replacement or not.

- If the consumer is PCF, it may include the 5G ProSe Capability as specified in TS 23.304 [77].

- If the consumer is PCF, it may include the V2X capability as specified in TS 23.287 [73].

- If the consumer is PCF, it may include the A2X capability as specified in TS 23.256 [80].

- If the consumer is PCF, it may include the Ranging/SL Positioning Capability as specified in TS 23.586 [88].

- If the consumer is PCF, it may include the indication of PCF support of URSP delivery in EPS.

- If the consumer is PCF, it may include the indication of PCF support of VPLMN specific rules.

- If the consumer is PCF, it may include the indication of PCF support of URSP rule enforcement.

- If the consumer is NWDAF, it may include:

- Analytics ID(s) (possibly per service).

- NWDAF Serving Area information and Supported Analytics Delay per Analytics ID(s) (if available).

- Analytics aggregation capability and/ or Analytics metadata provisioning capability if such capability is provided by the NWDAF.

- Roaming exchange capability if such capability is provided by NWDAF.

- If the consumer NWDAF contains MTLF, it may also include the ML model Filter information parameters S-NSSAI(s) and Area(s) of Interest for the trained ML model(s) per Analytics ID(s) and ML Model Interoperability indicator per Analytics ID(s), if available (see clause 5.2 of TS 23.288 [50]).

- If the consumer is NWDAF containing MTLF with Federated Learning (FL) capability, it includes FL capability information per analytics ID containing FL capability type (i.e. FL client and/or FL server, if available) and Time interval supporting FL, if available (see clause 5.2 of TS 23.288 [50]).

- If the consumer is NWDAF containing MTLF with ML Model Accuracy checking capability, it includes ML Model Accuracy checking capability for ML model accuracy monitoring (see clause 5.2 of TS 23.288 [50]).

- If the consumer is NWDAF containing AnLF with Analytics Accuracy checking capability, it includes Analytics Accuracy checking capability for Analytics Accuracy Monitoring (see clause 5.2 of TS 23.288 [50]).

- It may also include NF Set ID and NF Type of the NF data sources, if data management service is available.

Details about NWDAF specific information are described in clause 6.3.13 of TS 23.501 [2].

- If the consumer is ADRF, it may include:

- Data and analytics storage and retrieval capability if available.

- ML model storage and retrieval capability if available.

Details about ADRF specific information are described in clause 6.3.20 of TS 23.501 [2].

- If the consumer is NEF, it may include Event ID(s) supported by AFs, the S-NSSAI and DNN corresponding to the untrusted AF served by the NEF, Application Identifier(s) supported by AFs, range(s) of External Identifiers, or range(s) of External Group Identifiers, or the domain names served by the NEF. It may also include an indication whether the untrusted AF supports mapping between UE IP address (IPv4 address or IPv6 prefix) and external UE ID (i.e. GPSI). If the consumer is local NEF, it may include parameters of list of supported TAI or list of supported DNAI additionally.

- If the consumer is a NSACF, it includes the S-NSSAI(s) of the PLMN or SNPN where the NSACF is located, the NSAC Service Area Identifier(s) n and NSACF service capabilities. Details about NSAC Service Area Identifier and NSACF service capabilities are described in clause 6.3.22 of TS 23.501 [2].

- Notification endpoint for default subscription for each type of notification that the NF is interested in receiving.

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

- NF capacity information.

- NF priority information.

- If consumer is NF, SCP domain the NF belongs to.

- If the consumer is SCP, it may include:

- SCP domain(s) the SCP belongs to.

- Remote PLMNs reachable through SCP.

- Endpoint addresses or Address Domain(s) (e.g. IP Address or FQDN ranges) accessible via the SCP.

- NF sets of NFs served by the SCP.

- If the consumer NF is MB-SMF, it may include MB-SMF service area and the MBS Session ID(s), Area Session ID(s), the corresponding MBS service area(s) if available, as specified in TS 23.247 [78].

- If the consumer is DCCF, the request may include DCCF Serving Area information, NF type of the NF data source, NF Set ID of the NF data sources, support for relocation of data subscription. Details about DCCF discovery and selection are described in clause 6.3.19 of TS 23.501 [2].

- If the consumer is EASDF, it may include S-NSSAI, DNN, N6 IP address of the PSA UPF, Supported DNS security protocols of EASDF, location as per NF profile and DNAI (if exists).

- For ON-SNPN, if the consumer is AMF, Capability to support SNPN Onboarding, or, if the consumer is SMF, Capability to support User Plane Remote Provisioning.

