3GPP TS 23.501 V2.0.1 (2017-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
System Architecture for the 5G System;
Stage 2
(Release 15)

Keywords

3GPP, Architecture, 5G System, NextGen

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the Stage 2 system architecture for the 5G System. The 5G System provides data connectivity and services.

This specification covers both roaming and non-roaming scenarios in all aspects, including interworking between 5GS and EPS, mobility within 5GS, policy control and charging, and authentication.

ITU-T Recommendation I.130 [11] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [12] defines Stage 2 of the method.

TS 23.502 [3] contains the stage 2 procedures and flows for 5G System and it is a companion specification to this specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[5] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS); Stage 2".

[6] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface: Stage 3".

[7] IETF RFC 7157: "IPv6 Multihoming without Network Address Translation".

[8] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

[9] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[10] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[11] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[12] ITU-T Recommendation Q.65: "The unified functional methodology for the characterization of services and network capabilities".

[13] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS): Stage 3".

[14] IETF RFC 3736: "Stateless DHCP Service for IPv6".

[15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16] 3GPP TS 22.173: "IMS Multimedia Telephony Service and supplementary services; Stage 1".

[17] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station in idle mode".

[18] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[19] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[20] IETF RFC 4282: "The Network Access Identifier".

[21] 3GPP TS 23.002: "Network Architecture".

[22] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows; Stage 2".

[23] 3GPP TS 23.221: "Architectural requirements".

[24] 3GPP TS 22.153: "Multimedia priority service".

[25] 3GPP TS 22.011: "Service Accessibility".

[26] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[27] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

[28] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol Specification".

[29] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[30] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[31] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[32] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".

[33] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Service aspects; Service principles".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[35] 3GPP TS 33.106: "Lawful Interception Requirements".

[36] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[37] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[38] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[39] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[40] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[41] 3GPP TS 32.240: "Charging management; Charging architecture and principles".

[42] 3GPP TS 38.401: "NG-RAN Architecture description".

[43] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[44] IETF RFC 4960: "Stream Control Transmission Protocol".

[45] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[46] 3GPP TS 23.041: "Public Warning System".

[47] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[48] 3GPP TS 24.502: "Access to the 5G System (5GS) via non-3GPP access networks; Stage 3".

[49] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[50] 3GPP TS 38.304: "NR; User Equipment (UE) procedures in idle mode".

[51] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[52] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[53] IETF RFC 1027: "Using ARP to Implement Transparent Subnet Gateways".

[54] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[55] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[56] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".[57] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[58] 3GPP TS 29.510: "5G System: Network function repository services; Stage 3".

[59] 3GPP TS 29.502: "5G System: Session Management Services: Stage 3".

[60] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2) ".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

5G Access Network: An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network.

5G Core Network: The core network specified in the present document. It connects to a 5G Access Network.

5G QoS Flow: The finest granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receive the same forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different QoS forwarding treatment requires separate 5G QoS Flow.

5G QoS Identifier: A scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow. This may be implemented in the access network by the 5QI referencing node specific parameters that control the QoS forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

5G System: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE.

Allowed NSSAI: NSSAI provided by the Serving PLMN during e.g. a registration procedure, indicating the S-NSSAIs values to be used by the UE in the Serving PLMN for the current registration area.

Allowed Area: Area where the UE is allowed to initiate communication as specified in clause 5.3.2.3.

AMF Region: An AMF Region consists of one or multiple AMF Sets.

AMF Set: An AMF Set consists of some AMFs that serve a given area and Network Slice. Multiple AMF Sets may be defined per AMF Region and Network Slice(s).

Application identifier: An identifier that can be mapped to a specific application traffic detection rule.

Configured NSSAI: NSSAI provisioned in the UE per PLMN.

DN Access Identifier (DNAI): Identifier of a user plane access to one or more DN(s) where applications are deployed.

Expected UE Behaviour: Set of parameters provisioned by an external party to 5G network functions on the foreseen or expected UE behaviour, see clause 5.20.

Forbidden Area: An area where the UE is not allowed to initiate communication as specified in clause 5.3.2.3.

Initial Registration: UE registration in RM-DEREGISTERED state as specified in clause 5.3.2.

Local Area Data Network: a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.

Local Break Out (LBO): Roaming scenario for a PDU Session where the PDU Session Anchor and its controlling SMF are located in the serving PLMN (VPLMN).

Mobility Pattern: Network concept of determining within the AMF the UE mobility parameters as specified in clause 5.3.2.4.

Mobility Registration update: UE re-registration when entering new TA outside the TAI List as specified in clause 5.3.2.

MPS-subscribed UE: A UE having a USIM with MPS subscription.

NGAP UE association: The logical per UE association between a 5G-AN node and an AMF.

NGAP UE-TNLA-binding: The binding between a NGAP UE association and a specific TNL association for a given UE.

Network Function: A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces.

NOTE 2: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

Network instance: Information identifying a domain. Used by the UPF for traffic detection and routing in case of different IP domains or overlapping IP addresses.

Network Slice: A logical network that provides specific network capabilities and network characteristics.

Network Slice instance: A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.

NSI ID: an identifier for a Network Slice instance.

NF service: a functionality exposed by a NF through a service based interface and consumed by other authorized NFs.

NF service operation: An elementary unit a NF service is composed of.

NG-RAN: A radio access network that supports one or more of the following options with the common characteristics that it connects to 5GC:

1) Standalone New Radio.

2) New Radio is the anchor with E-UTRA extensions.

3) Standalone E-UTRA.

4) E-UTRA is the anchor with New Radio extensions.

Non-Allowed area: Area where the UE is allowed to initiate registration procedure but no other communication as specified in clause 5.3.2.3.

Non-Seamless Non-3GPP offload: The offload of user plane traffic via non-3GPP access without traversing either N3IWF or UPF.

PDU Connectivity Service: A service that provides exchange of PDUs between a UE and a Data Network.

PDU Session: Association between the UE and a Data Network that provides a PDU connectivity service.

PDU Session Type: The type of PDU Session which can be IPv4, IPv6, Ethernet or Unstructured.

Periodic Registration update: UE re-registration at expiry of periodic registration timer as specified in clause 5.3.2.

(Radio) Access Network: See 5G Access Network.

Requested NSSAI: NSSAI provided by the UE to the Serving PLMN during registration.

Service based interface: It represents how a set of services is provided/exposed by a given NF.

Service Continuity: The uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point change.

Service Data Flow Filter: A set of packet flow header parameter values/ranges used to identify one or more of the packet (IP or Ethernet) flows constituting a Service Data Flow.

Service Data Flow Template: The set of Service Data Flow filters in a policy rule or an application identifier in a policy rule referring to an application detection filter, required for defining a Service Data Flow.

Session Continuity: The continuity of a PDU Session. For PDU Session of IPv4 or IPv6 type "session continuity" implies that the IP address is preserved for the lifetime of the PDU Session.

Subscribed S-NSSAI: S-NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN

UPF Service Area: The area within which PDU Session associated with the UPF can be served by (R)AN nodes via a N3 interface between the (R)AN and the UPF without need to add a new UPF in between or to remove/re-allocate the UPF.

Uplink Classifier: UPF functionality that aims at diverting Uplink traffic, based on filter rules provided by SMF, towards Data Network.

For the purposes of the present document, the following terms and definitions given in TS 33.501 [29] apply:

Subscription Concealed Identifier

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
5GS	5G System
5G-AN	5G Access Network
5G-GUTI	5G Globally Unique Temporary Identifier
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility Management Function
AS	Access Stratum
AUSF	Authentication Server Function
CP	Control Plane
DL	Downlink
DN	Data Network
DNAI	DN Access Identifier
DNN	Data Network Name
FQDN	Fully Qualified Domain Name

GFBR	Guaranteed Flow Bit Rate
GMLC	Gateway Mobile Location Centre
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
HR	Home Routed (roaming)
LADN	Local Area Data Network
LBO	Local Break Out (roaming)
LMF	Location Management Function
LRF	Location Retrieval Function
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only
N3IWF	Non-3GPP InterWorking Function
NAI	Network Access Identifier
NEF	Network Exposure Function
NF	Network Function
NR	New Radio
NRF	Network Repository Function
NSI ID	Network Slice Instance Identifier
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSP	Network Slice Selection Policy
PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PER	Packet Error Rate
PFD	Packet Flow Description
PPD	Paging Policy Differentiation
PPI	Paging Policy Indicator
PSA	PDU Session Anchor
QFI	QoS Flow Identifier
QoE	Quality of Experience
(R)AN	(Radio) Access Network
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
SA NR	Standalone New Radio
SBA	Service Based Architecture
SBI	Service Based Interface
SD	Slice Differentiator
SEAF	Security Anchor Functionality
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SSC	Session and Service Continuity
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
UDSF	Unstructured Data Storage Function
UL	Uplink
UL CL	Uplink Classifier
UPF	User Plane Function
UDR	Unified Data Repository
URSP	UE Route Selection Policy

4 Architecture model and concepts

4.1 General concepts

The 5G System architecture is defined to support data connectivity and services enabling deployments to use techniques such as e.g. Network Function Virtualization and Software Defined Networking. The 5G System architecture shall leverage service-based interactions between Control Plane (CP) Network Functions where identified. Some key principles and concept are to:

- Separate the User Plane (UP) functions from the Control Plane (CP) functions, allowing independent scalability, evolution and flexible deployments e.g. centralized location or distributed (remote) location.
- Modularize the function design, e.g. to enable flexible and efficient network slicing.
- Wherever applicable, define procedures (i.e. the set of interactions between network functions) as services, so that their re-use is possible.
- Enable each Network Function to interact with other NF directly if required. The architecture does not preclude the use of an intermediate function to help route Control Plane messages (e.g. like a DRA).
- Minimize dependencies between the Access Network (AN) and the Core Network (CN). The architecture is defined with a converged core network with a common AN - CN interface which integrates different Access Types e.g. 3GPP access and non-3GPP access.
- Support a unified authentication framework.
- Support "stateless" NFs, where the "compute" resource is decoupled from the "storage" resource.
- Support capability exposure.
- Support concurrent access to local and centralized services. To support low latency services and access to local data networks, UP functions can be deployed close to the Access Network.
- Support roaming with both Home routed traffic as well as Local breakout traffic in the visited PLMN.

