**3GPP TSG-WG SA2 Meeting #164S2-2407554r1**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.501** | **CR** | **5420** | **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 information exposure and Packet Inspection functionality in the UPF NF profile | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Rakuten Mobile, CMCC?, ZTE?, Huawei, HiSilicon? Ericsson?, Samsung?, Nokia?, SKT? | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPEAS\_Ph2 | | | | |  | ***Date:*** | | | 2024-06-17 |
|  |  | | | |  | |  | | |  |
| ***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 followings are agreed upon in Rel-19 in accordance with the conclusions for KI#1 in TR 23.700-63:  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 based on other means, e.g. layer 7 DPI).  Based on conclusions of TR 23.700-63, 3GPP TS 23.501 should be updated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * Added Abbreviation for NAT * Modified a note in clause 5.6.10.1 * Added packet inspection functionality support for UPF in clause 6.2.3 * Added support for NAT and packet inspection functionaility in clause 6.2.6.2 * Added support for NAT and packet inspection functionaility in 6.3.3.2 and 6.3.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Support for UPF supporitng NAT and packet inspection feature will be missing | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.2, 5.6.10.1, 6.2.3, 6.2.6.2, 6.3.3.2, 6.3.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR’s revision history:*** | |  | | | | | | | | |

\* \* \* \* First change \* \* \*

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

5GC 5G Core Network

5G DDNMF 5G Direct Discovery Name Management Function

5G LAN 5G Local Area Network

5GS 5G System

5G-AN 5G Access Network

5G-AN PDB 5G Access Network Packet Delay Budget

5G-EIR 5G-Equipment Identity Register

5G-GUTI 5G Globally Unique Temporary Identifier

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5G GM 5G Grand Master

5G NSWO 5G Non-Seamless WLAN offload

5G-RG 5G Residential Gateway

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G VN 5G Virtual Network

5QI 5G QoS Identifier

ADRF Analytics Data Repository Function

AF Application Function

AI/ML Artificial Intelligence/Machine Learning

AKMA Authentication and Key Management for Applications

AnLF Analytics Logical Function

AMF Access and Mobility Management Function

AoI Area of Interest

AS Access Stratum

ATSSS Access Traffic Steering, Switching, Splitting

ATSSS-LL ATSSS Low-Layer

AUSF Authentication Server Function

BMCA Best Master Clock Algorithm

BSF Binding Support Function

CAG Closed Access Group

CAPIF Common API Framework for 3GPP northbound APIs

CH Credentials Holder

CHF Charging Function

CN PDB Core Network Packet Delay Budget

CP Control Plane

CQRCI Clock Quality Reporting Control Information

DAPS Dual Active Protocol Stacks

DCCF Data Collection Coordination Function

DCS Default Credentials Server

DetNet Deterministic Networking

DL Downlink

DN Data Network

DNAI DN Access Identifier

DNN Data Network Name

DRX Discontinuous Reception

DS-TT Device-side TSN translator

EAC Early Admission Control

ePDG evolved Packet Data Gateway

EBI EPS Bearer Identity

EUI Extended Unique Identifier

FAR Forwarding Action Rule

FL Federated Learning

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

FN-RG Fixed Network RG

FQDN Fully Qualified Domain Name

GBA Generic Bootstrapping Architecture

GEO Geostationary Orbit

GFBR Guaranteed Flow Bit Rate

GIN Group ID for Network Selection

GMLC Gateway Mobile Location Centre

GPSI Generic Public Subscription Identifier

GUAMI Globally Unique AMF Identifier

HMTC High-Performance Machine-Type Communications

HR Home Routed (roaming)

IAB Integrated access and backhaul

IMEI/TAC IMEI Type Allocation Code

IPUPS Inter PLMN UP Security

I-SMF Intermediate SMF

I-UPF Intermediate UPF

LADN Local Area Data Network

LBO Local Break Out (roaming)

LEO Low Earth Orbit

LMF Location Management Function

LoA Level of Automation

LPP LTE Positioning Protocol

LRF Location Retrieval Function

L4S Low Latency, Low Loss and Scalable Throughput

MBS Multicast/Broadcast Service

MBSF Multicast/Broadcast Service Function

MBSR Mobile Base Station Relay

MBSTF Multicast/Broadcast Service Transport Function

MB-SMF Multicast/Broadcast Session Management Function

MB-UPF Multicast/Broadcast User Plane Function

MEO Medium Earth Orbit

MFAF Messaging Framework Adaptor Function

MCX Mission Critical Service

MDBV Maximum Data Burst Volume

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MINT Minimization of Service Interruption