- If the consumer is NEF, it may include the support for UAS NF functionality, the capability to support Multi-member AF session with required QoS and the capability to support member UE selection assistance functionality.

- If the consumer is UPF UPF can expose NAT information, it may include the range of IP addresses the NAT uses towards the DN (e.g. public IP addresses). This IP address range may be on a per IP domain, DNN and S-NSSAI.

- If the consumer is DCSF, it may include an IMS domain name or a list of IMS domain names it serves, IMPU range of calling identity or called identity it serves, or IMPI range it serves.

- If the consumer is MF, it includes the data channel media capabilities it supports. It may also include MF location information as specified in TS 23.228 [55].

- If the consumer is MRF or MRFP, it includes the list of supported IMS media services (as defined in TS 23.228 [55]).

**Outputs, Required:** Result indication.

**Outputs, Optional:** None.

See clause 5.21.2.1 of TS 23.501 [2], the AMF registers itself to NRF.

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

#### 5.2.7.3 Nnrf\_NFDiscovery service

##### 5.2.7.3.1 General

**Service description:** This service enables one NF or SCP to discover a set of NF instances with specific NF service or a target NF type or one or more SCPs. The service also enables one NF service or SCP to discover a specific NF service. The service operations defined below allow the NF/NF services or SCP to communicate with NRF.

This service also enables an SCP to discover SCPs.

NOTE: For the purpose of the Nnrf\_NFDiscovery service, the SCP is treated in the same way as NFs. It is designated with a specific NF type. However, the SCP does not support services.

##### 5.2.7.3.2 Nnrf\_NFDiscovery\_Request service operation

**Service operation name:** Nnrf\_NFDiscovery\_Request

**Description:** provides the IP address or FQDN of the expected NF instance(s) and if present in NF profile, the Endpoint Address(es) of NF service instance(s) to the NF service consumer or SCP.

**Inputs, Required:** one or more target NF service Name(s), NF type of the target NF, NF type of the NF service consumer.

If the NF service consumer intends to discover an NF service producer providing all the standardized services, it provides a wildcard NF service name.

**Inputs, Optional:**

- S-NSSAI and the associated NSI ID (if available), DNN, target NF/NF service PLMN ID (or realm in the case of network specific identifier type SUCI/SUPI, see clause 4.17.5a), NRF to be used to select NFs/services within HPLMN or Credentials Holder, Serving PLMN ID (or PLMN ID and NID in the case of SNPN, see clause 4.17.5a), the NF service consumer ID, preferred target NF location, TAI.

NOTE 1: For network slicing the NF service consumer ID is a required input.

- FQDN for the S5/S8 interface of the SMF+PGW-C, to discover the N11/N16 interface of the SMF+PGW-C in the case of EPS to 5GS mobility.

- If the target NF stores Data Set(s) (e.g. UDR, BSF): SUPI, GPSI, IMPI, IMPU, Data Set Identifier(s). (UE) IPv4 address, IP domain or (UE) IPv6 Prefix.

NOTE 2: GPSI is relevant for BSF.

NOTE 3: If the request includes a subscriber identifier the NRF may need to use the association between the supplied subscriber identifier and the appropriate NF Group ID as described in clause 6.3.1 of TS 23.501 [2] to determine the applicable set of NF instances for the response.

NOTE 4: The (UE) IPv4 address or (UE) IPv6 Prefix is provided for BSF discovery: in that case the NRF looks up for a match within one of the Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes provided by BSF(s) as part of the invocation of Nnrf\_NFManagement\_NFRegister operation. The NRF is not meant to store individual (UE) IPv4 addresses or (UE) IPv6 prefixes.

- If the target NF is UDM or AUSF, the request may include the UE's Routing Indicator, or the UE's Routing Indicator and Home Network Public Key identifier.

- If the target UDM or NF is AUSF, the request may include the UE's HNI: PLMN ID in the case of PLMN, PLMN ID + NID in the case of SNPN. Optionally, some NFs may additionally include a Home Network Identifier in the form of a realm e.g. in the case of access to an SNPN using credentials owned by CH with AAA Server or in the case of SNPN Onboarding using a DCS with AAA Server.

- If the target NF is NSSAAF, the request may include Home Network Identifier in the form of a realm e.g. in the case of access to an SNPN using credentials owned by CH with AAA Server or in the case of SNPN Onboarding using credentials from a DCS with AAA Server.

- If the target NF is AMF and the consumer NF is MB-SMF for broadcast service, the request includes TAI(s) (see clause 7.3 of TS 23.247 [78]).