4.2 Architecture reference model

4.2.1 General

This specification describes the architecture for the 5G System. The 5G architecture is defined as service-based and the interaction between network functions is represented in two ways.

- A service-based representation, where network functions (e.g. AMF) within the Control Plane enables other authorized network functions to access their services. This representation also includes point-to-point reference points where necessary.
- A reference point representation, shows the interaction exist between the NF services in the network functions described by point-to-point reference point (e.g. N11) between any two network functions (e.g. AMF and SMF).

Service-based interfaces are listed in clause 4.2.6. Reference points are listed in clause 4.2.7.

Network functions within the 5GC Control Plane shall only use service-based interfaces for their interactions.

NOTE: The interactions between NF services within one NF will not be specified in this release.

4.2.2 Network Functions and entities

The 5G System architecture consists of the following network functions (NF). The functional description of these network functions is specified in clause 6.

- Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)
- Data Network (DN), e.g. operator services, Internet access or 3rd party services
- Unstructured Data Storage Function (UDSF)
- Network Exposure Function (NEF)

- NF Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- Unified Data Repository (UDR)
- User Plane Function (UPF)
- Application Function (AF)
- User Equipment (UE)
- (Radio) Access Network ((R)AN)
- 5G-Equipment Identity Register (5G-EIR)
- Security Edge Protection Proxy (SEPP)

4.2.3 Non-roaming reference architecture

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

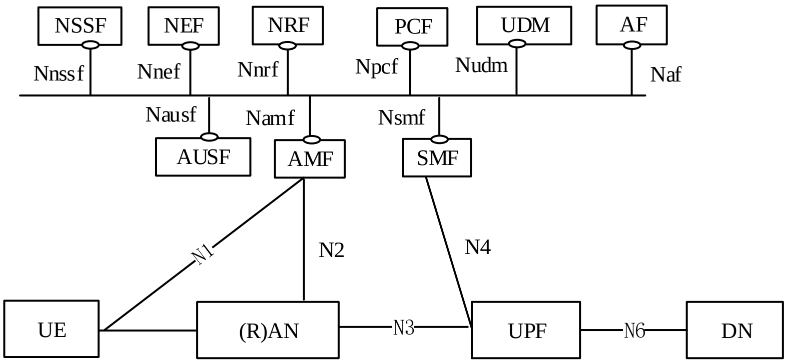


Figure 4.2.3-1: 5G System architecture

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

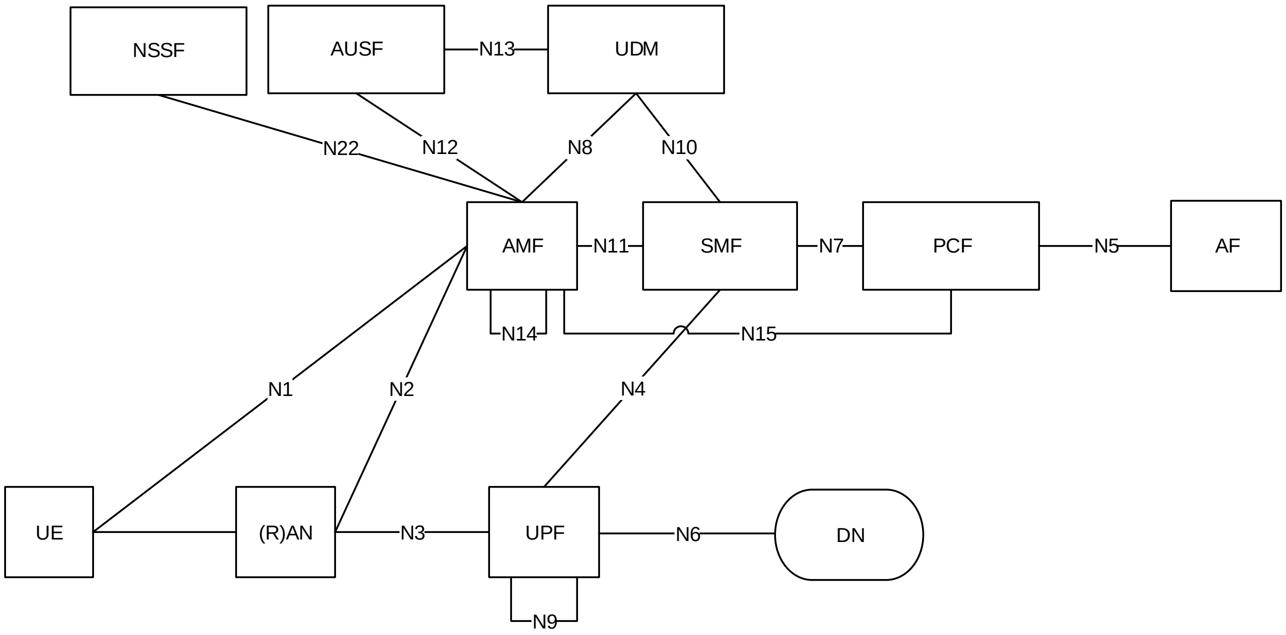


Figure 4.2.3-2: Non-Roaming 5G System Architecture in reference point representation

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

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

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

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

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

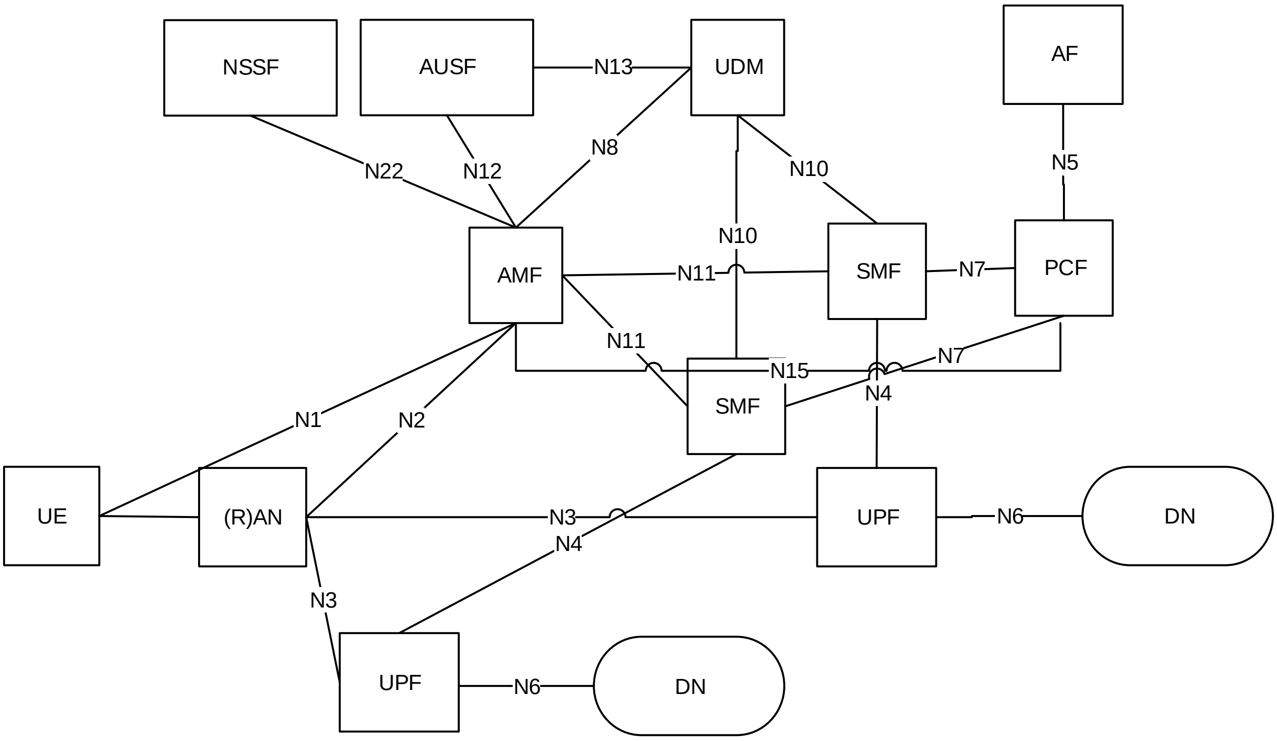


Figure 4.2.3-3: Applying non-roaming 5G System architecture for multiple PDU Session in reference point representation

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

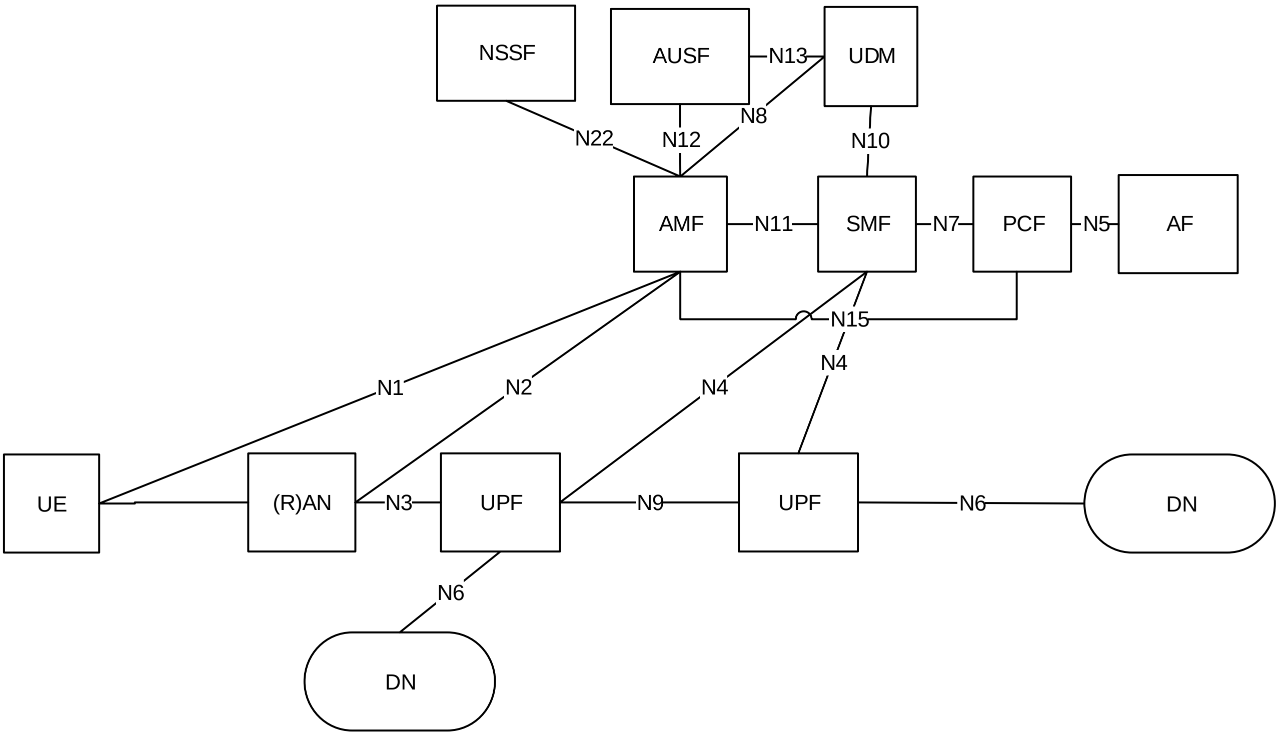


Figure 4.2.3-4: Applying non-roaming 5G System architecture for concurrent access to two (e.g. local and central) data networks (single PDU Session option) in reference point representation