ML Machine Learning

MPQUIC Multi-Path QUIC

MPS Multimedia Priority Service

MPTCP Multi-Path TCP Protocol

MTLF Model Training Logical Function

N3IWF Non-3GPP InterWorking Function

N3QAI Non-3GPP QoS Assistance Information

N5CW Non-5G-Capable over WLAN

NAI Network Access Identifier

NAT Network Address Translation

NCR Network Controlled Repeater

NCR-MT NCR Mobile Termination

NEF Network Exposure Function

NF Network Function

NGAP Next Generation Application Protocol

NID Network identifier

NPN Non-Public Network

NR New Radio

NRF Network Repository Function

NS-AoS Network Slice Area of Service

NSAC Network Slice Admission Control

NSACF Network Slice Admission Control Function

NSAG Network Slice AS Group

NSI ID Network Slice Instance Identifier

NSSAA Network Slice-Specific Authentication and Authorization

NSSAAF Network Slice-specific and SNPN Authentication and Authorization Function

NSSAI Network Slice Selection Assistance Information

NSSF Network Slice Selection Function

NSSP Network Slice Selection Policy

NSSRG Network Slice Simultaneous Registration Group

NSWO Non-Seamless WLAN offload

NSWOF Non-Seamless WLAN offload Function

NW-TT Network-side TSN translator

NWDAF Network Data Analytics Function

ONN Onboarding Network

ON-SNPN Onboarding Standalone Non-Public Network

PCF Policy Control Function

PDB Packet Delay Budget

PDR Packet Detection Rule

PDU Protocol Data Unit

PDV Packet Delay Variation

PEGC PIN Element with Gateway Capability

PEI Permanent Equipment Identifier

PEMC PIN Element with Management Capability

PER Packet Error Rate

PFD Packet Flow Description

PIN Personal IoT Network

PINE PIN Element

PLR Packet Loss Rate

PNI-NPN Public Network Integrated Non-Public Network

PPD Paging Policy Differentiation

PPF Paging Proceed Flag

PPI Paging Policy Indicator

PSA PDU Session Anchor

PSDB PDU Set Delay Budget

PSER PDU Set Error Rate

PSIHI PDU Set Integrated Handling Information

PTP Precision Time Protocol

PVS Provisioning Server

QFI QoS Flow Identifier

QMC QoE Measurement Collection

QoE Quality of Experience

RACS Radio Capabilities Signalling optimisation

(R)AN (Radio) Access Network

RG Residential Gateway

RIM Remote Interference Management

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSN Redundancy Sequence Number

RTT Round Trip Time

SA NR Standalone New Radio

SBA Service Based Architecture

SBI Service Based Interface

SCP Service Communication Proxy

SD Slice Differentiator

SEAF Security Anchor Functionality

SEPP Security Edge Protection Proxy

SF Service Function

SFC Service Function Chain

SMF Session Management Function

SMSF Short Message Service Function

SN Sequence Number

SNPN Stand-alone Non-Public Network

S-NSSAI Single Network Slice Selection Assistance Information

SO-SNPN Subscription Owner Standalone Non-Public Network

SSC Session and Service Continuity

SSCMSP Session and Service Continuity Mode Selection Policy

SST Slice/Service Type

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

SV Software Version

TA Tracking Area

TAI Tracking Area Identity

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TNL Transport Network Layer

TNLA Transport Network Layer Association

TSC Time Sensitive Communication

TSCAC TSC Assistance Container

TSCAI Traffic Assistance Information

TSCTSF Time Sensitive Communication and Time Synchronization Function

TSN Time Sensitive Networking

TSN GM TSN Grand Master

TSP Traffic Steering Policy

TSS Timing Synchronization Status

TT TSN Translator

TWIF Trusted WLAN Interworking Function

UAS NF Uncrewed Aerial System Network Function

UCMF UE radio Capability Management Function

UDM Unified Data Management

UDR Unified Data Repository

UDSF Unstructured Data Storage Function

UL Uplink

UL CL Uplink Classifier

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

URRP-AMF UE Reachability Request Parameter for AMF

URSP UE Route Selection Policy

VID VLAN Identifier

VLAN Virtual Local Area Network

W-5GAN Wireline 5G Access Network

W-5GBAN Wireline BBF Access Network

W-5GCAN Wireline 5G Cable Access Network

W-AGF Wireline Access Gateway Function

\* \* \* \* Second change \* \* \*

#### 5.6.10.1 Support of IP PDU Session type

The IP address allocation is defined in clause 5.8.1

The UE may acquire following configuration information from the SMF, during the lifetime of a PDU Session:

- Address(es) of P-CSCF(s);

- Address(es) of DNS server(s).

- If the UE indicates support of DNS with security as defined in TS 33.501 [29] to the network in PCO and the network wants to enforce the use of DNS with security, the configuration information sent by the SMF via PCO may also include the corresponding DNS server security information as specified in TS 24.501 [47] and TS 33.501 [29].

- the GPSI of the UE.

The UE may acquire from the SMF, at PDU Session Establishment, the MTU that the UE shall consider, see clause 5.6.10.4.

The UE may provide following information to the SMF during the lifetime of a PDU Session:

- an indication of the support of P-CSCF re-selection based on procedures specified in TS 24.229 [62] (clauses B.2.2.1C and L.2.2.1C).

- PS data off status of the UE.

NOTE 2: An operator can deploy NAT functionality in the network; a UPF supporting NAT functionality can register this capability with the NRF and the UPF can expose mapping between public and private IP addresses.

\* \* \* \* Third of change \* \* \*

### 6.2.3 UPF

The User plane function (UPF) includes the following functionality. Some or all of the UPF functionalities may be supported in a single instance of a UPF:

- Anchor point for Intra-/Inter-RAT mobility (when applicable).

- Allocation of UE IP address/prefix (if supported) in response to SMF request.

- External PDU Session point of interconnect to Data Network.

- Packet routing & forwarding (e.g. support of Uplink classifier to route traffic flows to an instance of a data network, support of Branching point to support multi-homed PDU Session, support of traffic forwarding within a 5G VN group (UPF local switching, via N6, via N19)).

- Packet inspection (e.g. Application detection based on service data flow template and the optional PFDs received from the SMF in addition, IP or MAC filter-based packet detection, and the packet detection based on other means, e.g. application 7 DPI)

- User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering).

- Lawful intercept (UP collection).

- Traffic usage reporting.

- QoS handling for user plane, e.g. UL/DL rate enforcement, Reflective QoS marking in DL.

- Uplink Traffic verification (SDF to QoS Flow mapping).

- Transport level packet marking in the uplink and downlink.

- Downlink packet buffering and downlink data notification triggering.

- Sending and forwarding of one or more "end marker" to the source NG-RAN node.

- Functionality to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs. The UPF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request.

- Packet duplication in downlink direction and elimination in uplink direction in GTP-U layer.

- NW-TT functionality.

- High latency communication, see clause 5.31.8.

- ATSSS Steering functionality to steer the MA PDU Session traffic, refer to clause 5.32.6.

NOTE 1: Not all of the UPF functionalities are required to be supported in an instance of user plane function of a Network Slice.

- Inter PLMN UP Security (IPUPS) functionality, specified in clause 5.8.2.14.

- Event exposure, including exposure of network information, i.e. the QoS monitoring information, as specified in clause 5.8.2.18, events as specified in clause 5.2.26.2 of TS 23.502 [3], exposure of data collected for analytics, as specified in clause 5.2.26.2 of TS 23.502 [3] and exposure of the TSC management information as specified in clause 5.8.5.14.

- Exposure of the UE information, e.g. UE IP address translation information as specified in clause 5.2.26.3 of TS 23.502 [3] and clause 4.15.10 of TS 23.502 [3] if Network address translation (i.e. NAT) functionality of the UE IP address is deployed within UPF.

- Support PDU Set Handling as defined in clause 5.37.5.

- NAT information exposure functionaility (if NAT is deployed within UPF).

NOTE 2: SMF may become aware of the Packet inspection functionality or the NAT information exposure functionality via N4 Node Level Procedures as specified in clause 4.4.3 of TS 23.502 [3], or the SMF may utilize the NRF to discover UPF(s) that supports Packet inspection functionality or NAT information exposure functionality as specified in clause 4.17 of TS 23.502 [3].