- If the target NF is AMF and the consumer NF is other than MB-SMF, the request may include:

- AMF region, AMF Set, GUAMI and Target TAI(s).

- If the target NF is UDR or UDM or AUSF or PCF or BSF, the request may include UDR Group ID or UDM Group ID or AUSF Group ID or PCF Group ID or BSF Group ID respectively.

NOTE 5: It is assumed that the corresponding NF service consumer is either configured with the corresponding Group ID or it received it via earlier Discovery output.

- If the target NF is UDM, the request may include SUPI, GPSI, Internal Group ID and External Group ID.

- If the target NF is UPF, the request may include SMF Area Identity, UE IPv4 Address/IPv6 Prefix, supported ATSSS steering functionality, the supported UPF event exposure service, the supported Event IDs that can be subscribed, supported NAT information exposure functionality, and supported packet inspection functionaility (see clause 6.2.3 of TS 23.501 [2]). And if UPF can expose NAT information, the UE IPv4 address/IPv6 Prefix seen by the DN (e.g. a Public IP address).

NOTE 6: If UE's IPv4 address or IPv6 Prefix is provided for UPF discovery, then the NRF looks up for a match within one of the Range(s) of IPv4 addresses or IPv6 prefixes provided by UPF in the NF profile at the invocation of Nnrf\_NFManagement\_NFRegister operation. The NRF is not meant to store the UE's individual IPv4 addresses or IPv6 prefixes.

NOTE 7: Discovering UPF at PDU Session Establishment time and creating the N4 association assumes full connectivity between SMF and UPFs.

- If the target NF is CHF, the request may include SUPI or GPSI as specified in TS 32.290 [42].

- If the target NF is PCF or SMF, the request may include the MA PDU Session capability to indicate that a NF instance supporting MA PDU session capability is requested.

- If the target NF is PCF, the request may include the DNN replacement capability to indicate that a NF instance supporting DNN replacement capability is preferred.

- If the target NF is PCF or SMF, the request may include the slice replacement capability to indicate that a NF instance supporting slice replacement capability is preferred.

- If the target NF is PCF, the request may include the 5G ProSe Capability as specified in TS 23.304 [77].

- If the target NF is PCF, the request may include the V2X capability as specified in TS 23.287 [73].

- If the target NF is PCF, the request may include the A2X capability as specified in TS 23.256 [80].

- If the target NF is PCF, the request may include the URSP delivery in EPS capability.

- If the target NF is PCF, the request may include the Ranging/SL Positioning Capability as specified in TS 23.586 [88].

- If the target NF is NWDAF, the request may include:

- Analytics ID(s) (possibly per service).

- TAI(s).

- Analytics aggregation capability and/or Analytics metadata provisioning capability.

- A Real-Time Communication Indication per Analytics ID, NF Set ID and NF Type of the NF data sources.

- Roaming exchange capability if data/analytics exchange between PLMNs is needed.

- The S-NSSAI(s), Area(s) of Interest of the Trained ML Model required and NF consumer information when the target is an NWDAF containing MTLF.

- Required FL capability type (i.e. FL server, FL client, if available) and Time period of interest when the target is an NWDAF containing MTLF with FL capability. When the target is an NWDAF containing MTLF with FL client capability, NF Set ID(s) of data source and NF type(s) where data can be collected as input for local model training may be included.

- If the target NF is NWDAF containing MTLF with ML Model Accuracy checking capability, it includes ML Model Accuracy checking capability for ML model Accuracy Monitoring (see clause 5.2 of TS 23.288 [50]).

- If the target NF is NWDAF containing AnLF with Analytics Accuracy checking capability, it includes Analytics Accuracy checking capability for Analytics Accuracy Monitoring (see clause 5.2 of TS 23.288 [50]).

Details about NWDAF discovery and selection are described in clause 6.3.13 of TS 23.501 [2].

NOTE 8: Analytics metadata provisioning capability is only applicable when NF service consumer is NWDAF.

NOTE 9: NF consumer information such as vendor ID is defined in stage 3.

- If target NF is ADRF, the request may include:

- Data and analytics storage and retrieval capability.

- ML model storage and retrieval capability.

Details about ADRF discovery and selection are described in clause 6.3.20 of TS 23.501 [2].

- If the target NF is HSS, the request may include IMPI and/or IMPU and/or HSS Group ID.

- If the NF service consumer needs to discover NF service producer instance(s) within an NF instance, the request includes the target NF Instance ID and NF Service Set ID of the producer.

- If the NF service consumer needs to discover NF service producer instance(s) in an equivalent NF Service Set within an NF Set, the request includes the identification of the equivalent NF service Set and NF Set ID of producer.