4.2.4 Roaming reference architectures

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

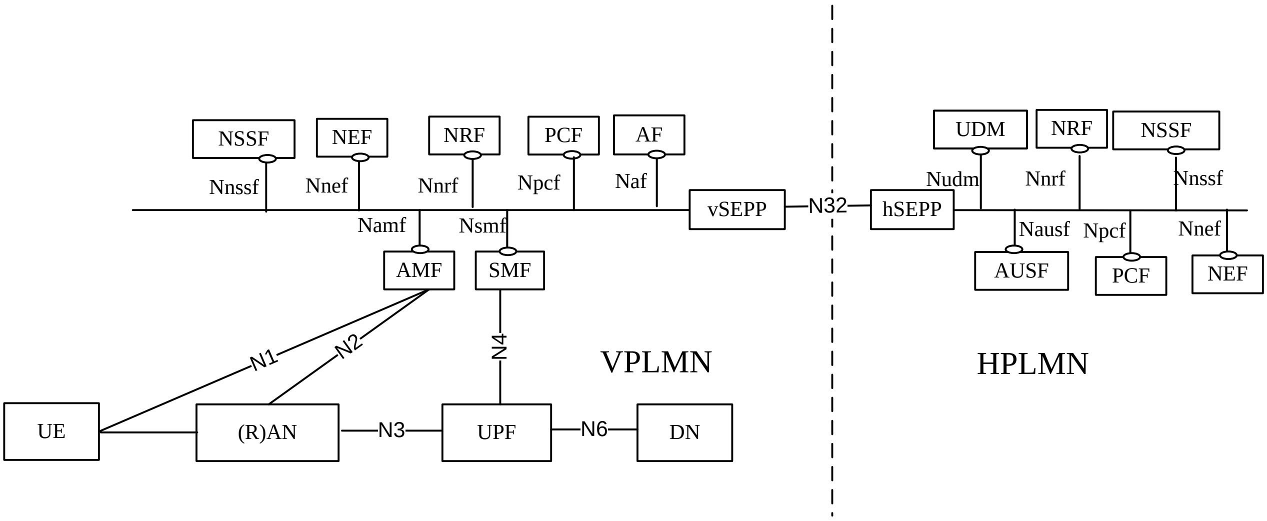


Figure 4.2.4-1 Roaming 5G System architecture- local breakout scenario in service-based interface representation

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

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

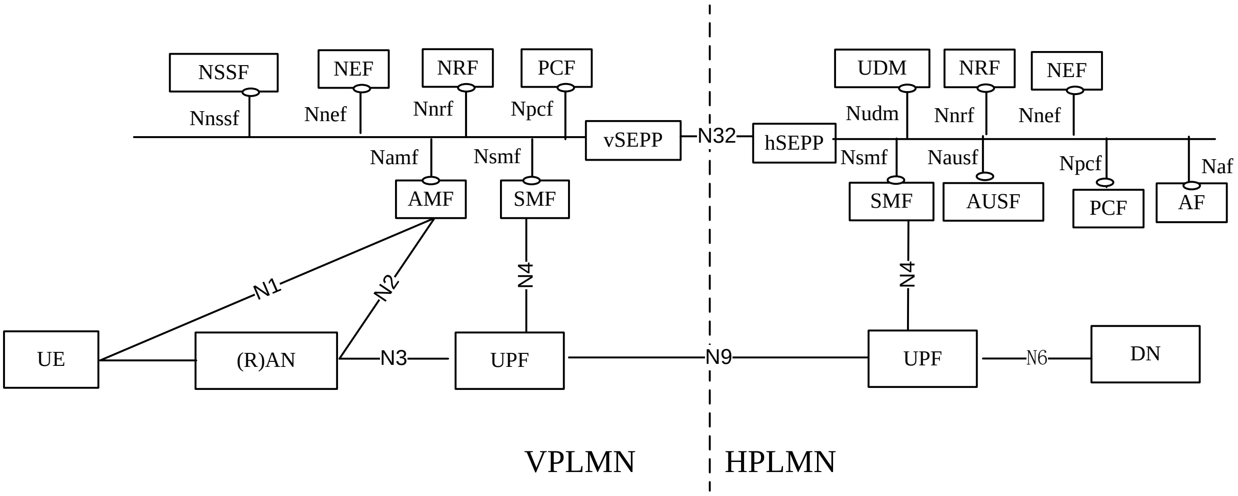


Figure 4.2.4-3 Roaming 5G System architecture - home routed scenario in service-based interface representation

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

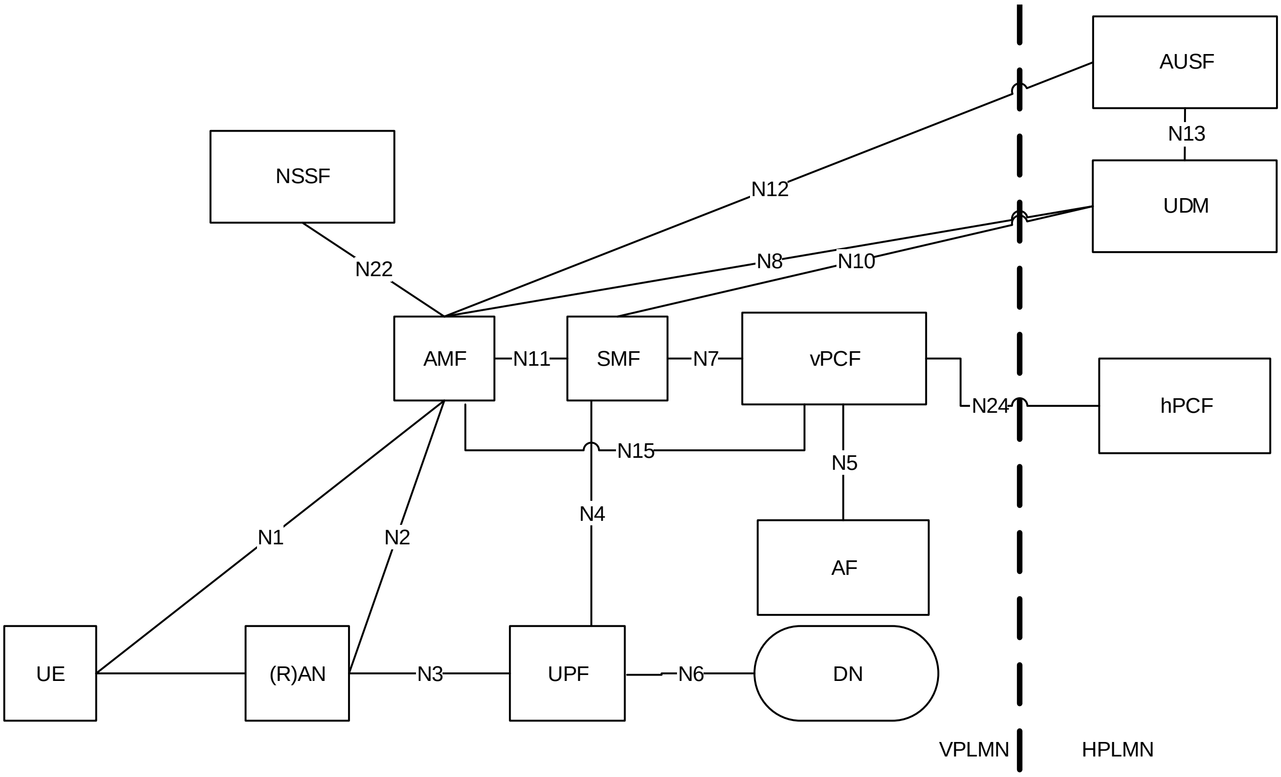


Figure 4.2.4-4: Roaming 5G System architecture - local breakout scenario in reference point representation

NOTE 2: The NRF is not depicted in reference point architecture figures. Refer to Figure 4.2.4-7 for details on NRF and NF interfaces.