\* \* \* \* Fourth change \* \* \*

#### 6.2.6.2 NF profile

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

- NF instance ID.

- NF type.

- PLMN ID in the case of PLMN, PLMN ID + NID in the case of SNPN.

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

- FQDN or IP address of NF.

- NF capacity information.

- NF priority information.

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

- NF Set ID.

- NF Service Set ID of the NF service instance.

- NF Specific Service authorization information.

- if applicable, Names of supported services.

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

- Identification of stored data/information.

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

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

- Location information for the NF instance.

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

- TAI(s).

- NF load information.

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

- For UDM, AUSF and NSSAAF in the case of access to an SNPN using credentials owned by a Credentials Holder with AAA Server, identification of Credentials Holder (i.e. the realm of the Network Specific Identifier based SUPI).

- For UDM and AUSF, and if UDM/AUSF is used for access to an SNPN using credentials owned by a Credentials Holder, identification of Credentials Holder (i.e. the realm if Network Specific Identifier based SUPI is used or the MCC and MNC if IMSI based SUPI is used); see clause 5.30.2.1.

- For AUSF and NSSAAF in the case of SNPN Onboarding using a DCS with AAA server, identification of DCS (i.e. the realm of the Network Specific Identifier based SUPI).

- For UDM and AUSF, and if UDM/AUSF is used as DCS in the case of SNPN Onboarding, identification of DCS (i.e. the realm if Network Specific Identifier based SUPI, or the MCC and MNC if IMSI based SUPI).

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

- For the UPF, see clause 5.2.7.2.2 of TS 23.502 [3].

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

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

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

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

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

- For NWDAF, the following information are supported:

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

- NWDAF Serving Area information (i.e. list of TAIs for which the NWDAF can provide services and/or data).

- Supported Analytics Delay per Analytics ID (if available).

- NF types of the NF data sources, NF Set IDs of the NF data sources, if available.

- Analytics aggregation capability (if available).

- Analytics metadata provisioning capability (if available).

- ML model Filter information parameters include S-NSSAI(s) and Area(s) of Interest for the trained ML model(s) per Analytics ID(s).

- ML Model Interoperability indicator (if available) per Analytics ID(s).

- FL capability information per analytics ID including FL capability type (i.e. FL server and/or FL client, if available).

- Time interval supporting FL (if available).

- Accuracy checking capability for ML model accuracy monitoring or Analytics Accuracy Monitoring (if available).

- Roaming exchange capability (if available).

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

NOTE 5: The Analytics IDs supported by the NWDAF may be associated with a Supported Analytics Delay i.e. the Analytics report can be generated with a time (including data collection delay and inference delay) in less than or equal to the Supported Analytics Delay.

NOTE 6: The determination of Supported Analytics Delay, and how the NWDAF avoid updating its Supported Analytics Delay in NRF frequently is NWDAF implementation specific.

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

- Event Exposure service supported event ID(s) by UPF.

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

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

NOTE 7: This is applicable when NEF exposes AF information for analytics purpose as detailed in TS 23.288 [86].

NOTE 8: It is expected service authorization information is usually provided by OA&M system, and it can also be included in the NF profile in the case that e.g. an NF instance has an exceptional service authorization information.

NOTE 9: The NRF may store a mapping between UDM Group ID and SUPI(s), UDR Group ID and SUPI(s), AUSF Group ID and SUPI(s) and PCF Group ID and SUPI(s), to enable discovery of UDM, UDR, AUSF and PCF using SUPI, SUPI ranges as specified in clause 6.3 or interact with UDR to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID based on UE identity, e.g. SUPI (see clause 6.3.1 for details).

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

- SCP Domain the NF belongs to.

- DCCF Serving Area information, NF types of the data sources, NF Set IDs of the data sources, if available, in the case of DCCF.

- Supported DNAI list, in the case of SMF.

- For SNPN, capability to support SNPN Onboarding in the case of AMF and capability to support User Plane Remote Provisioning in the case of SMF.

- IP address range, DNAI for UPF.

- Supported DNS security protocols, in the case of EASDF.

- Additional V2X related NF profile parameters are defined in TS 23.287 [121].

- Additional ProSe related NF profile parameters are defined in TS 23.304 [128].