NOTE 10: TS 29.510 [37] specifies the mechanism to identify equivalent NF Service Sets.

- If the NF service consumer needs to discover NF service producer instance(s) in the NF Set, the request includes the target NF Set ID of the producer.

- If the target NF is SMF, the request may include:

- the UE location (TAI); or

- TAI list.

- If the target NF is P-CSCF, the request may include UE location information, UE IP address/IP prefix, Access Type.

- If the target NF is NEF, the request may include Event ID(s) provided by AF and optional AF identification as described in clause 6.2.2.3 of TS 23.288 [50]. When the consumer is an AF, the request may include an External Identifier, External Group Identifier, or a domain name. If the target NF is local NEF, the request may include the parameters of list of supported TAI or list of supported DNAI additionally.

- If the target NF is SMF, the request may include the Control Plane CIoT 5GS Optimisation Indication or User Plane CIoT 5GS Optimisation Indication.

- If the target NF is a NSACF, the request may include the S-NSSAI(s) of the PLMN or SNPN where the NSACF is located , the NSAC Service Area Identifier and NSACF service capability. Details about NSACF discovery and selection are described in clause 6.3.22 of TS 23.501 [2].

- If the target NF is SCP, the request may include information about:

- SCP domain(s).

- Remote PLMN reachable through SCP.

- Endpoint addresses or Address Domain(s) (e.g. IP Address or FQDN ranges) accessible via the SCP.

- NF sets of NFs served by the SCP.

- If the target NF is MB-SMF, the request may include UE location (i.e. TAI), MBS Session ID and Area Session ID. Details about MB-SMF discovery and selection are described in TS 23.247 [78].

- If the target NF is 5G DDNMF, the request may include SUPI, IP Address or FQDN of 5G DDNMF.

- If the target NF is DCCF, the request may include TAI(s), NF type of the NF data sources, NF Set ID of the NF data sources, support for relocation of data subscription. Details about DCCF discovery and selection are described in clause 6.3.19 of TS 23.501 [2].

- If the target NF is EASDF, the request may include S-NSSAI, DNN, N6 IP address of the PSA UPF, Supported DNS security protocols, location as per NF profile and DNAI(if exist). Details about EASDF discovery and selection are described in clause 6.3.23 of TS 23.501 [2].

- If the target NF is AMF, the request may include the support of SNPN Onboarding to indicate whether the target NF instance supports SNPN Onboarding or not.

- If the target NF is SMF, the request may include the support of User Plane Remote Provisioning to indicate whether the target NF instance supports User Plane Remote Provisioning or not as described in clause 5.30.2.10.4.3 of TS 23.501 [2].

- If the target NF is NEF, the request may include the support of UAS NF functionality, the capability to support Multi-member AF session with required QoS and the capability to support member UE selection assistance functionality.

- If the target NF is NSSAAF, the request may include SUPI or Internal Group ID.

- If the target NF is DCSF, the request may include IMPU of calling party, SIP URI or Tel URI of called party.

- If the target NF is MF, the request may include the list of required data channel media capabilities or MF location information as specified in TS 23.228 [55].

- If the target NF is MRF or MRFP, it includes the list of required IMS media services (as defined in TS 23.228 [55]).

- If the target NF is in another PLMN or domain, the request may include an indication of "support of the indirect communication with delegated discovery with NF selection at target domain feature" and/or an indication of "support of indirect communication without delegated discovery with NF selection at target domain feature".

**Outputs, Required:**

- One of the following:

- A set of NF instance profiles; or

- an indication that "indirect communication with delegated discovery with NF selection at target domain is requested"; or

- an indication that "indirect communication without delegated discovery with NF selection at target domain is requested" together with a set of NF instance profiles;

- a validity period for the discovery result.

The set of NF instance profiles shall contain per NF Instance: NF type, NF instance ID, FQDN or IP address(es) of the NF instance and if applicable, a list of services instances, where each service instance has a service name, a NF service instance ID and optionally Endpoint Address(es)

Endpoint Address(es) may be a list of IP addresses or an FQDN for the NF service instance.

NOTE 11: SCPs does not have any service instances.

**Outputs, Optional:** Per NF instance, other information in the NF profile listed in clause 6.2.6 of TS 23.501 [2] related to the NF instance, such as:

- NF load information.

- NF capacity information.

- NF priority information.

- If the target NF stores Data Set(s) (e.g. UDR): Range(s) of SUPIs, range(s) of GPSIs, range(s) of external group identifiers, Data Set Identifier(s). If the target NF is BSF or P-CSCF: Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes, Range(s) of SUPIs, range(s) of GPSIs.