NOTE 3: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

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

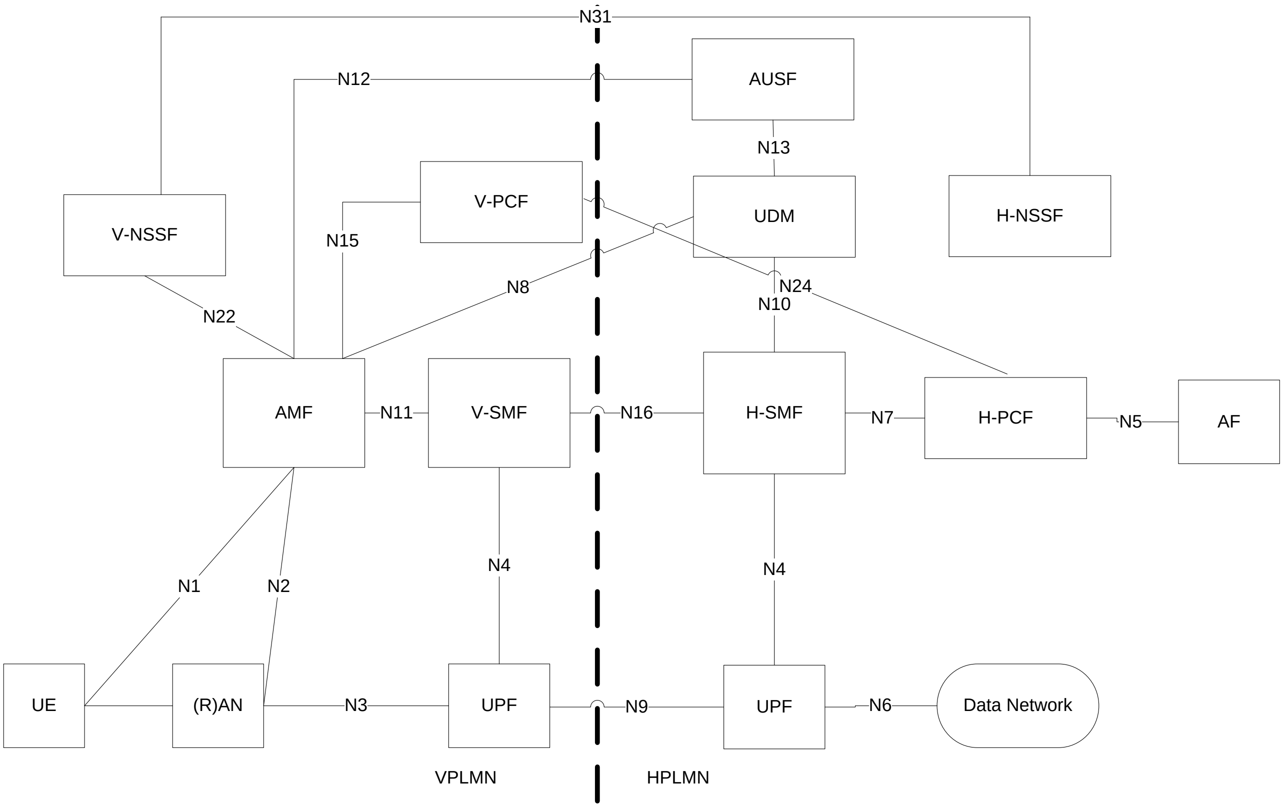


Figure 4.2.4-6: Roaming 5G System architecture-Home routed scenario in reference point representation

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

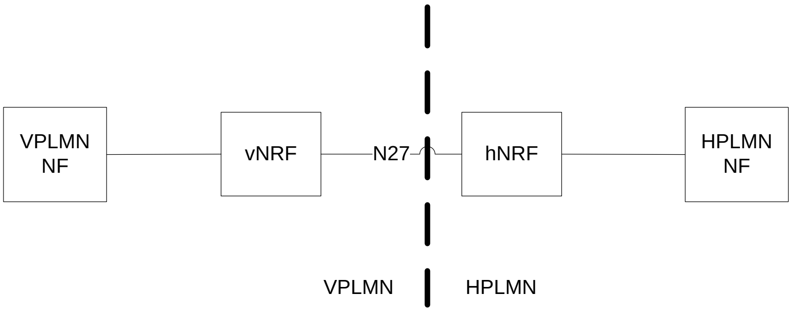


Figure 4.2.4-7: NRF Roaming architecture in reference point representation

NOTE 4: For the sake of clarity, SEPPs are not depicted in figure 4.2.4-7.

4.2.5 Data Storage architectures

As depicted in Figure 4.2.5-1, the 5G System architecture allows any NF to store and retrieve its unstructured data into/from a UDSF (e.g. UE contexts). The UDSF belongs to the same PLMN where the network function is located. CP NFs may share a UDSF for storing their respective unstructured data or may each have their own UDSF (e.g. a UDSF may be located close to the respective NF).

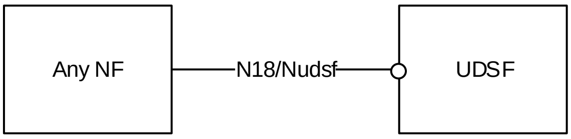


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF

NOTE 1: 3GPP will specify (possibly by referencing) the N18/Nudsf interface.

As depicted in Figure 4.2.5-2, the 5G System architecture allows the UDM, PCF and NEF to store data in the UDR, including subscription data and policy data by UDM and PCF, structured data for exposure and application data (including Packet Flow Descriptions (PFDs) for application detection, application request information for multiple UEs) by the NEF. UDR can be deployed in each PLMN and it can serve different functions as follows:

- UDR accessed by the NEF belongs to the same PLMN where the NEF is located.
- UDR accessed by the UDM belongs to the same PLMN where the UDM is located if UDM supports a split architecture.
- UDR accessed by the PCF belongs to the same PLMN where the PCF is located.

NOTE 2: The UDR deployed in each PLMN can store application data for roaming subscribers.

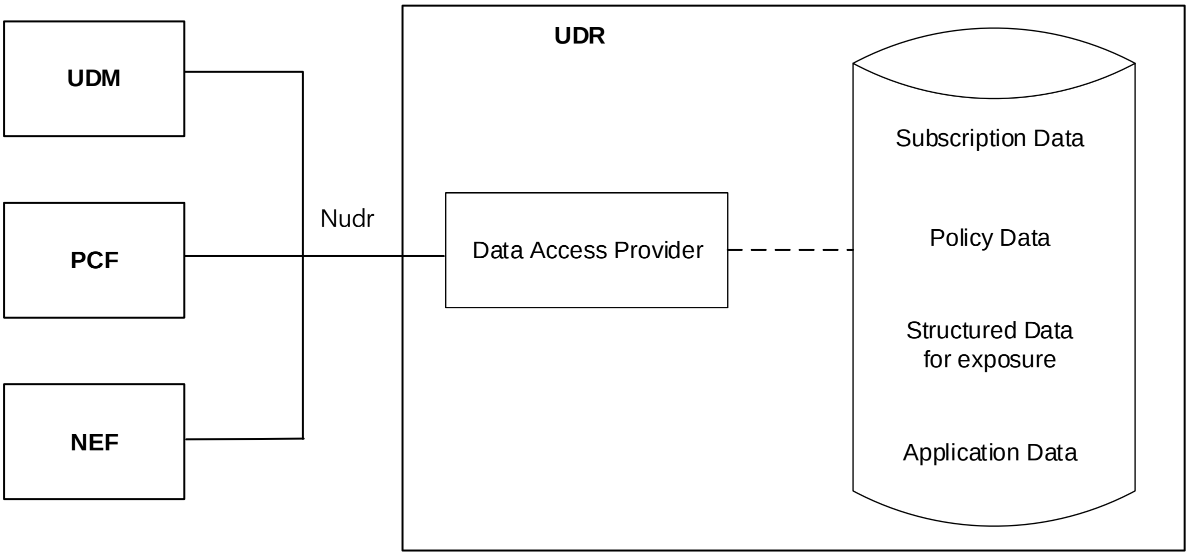


Figure 4.2.5-2: Data storage architecture

NOTE 3: There can be multiple UDRs deployed in the network, each of which can accommodate different data sets or subsets, (e.g. subscription data, subscription policy data, data for exposure, application data) and/or serve different sets of NFs. Deployments where a UDR serves a single NF and stores its data, and, thus, can be integrated with this NF, can be possible.

NOTE 4: The internal structure of the UDR in figure 4.2.5-2 is shown for information only.

The Nudr interface is defined for the network functions, such as UDM, PCF and NEF, to access a particular set of the data stored and to read, update (including add, modify), delete, and subscribe to notification of relevant data changes in the UDR.

Each NF service consumer accessing the UDR, via Nudr, shall be able to add, modify, update or delete only the data it is authorised to change. This authorisation shall be performed by the UDR on a per data set and NF service consumer basis and potentially on a per UE, subscription granularity.

The following data in the UDR sets exposed via Nudr to the respective NF service consumer and stored shall be standardized:

- Subscription Data,

- Policy Data,
- Structured Data for exposure,
- application request information for multiple UEs (as defined in clause 5.6.7).

The content and format/encoding of the 3GPP defined information elements exposed by the data sets shall be standardized.

In addition, it shall be possible to access operator specific data sets by the consumers from the UDR as well as operator specific data for each specific data set, The content and format/encoding of these data or data sets is not subject for standardization.

NOTE 5: The organization of the different data stored in the UDR is not to be standardized.

4.2.6 Service-based interfaces

The 5G System Architecture contains the following service-based interfaces:

Namf: Service-based interface exhibited by AMF.

Nsmf: Service-based interface exhibited by SMF.

Nnef: Service-based interface exhibited by NEF.

Npcf: Service-based interface exhibited by PCF.

Nudm: Service-based interface exhibited by UDM.

Naf: Service-based interface exhibited by AF.

Nnrf: Service-based interface exhibited by NRF.

Nnssf: Service-based interface exhibited by NSSF.

Nausf: Service-based interface exhibited by AUSF.

Nudr: Service-based interface exhibited by UDR.

Nudsf: Service-based interface exhibited by UDSF.

N5g-eir: Service-based interface exhibited by 5G-EIR.

4.2.7 Reference points

The 5G System Architecture contains the following reference points:

N1: Reference point between the UE and the AMF.

N2: Reference point between the (R)AN and the AMF.

N3: Reference point between the (R)AN and the UPF.

N4: Reference point between the SMF and the UPF.

N6: Reference point between the UPF and a Data Network.

NOTE 1: The traffic forwarding details of N6 between a UPF acting as an uplink classifier and a local data network will not be specified in this release.

N9: Reference point between two UPFs.

The following reference points show the interactions that exist between the NF services in the NFs. These reference points are realized by corresponding NF service-based interfaces and by specifying the identified consumer and producer NF service as well as their interaction in order to realize a particular system procedure.

N5: Reference point between the PCF and an AF.

N7: Reference point between the SMF and the PCF.

N24: Reference point between the PCF in the visited network and the PCF in the home network.

N8: Reference point between the UDM and the AMF.

N10: Reference point between the UDM and the SMF.

N11: Reference point between the AMF and the SMF.

N12: Reference point between AMF and AUSF.

N13: Reference point between the UDM and Authentication Server function the AUSF.

N14: Reference point between two AMFs.

N15: Reference point between the PCF and the AMF in case of non-roaming scenario, PCF in the visited network and AMF in case of roaming scenario.

N16: Reference point between two SMFs, (in roaming case between SMF in the visited network and the SMF in the home network).

N17: Reference point between AMF and 5G-EIR.

N18: Reference point between any NF and UDSF.

N22: Reference point between AMF and NSSF.

N27: Reference point between NRF in the visited network and the NRF in the home network.

N31: Reference point between the NSSF in the visited network and the NSSF in the home network.