- Additional MBS related NF profile parameters are defined in TS 23.247 [129].

- Additional UAS related NF profile parameters are defined in TS 23.256 [136].

- Additional Ranging based services and Sidelink Positioning related NF profile parameters are defined in TS 23.586 [180].

- For additional information in PCF profile, see clause 5.2.7.2.2 of TS 23.502 [3].

\* \* \* \* Fifth change \* \* \*

### 6.3.3 User Plane Function Selection

#### 6.3.3.1 Overview

The selection and reselection of the UPF for PDU session establishment, UE mobility or UE traffic offloading are performed by the SMF by considering UPF deployment scenarios such as centrally located UPF and distributed UPF located close to or at the Access Network site. The selection of the UPF shall also enable deployment of UPF with different capabilities, e.g. UPFs supporting no or a subset of optional functionalities.

When the UPF selection for PDU session establishment takes place in home routed roaming case, the UPF(s) in home PLMN is selected by SMF(s) in HPLMN, and the UPF(s) in the VPLMN is selected by SMF(s) in VPLMN. The exact set of parameters used for the selection mechanism is deployment specific and controlled by the operator configuration.

The UPF selection for PDU session establishment, UE mobility or UE traffic offloading involves:

- A step of SMF Provisioning of available UPF(s) (details are described in clause 6.3.3.2). This step may take place while there is no PDU Session to establish and is followed by N4 Node Level procedures defined in clause 4.4.3 of TS 23.502 [3] where the UPF and the SMF may exchange information such as the support of optional functionalities and capabilities.

- A step of selection of an UPF for a particular PDU Session (details are described in clause 6.3.3.3) which is followed by N4 session management procedures defined in clause 4.4.1 of TS 23.502 [3].

The selection and reselection of the UPF is also performed by an NF (other than the SMF) in order to collect the data from the UPF as defined in clause 5.8.2.17. In this case, the related dedicated UPF is discovered and selected as follows:

- When the NF consumer or SCP directly subscribes to the UPF (if allowed by the conditions defined in clause 5.8.2.17), the NF consumer or SCP queries the NRF including the related discovery parameters. The NRF returns the UPF(s) which meet(s) the discovery request.

- When the NF consumer or SCP shall subscribe via the SMF, the NF consumer gets the serving SMF information from the UDM per SUPI, DNN and S-NSSAI. After that, the NF consumer sends a subscription to the indicated SMF and the SMF identifies the related UPF(s) using the parameters of the subscription (e.g. target flow description, AoI, etc.) and transfers the related event subscription information to the identified UPF(s). If the NF consumer does not know the SUPI but only the UE IP address, it may need to invoke the BSF to get the SUPI corresponding to the triplet (UE IP address, DNN and S-NSSAI).

#### 6.3.3.2 SMF Provisioning of available UPF(s)

SMF may be locally configured with the information about the available UPFs, e.g. by OAM system when a UPF is instantiated or removed, or the SMF may become aware of a UPF via a UPF initiated N4 Association establishment (as described in clause 4.4.3 of TS 23.502 [3]).

NOTE 1: UPF information can be updated e.g. by OAM system any time after the initial provisioning, or UPF itself updates its information to the SMF via N4 node level procedures anytime after N4 Association establishment.

The UPF selection functionality in the SMF may optionally utilize the NRF to discover UPF(s). In this case, the SMF issues a request to the NRF that may include following parameters: DNN, S-NSSAI, SMF Area Identity, the requested functionalities and capabilities (e.g. ATSSS steering capabilities, functionality associated with high data rate low latency service, NAT information exposure functionaility, packet inspection functionaility etc.). In its answer, the NRF provides the NF profile(s) that include(s) the IP address(es) or the FQDN of the N4 interface of corresponding UPF(s) to the SMF.

UPFs may be associated with an SMF Area Identity in the NRF. This 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 in the case that an SMF is only allowed to control UPF(s) configured in NRF as belonging to a certain SMF Area Identity.

The NRF may be configured by OAM with information on the available UPF(s) or the UPF(s) may register its/their NF profile(s) in the NRF. This is further defined in clause 4.17 of TS 23.502 [3].

#### 6.3.3.3 Selection of an UPF for a particular PDU Session

The following parameter(s) and information may be considered by the SMF for UPF selection and re-selection:

- UPF's dynamic load.