NOTE 12: Range of SUPI(s) is limited in this release to a SUPI type of IMSI as defined in TS 23.003 [33].

- If the target NF is UDM, UDR, PCF, BSF or AUSF, they can include UDM Group ID, UDR Group ID, PCF Group ID, BSF Group ID, AUSF Group ID respectively.

- If the target NF is HSS, it can include HSS Group ID.

- For UDM and AUSF, Routing Indicator, or Routing Indicator and Home Network Public Key identifier.

- If the target NF is AMF, it includes list of GUAMI(s). In addition, it may include list of GUAMI(s) for which it can serve as backup for failure/maintenance.

- If the target NF is CHF, it includes primary CHF instance and the secondary CHF instance pair(s), if configured in CHF instance profile.

- For the UPF Management: UPF Provisioning Information as defined in clause 4.17.6.

- S-NSSAI(s) and the associated NSI ID(s) (if available).

- Information about the location of the target NF (operator specific information, e.g. geographical location, data centre).

- TAI(s).

- PLMN ID.

- If the target is PCF or SMF, it includes the MA PDU Session capability to indicate if the NF instance supports MA PDU session or not.

- If the target is PCF, it includes the DNN replacement capability to indicate if the NF instance supports DNN replacement or not.

- If the target NF is NWDAF, it may include:

- Analytics ID(s) (possibly per service).

- NF Set ID and NF Type of the NF data sources, if available, NWDAF Serving Area information.

- Analytics aggregation capability and/ or Analytics metadata provisioning capability, if such capability is provided by the NWDAF.

- Supported Analytics Delay per Analytics ID.

- If the target NF is NWDAF, it may also include the ML model Filter information parameters S-NSSAI(s) and Area(s) of Interest for the trained ML model(s) per Analytics ID(s) and ML Model Interoperability indicator per Analytics ID(s), if available (see clause 5.2 of TS 23.288 [50]).

- If the target NF is NWDAF with FL capability, it may also include FL capability information per analytics ID containing FL capability type (i.e. FL server and/or FL client, if available) and Time interval supporting FL, if available (see clause 5.2 of TS 23.288 [50]).

Details about NWDAF specific information are described in clause 6.3.13 of TS 23.501 [2].

NOTE 13: The Supported Analytics Delay is provided for an Analytics ID only when the NRF had received Real-Time Communication Indication for this Analytics ID in the NWDAF discovery request.

- If the target is a trusted AF, it includes one or multiple combination(s) of the S-NSSAI and DNN corresponding to the AF. In addition, it may include supported Application Id(s), Event ID(s) supported by the AF and Internal-Group Identifier.

- NF Set ID.

- NF Service Set ID.

- If the target NF is SMF, it may include the SMF(s) Service Area.

NOTE 14: If no SMF Service Area is provided, the AMF assumes that a SMF can serve the whole PLMN.

- If the target NF is P-CSCF, it includes P-CSCF FQDN(s) or IP address(es) and optional Access Type(s) associated with each P-CSCF.

- If the target NF is NEF, it may include Event ID(s) provided by AF and/or it includes one or multiple combination(s) of the S-NSSAI and DNN corresponding to the untrusted AF served by the NEF.

- SCP domain the NF belongs to.

NOTE 15: Only one SCP domain is registered in NF profile for an NF.

- If the target is SCP:

- SCP domain(s).

- Remote PLMNs reachable through SCP.

- Endpoint addresses or Address Domain(s) (e.g. IP Address or FQDN ranges) accessible via the SCP.

- NF sets of NFs served by the SCP.

- If the target NF is 5G DDNMF, it may include IP Address or FQDN of 5G DDNMF.

- If the target NF is MB-SMF, it may include the MBS Session ID(s), Area Session ID(s), corresponding MBS service area(s) as described in TS 23.247 [78].

- If the target NF is DCCF, it includes DCCF serving area information, NF type of the NF data sources, NF Set ID of the NF data sources, support for relocation of data subscription. Details about DCCF specific information are described in clause 6.3.19 of TS 23.501 [2].

- If an indication that "indirect communication with delegated discovery with NF selection at target domain is requested" or an "indication that "indirect communication without delegated discovery with NF selection at target domain is requested" is provided, optionally:

- an indication that the reply applies to all NF types; and/or

- the address of an SCP where to send the request.

See clause 4.17.4 and 4.17.5 for details on the usage of this service operation.

\* \* \* \* End of change \* \* \*