NOTE 2: in some cases, a couple of NFs may need to be associated with each other to serve a UE.

In addition to the reference points above, there are interfaces/reference point(s) between SMF and the charging system (CDF and OCS). The reference point(s) are not depicted in the architecture illustrations in this specification.

NOTE 3: The functionality of these interface/reference points are defined in TS 32.240 [41].

N32: Reference point between SEPP in the visited network and the SEPP in the home network.

NOTE 4: The functionality of N32 reference point is defined in TS 33.501 [29].

4.2.8 Support of non-3GPP access

4.2.8.1 General Concepts to Support Non-3GPP Access

The 5G Core Network supports the connectivity of the UE via non-3GPP access networks, e.g. WLAN access.

Only the support of non-3GPP access networks deployed outside the NG-RAN (referred to as "standalone" non-3GPP accesses) is described in this clause.

In this release of specification, 5G Core Network only supports untrusted non-3GPP accesses.

Non-3GPP access networks shall be connected to the 5G Core Network via a Non-3GPP InterWorking Function (N3IWF). The N3IWF interfaces the 5G Core Network CP and UP functions via N2 and N3 interfaces, respectively.

The N2 and N3 reference points are used to connect standalone non-3GPP accesses to 5G Core Network control-plane and user-plane functions respectively.

A UE that accesses the 5G Core Network over a standalone non-3GPP access shall, after UE attachment, support NAS signalling with 5G Core Network control-plane functions using the N1 reference point.

When a UE is connected via a NG-RAN and via a standalone non-3GPP access, multiple N1 instances shall exist for the UE i.e. there shall be one N1 instance over NG-RAN and one N1 instance over non-3GPP access.

A UE simultaneously connected to the same 5G Core Network of a PLMN over a 3GPP access and a non-3GPP access shall be served by a single AMF if the selected N3IWF is located in the same PLMN as the 3GPP access.

When a UE is connected to a 3GPP access of a PLMN, if the UE selects the N3IWF and the N3IWF is located in a PLMN different from the PLMN of the 3GPP access, e.g. in a different VPLMN or in the HPLMN, the UE is served separately by the two PLMNs. The UE is registered with two separate AMFs. PDU Sessions over the 3GPP access are served by V-SMFs different from the V-SMF serving the PDU Sessions over the non-3GPP access.

The PLMN selection for the 3GPP access does not depend on the N3IWF selection. If a UE is registered over a non-3GPP, the UE performs PLMN selection for the 3GPP access independently of the PLMN to which the N3IWF belongs.

A UE shall establish an IPSec tunnel with the N3IWF to attach to the 5G Core Network over untrusted non-3GPP access. The UE shall be authenticated by and attached to the 5G Core Network during the IPSec tunnel establishment procedure. Further details for UE attachment to 5G Core Network over untrusted non-3GPP access are described in clause 4.12.2 in TS 23.502 [3].

It shall be possible to maintain the UE signalling connection with the AMF over the non-3GPP access after all the PDU Sessions for the UE over that access have been released or handed over to 3GPP access.

N1 NAS signalling over standalone non-3GPP accesses shall be protected with the same security mechanism applied for N1 over a 3GPP access.

User plane QoS differentiation between UE and N3IWF is supported as described in clause 5.7 and TS 23.502 [3] clause 4.12.5.

4.2.8.2 Architecture Reference Model for Non-3GPP Accesses

4.2.8.2.1 Non-roaming Architecture for Non-3GPP Accesses

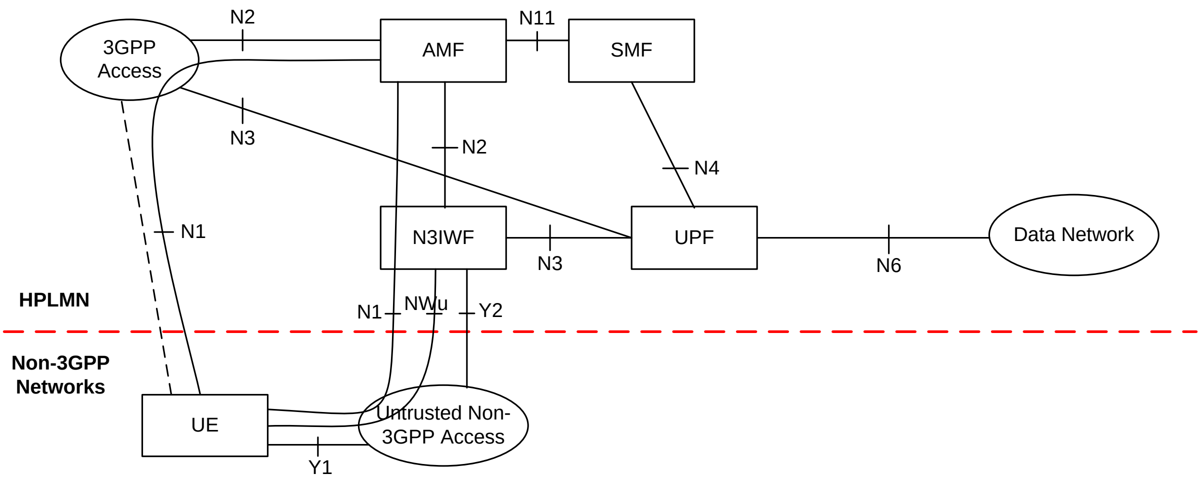


Figure 4.2.8.2.1-1: Non-roaming architecture for 5G Core Network with non-3GPP access

NOTE 1: The reference architecture in figure 4.2.8.2.1-1 only shows the architecture and the network functions directly connected to non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in figure 4.2.8.2.1-1 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.8.2.1-1 apply to a single AMF for a UE which is simultaneously connected to the same 5G Core Network over 3GPP access and non-3GPP access.

NOTE 4 The two N3 instances in Figure 4.2.8.2.1-1 may apply to different UPFs when different PDU Sessions are established over 3GPP access and non-3GPP access.

4.2.8.2.2 LBO Roaming Architecture for Non-3GPP Accesses, N3IWF in same PLMN as 3GPP access

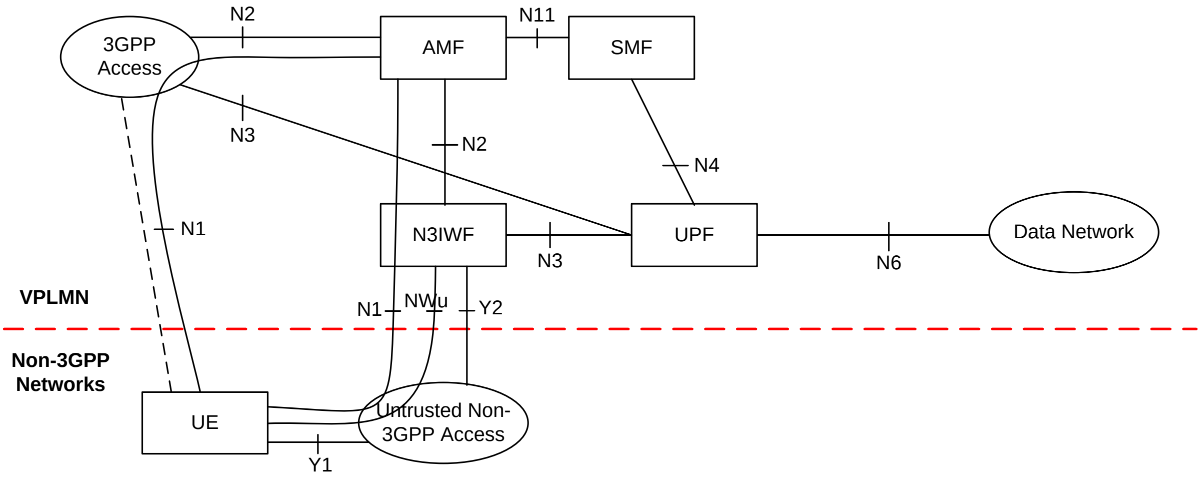


Figure 4.2.8.2.2-1: LBO Roaming architecture for 5G Core Network with non-3GPP access - N3IWF in the VPLMN

NOTE 1: The reference architecture in figure 4.2.8.2.2-1 only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in figure 4.2.8.2.2-1 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.8.2.2-1 apply to a single AMF for a UE which is connected to the 5G Core Network over 3GPP access and non-3GPP access simultaneously.

NOTE 4: The two N3 instances in Figure 4.2.8.2.2-1 may apply to different UPFs when different PDU Sessions are established over 3GPP access and non-3GPP access.

4.2.8.2.3 Home-routed Roaming Architecture for Non-3GPP Accesses, N3IWF in same PLMN as 3GPP access

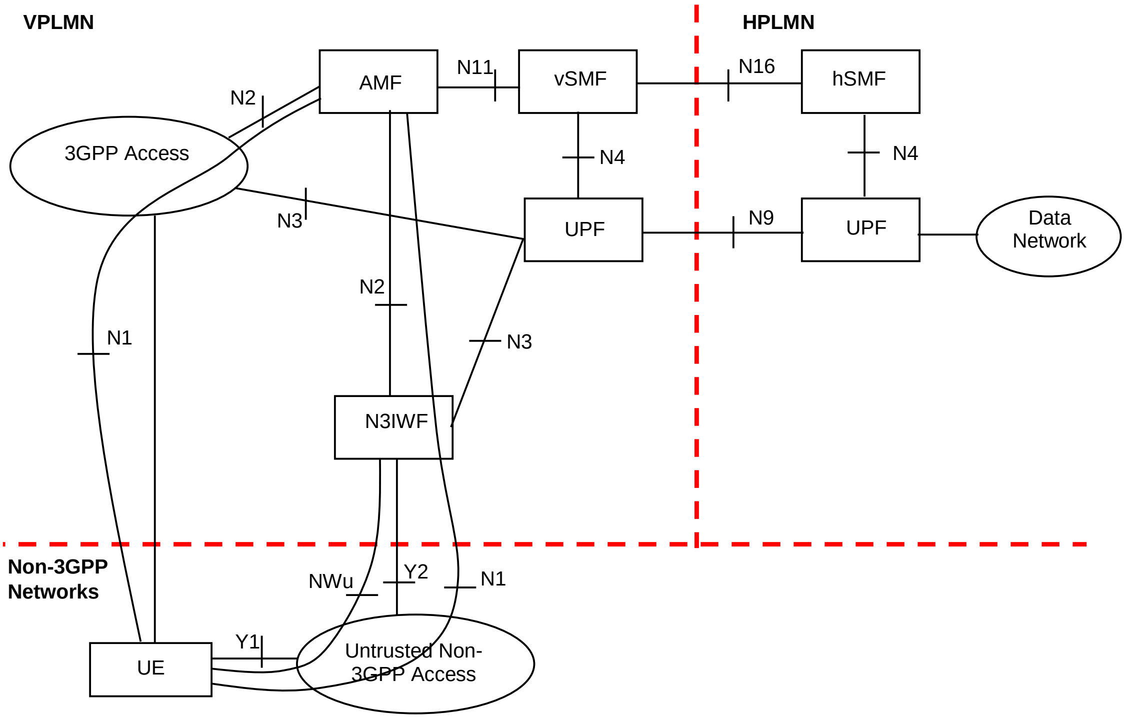


Figure 4.2.8.2.3-1: Home-routed Roaming architecture for 5G Core Network with non-3GPP access - N3IWF in the same VPLMN as 3GPP access

NOTE 1: The reference architecture in figure 4.2.8.2.3-1 only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The two N2 instances in Figure 4.2.8.2.3-1 apply to a single AMF for a UE which is connected to the 5G Core Network over 3GPP access and non-3GPP access simultaneously.