- Analytics (i.e. statistics or predictions) for UPF load, Service Experience analytics and/or DN Performance analytics per UP path (including UPF and/or DNAI and/or AS instance) and UE related analytics (UE mobility, UE communication, and expected UE behavioural parameters) as received from NWDAF (see TS 23.288 [86]), if NWDAF is deployed.

- UPF's relative static capacity among UPFs supporting the same DNN.

- UPF location available at the SMF.

- UE location information.

- Capability of the UPF and the functionality required for the particular UE session: An appropriate UPF can be selected by matching the functionality and features required for an UE. These functionalities may also include NAT information exposure functionaility and packet inspection functionaility (see clause 6.2.3).

- Data Network Name (DNN).

- PDU Session Type (i.e. IPv4, IPv6, IPv4v6, Ethernet Type or Unstructured Type) and if applicable, the static IP address/prefix.

- SSC mode selected for the PDU Session.

- UE subscription profile in UDM which may include UPF functionalities that are required and/or preferred for the particular UE session. Preferred UPF functionalities are optional and a subset or none of them may be supported by the selected UPF.

- DNAI as included in the PCC Rules and described in clause 5.6.7.

- Local operator policies.

- S-NSSAI.

- Access technology being used by the UE.

- Information related to user plane topology and user plane terminations, that may be deduced from:

- 5G-AN-provided identities (e.g. CellID, TAI), available UPF(s) and DNAI(s);

- Identifiers (i.e. a FQDN and/or IP address(es)) of N3 terminations provided by a W-AGF or a TNGF or a TWIF;

NOTE 1: A W-AGF or a TNGF may provide Identifiers of its N3 terminations when forwarding over N2 uplink NAS signalling to the 5GC. The AMF may relay this information to the SMF, as part of session management signalling for a new PDU Session.

- Information regarding the user plane interfaces of UPF(s). This information may be acquired by the SMF using N4;

- Information regarding the N3 User Plane termination(s) of the AN serving the UE. This may be deduced from 5G-AN-provided identities (e.g. CellID, TAI);

- Information regarding the N9 User Plane termination(s) of UPF(s) if needed;

- Information regarding the User plane termination(s) corresponding to DNAI(s).

- RSN, support for redundant GTP-U path or support for redundant transport path in the transport layer (as in clause 5.33.2) when redundant UP handling is applicable.

- Information regarding the ATSSS Steering Capability of the UE session (e.g. any combination of ATSSS-LL capability, MPTCP capability, MPQUIC capability) and information on the UPF support of RTT measurements without PMF.

- Support for UPF allocation of IP address/prefix.

- Support of the IPUPS functionality, specified in clause 5.8.2.14.

- Support for High latency communication (see clause 5.31.8).

- Support for 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).

- User Plane Latency Requirements within AF request (see clause 5.6.7.1 and clause 6.3.6 of TS 23.548 [130]).

- List of supported Event ID(s) for exposure of UPF-related information via service based interface (see clause 7.2.29 and clause 5.2.26.2 of TS 23.502 [3]).

NOTE 2: How the SMF determines information about the user plane network topology from information listed above, and what information is considered by the SMF, is based on operator configuration.

NOTE 3: In this release the SMF uses no additional parameters for UPF selection for a PDU Session serving TSC or Deterministic Networking. If a PDU Session needs to connect to a specific UPF hosting a specific TSN 5GS bridge or 5GS router, this can be achieved e.g. by using a dedicated DNN/S-NSSAI combination.

If there is an existing PDU Session, and the SMF receives another PDU Session request to the same DNN and S-NSSAI, and if the SMF determines that interworking with EPC is supported for this PDU Session (as specified in clause 4.11.5 of TS 23.502 [3]), the SMF should select the same UPF if it supports all capabilities required for the new PDU Session. Otherwise, if the SMF determines that interworking with EPC is not supported for the new PDU Session or the UPF of the existing PDU Session does not support all capabilities required for the new PDU Session, a different UPF may be selected according to operator policy.

For the same DNN and S-NSSAI if different UPFs are selected at 5GC, when the UE is moved to EPC network, there is no requirement to enforce APN-AMBR. Whether and how to apply APN-AMBR for the PDN Connection associated with this DNN/APN is implementation dependent, e.g. possibly only AMBR enforcement per PDU Session applies.

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