4.2.8.2.4 LBO Roaming Architecture for Non-3GPP Accesses, N3IWF in different PLMN from 3GPP access

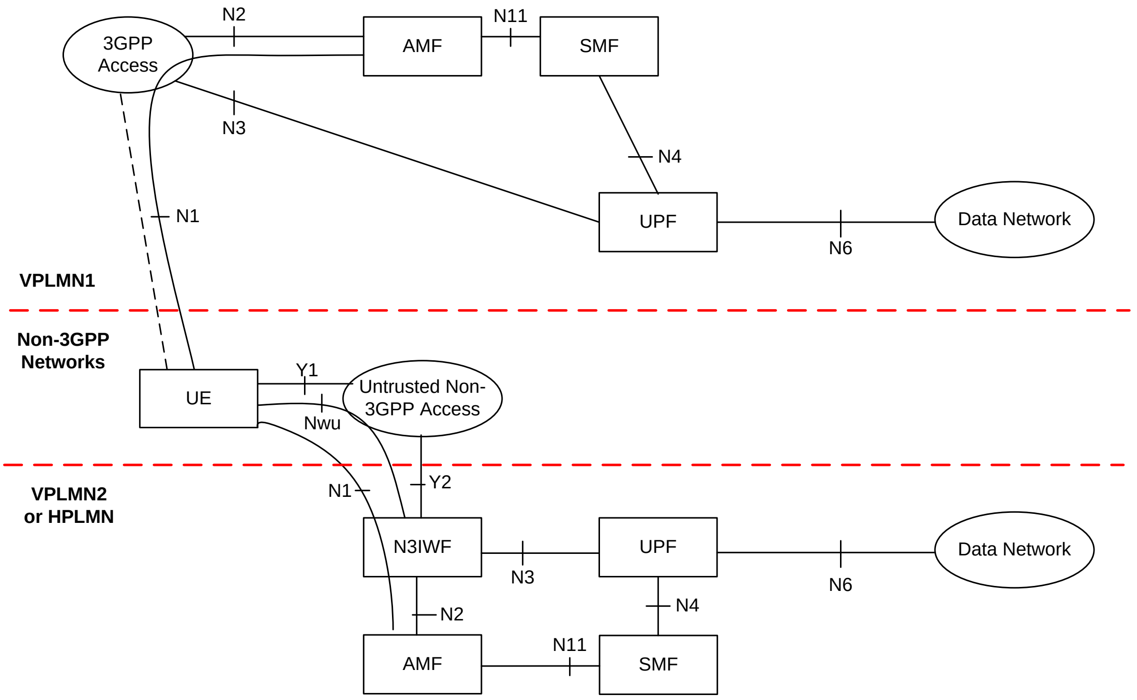


Figure 4.2.8.2.4-1: LBO Roaming architecture for 5G Core Network with non-3GPP access - N3IWF in the different PLMN from the 3GPP access

NOTE 1: The reference architecture in figure 4.2.8.2.4-1 only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in figure 4.2.8.2.4-1 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.8.2.4-1 apply to two different AMFs for a UE which is connected to the 5G Core Network over 3GPP access and non-3GPP access simultaneously.

4.2.8.2.5 Home-routed Roaming Architecture for Non-3GPP Accesses, N3IWF in different PLMN from 3GPP access

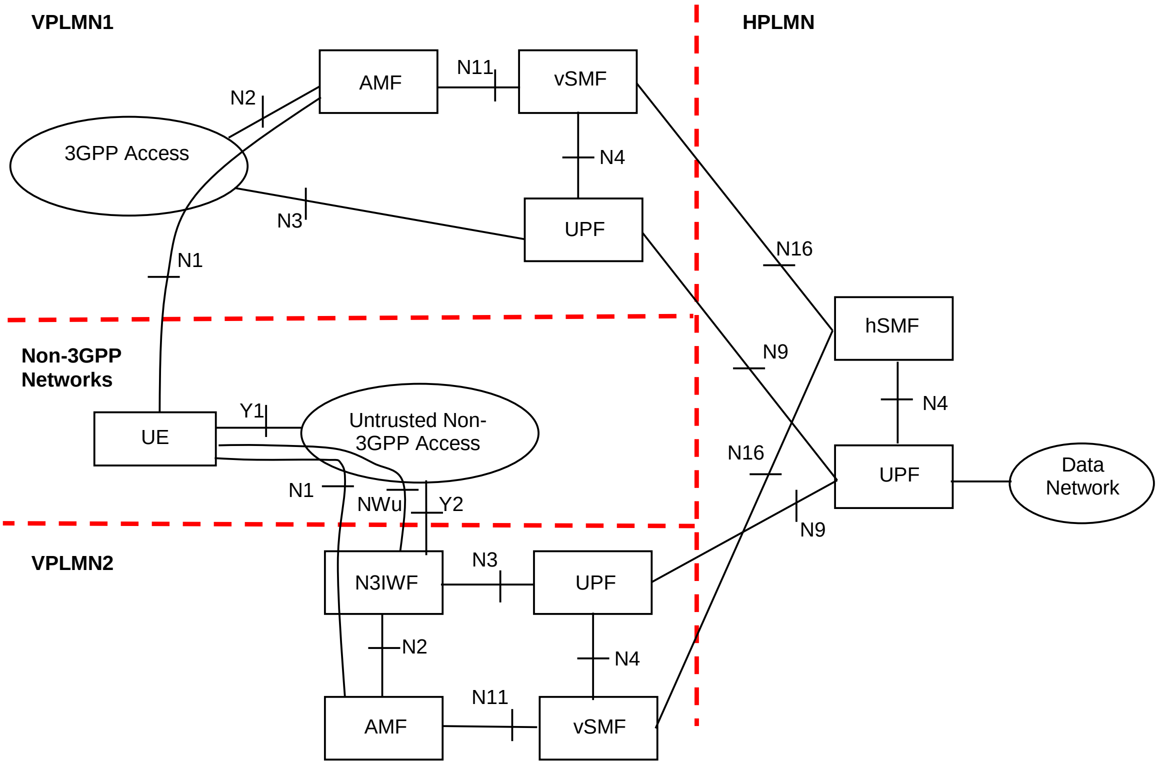


Figure 4.2.8.2.5-1: Home-routed Roaming architecture for 5G Core Network with non-3GPP access - N3IWF in the different VPLMN from the 3GPP access

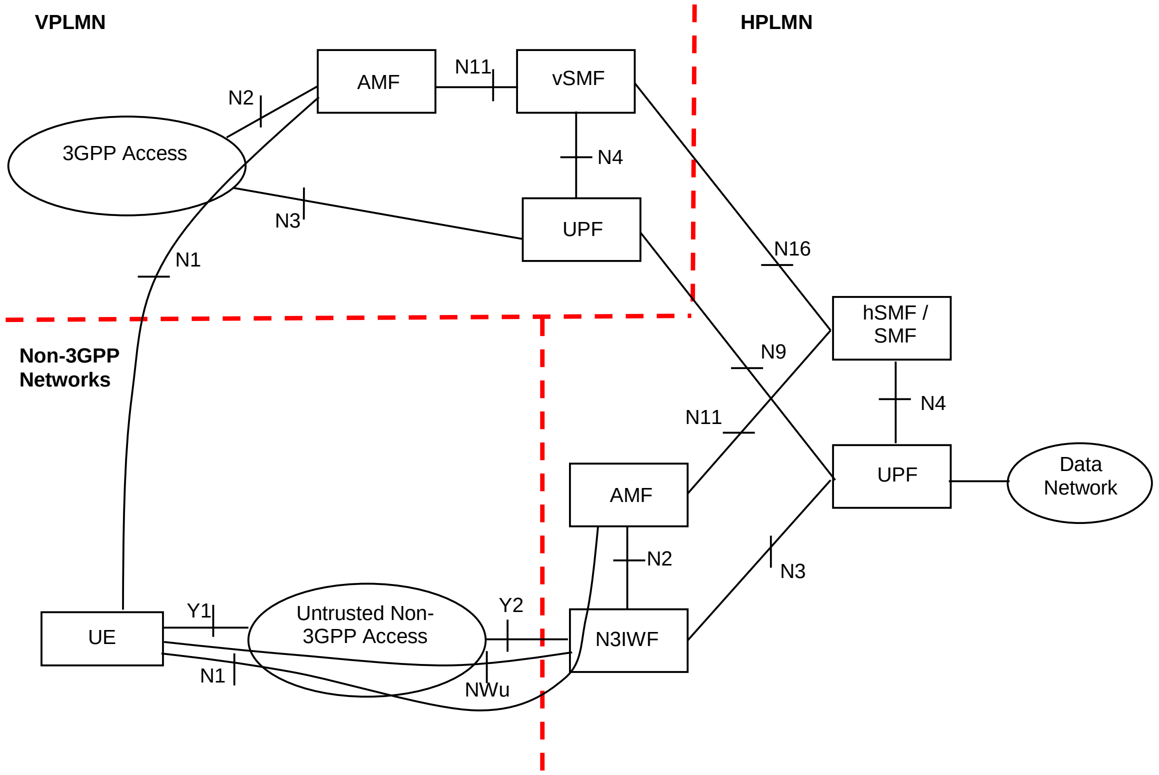


Figure 4.2.8.2.5-2: Home-routed Roaming architecture for 5G Core Network with non-3GPP access - N3IWF in HPLMN and different PLMN in 3GPP access

NOTE 1: The reference architecture in figure 4.2.8.2.5-1 and figure 4.2.8.2.5-2 only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The two N2 instances in figure 4.2.8.2.5-1 and figure 4.2.8.2.5-2 apply to two different AMFs for a UE which is connected to the 5G Core Network over 3GPP access and non-3GPP access simultaneously.

4.2.8.3 Non-3GPP Access Reference Points

The description of the reference points specific for the non-3GPP access:

N2, N3, N4, N6: these are defined in clause 4.2.

Y1 Reference point between the UE and the non-3GPP access (e.g. WLAN). This depends on the non-3GPP access technology and is outside the scope of 3GPP.

Y2 Reference point between the untrusted non-3GPP access and the N3IWF for the transport of NWu traffic.

NWu Reference point between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF so that control-plane and user-plane exchanged between the UE and the 5G Core Network is transferred securely over untrusted non-3GPP access.

4.3 Interworking with EPC

4.3.1 Non-roaming architecture

Figure 4.3.1-1 represents the non-roaming architecture for interworking between 5GS and EPC/E-UTRAN.

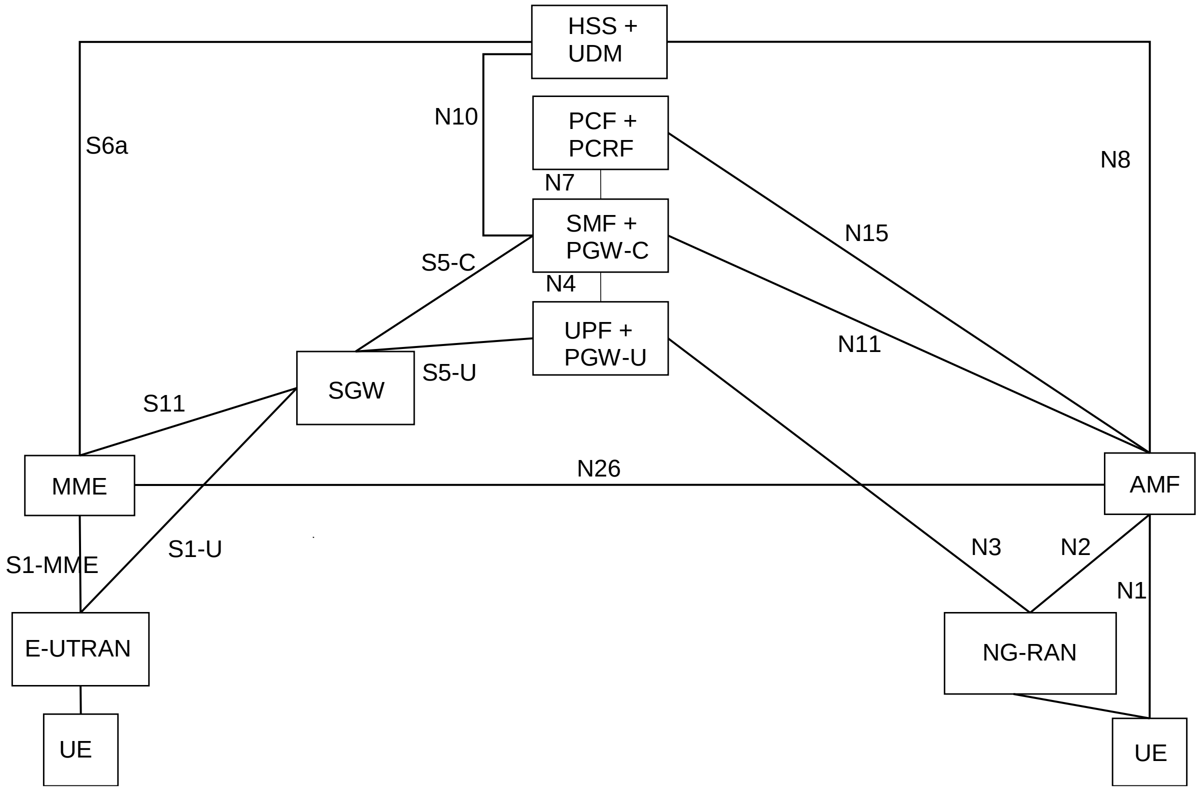


Figure 4.3.1-1: Non-roaming architecture for interworking between 5GS and EPC/E-UTRAN

NOTE 1: N26 interface is an inter-CN interface between the MME and 5GS AMF in order to enable interworking between EPC and the NG core. Support of N26 interface in the network is optional for interworking. N26 supports subset of the functionalities (essential for interworking) that are supported over S10.

NOTE 2: PCF + PCRF, PGW-C + SMF and UPF + PGW-U are dedicated for interworking between 5GS and EPC, which are optional and are based on UE and network capabilities. UEs that are not subject to 5GS and EPC interworking may be served by entities not dedicated for interworking, i.e. either by PGW/PCRF or SMF/UPF/PCF.

NOTE 3: There can be another UPF (not shown in the figure above) between the NG-RAN and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards an additional UPF, if needed.

NOTE 4: Figures and procedures in this specification that depict an SGW make no assumption whether the SGW is deployed as a monolithic SGW or as an SGW split into its control-plane and user-plane functionality as described in TS 23.214 [32].

4.3.2 Roaming architecture

Figure 4.3.2-1 represents the Roaming architecture with local breakout and Figure 4.3.2-2 represents the Roaming architecture with home-routed traffic for interworking between 5GS and EPC/E-UTRAN.

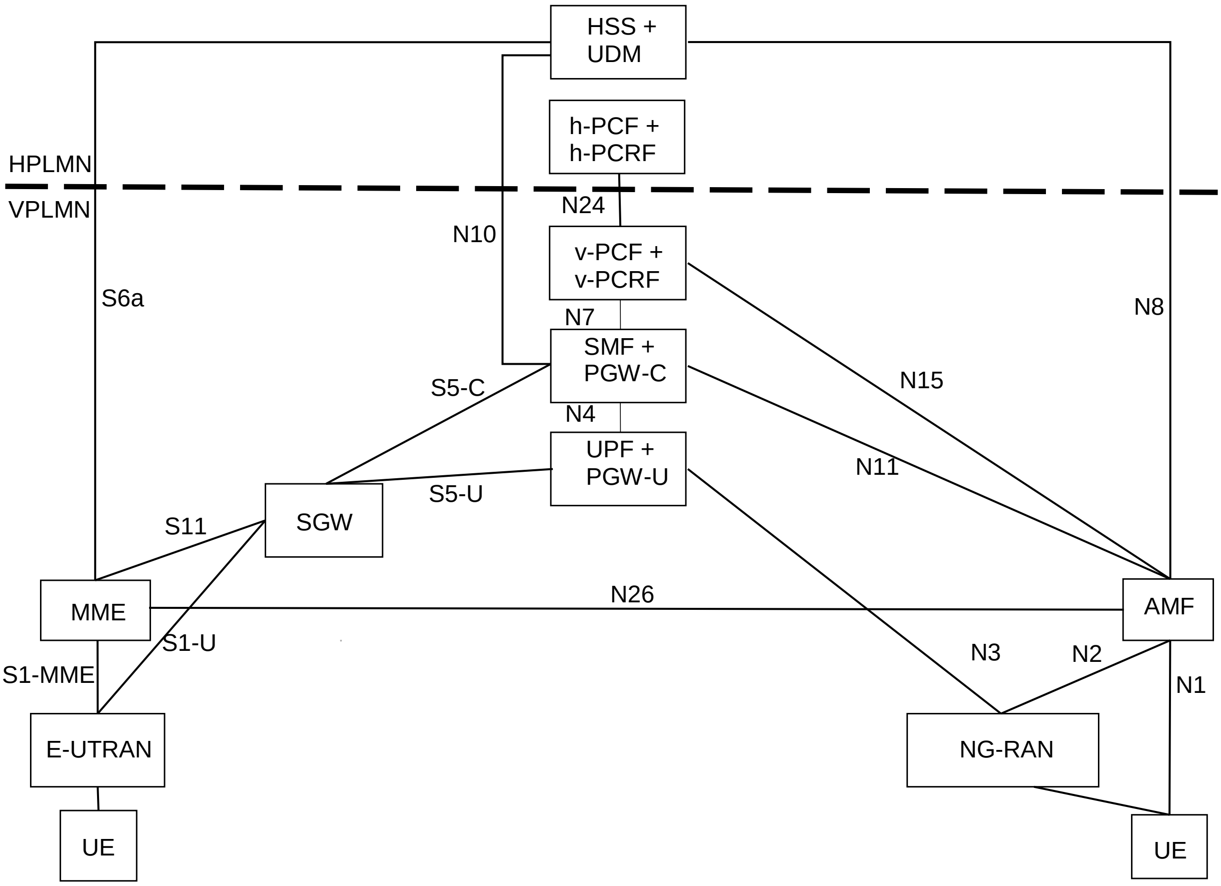


Figure 4.3.2-1: Local breakout roaming architecture for interworking between 5GS and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the NG-RAN and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards the additional UPF, if needed.

NOTE 2: S9 interface from EPC is not required since no known deployment exists.

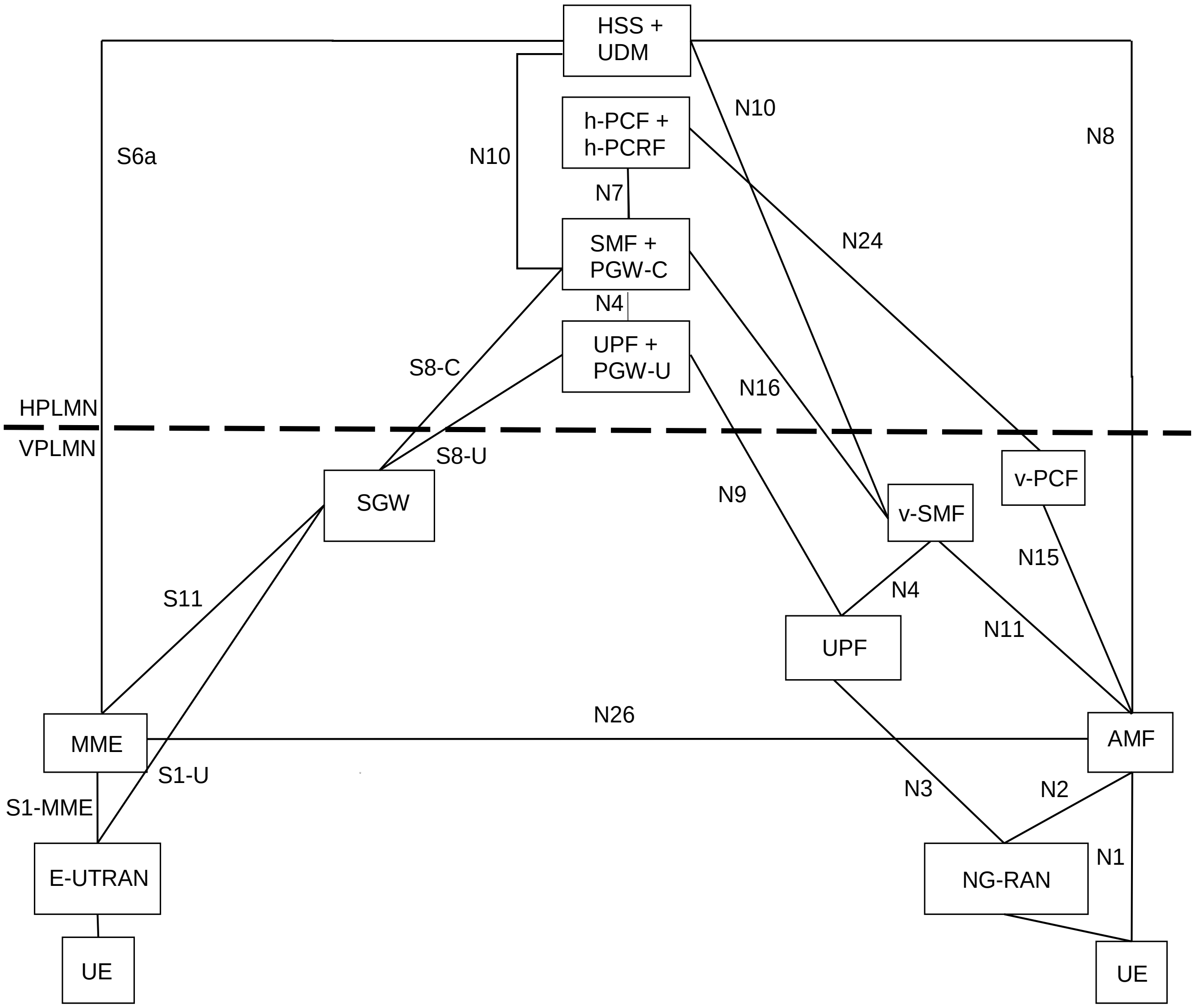


Figure 4.3.2-2: Home-routed roaming architecture for interworking between 5GS and EPC/E-UTRAN

4.3.3 Interworking between 5GC via non-3GPP access and E-UTRAN connected to EPC

4.3.3.1 Non-roaming architecture

Figure 4.3.3-1 represents the non-roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

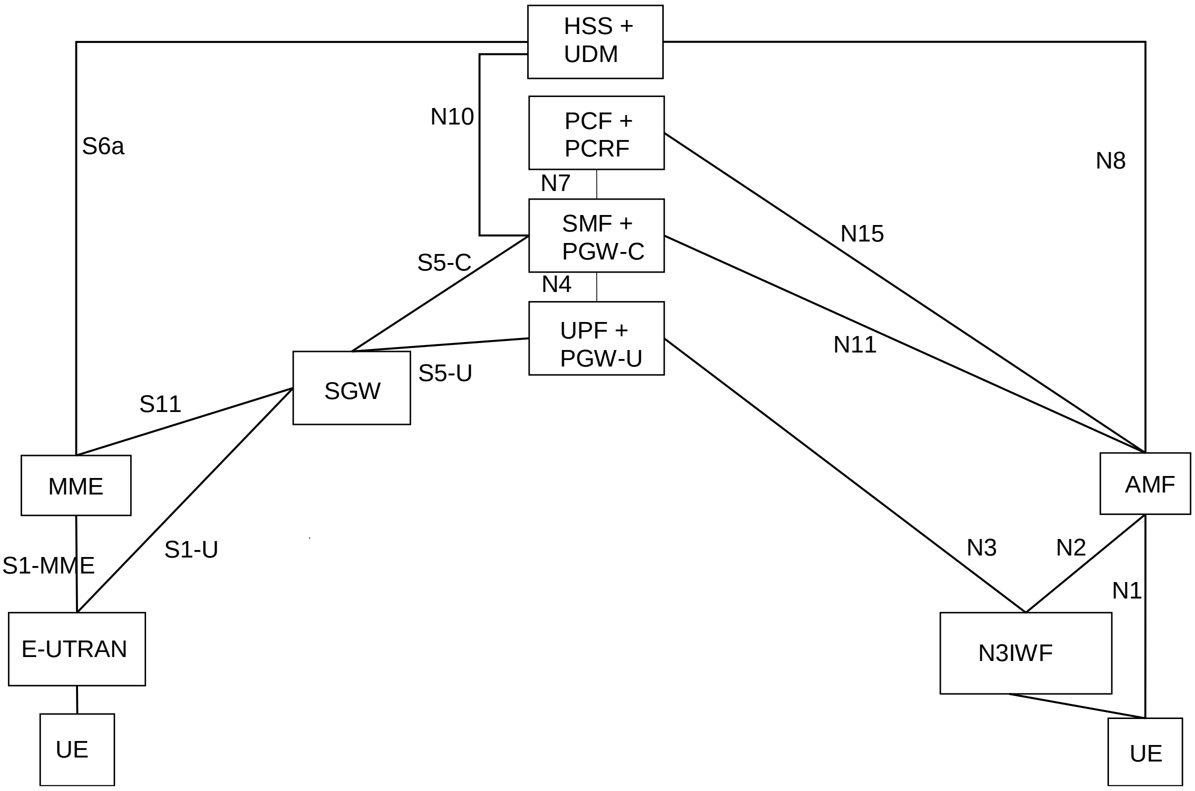


Figure 4.3.3-1: Non-roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the N3IWF and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards an additional UPF, if needed.

NOTE 2: N26 interface is not precluded, but it is not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

4.3.3.2 Roaming architecture

Figure 4.3.3.2-1 represents the Roaming architecture with local breakout and Figure 4.3.3.2-2 represents the Roaming architecture with home-routed traffic for interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

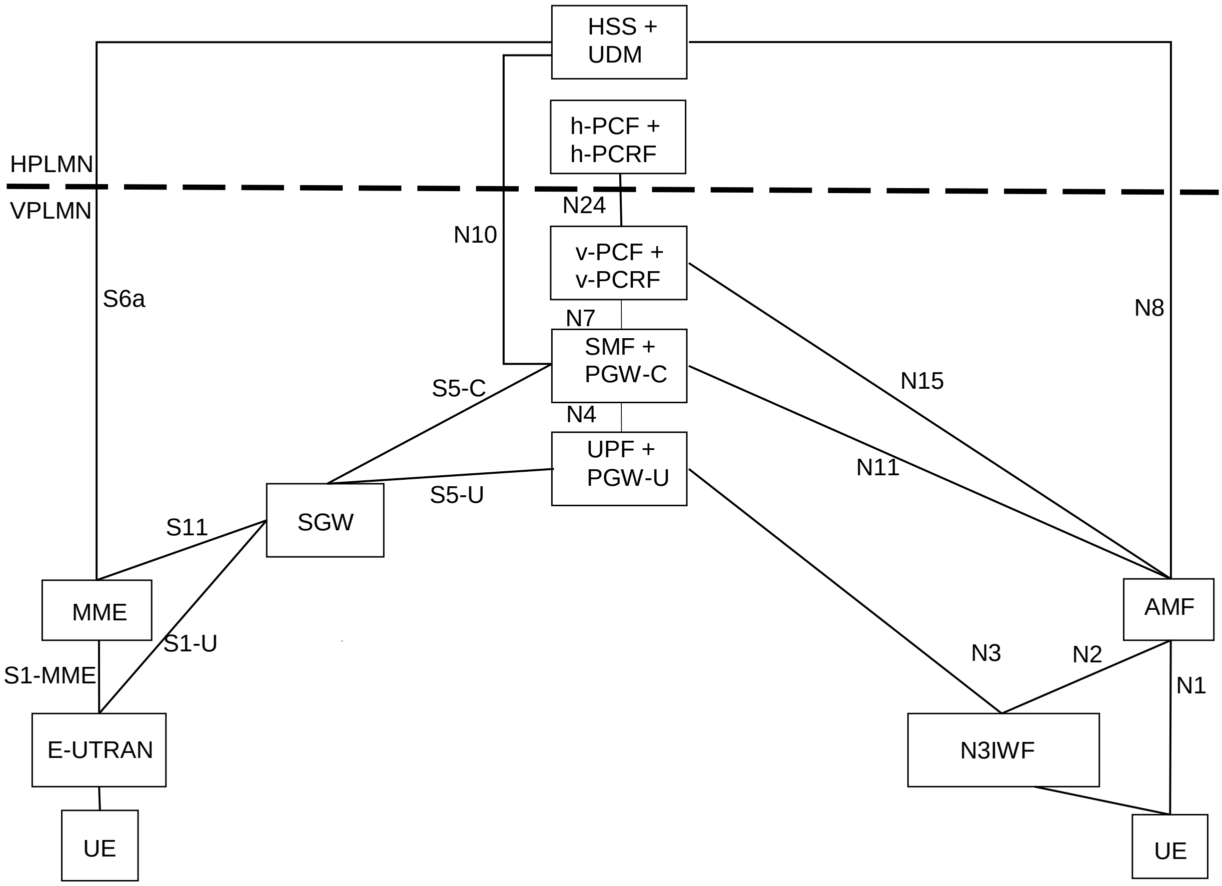


Figure 4.3.3-1: Local breakout roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the N3IWF and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards the additional UPF, if needed.

NOTE 2: S9 interface from EPC is not required since no known deployment exists.

NOTE 3: N26 interface is not precluded, but it not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

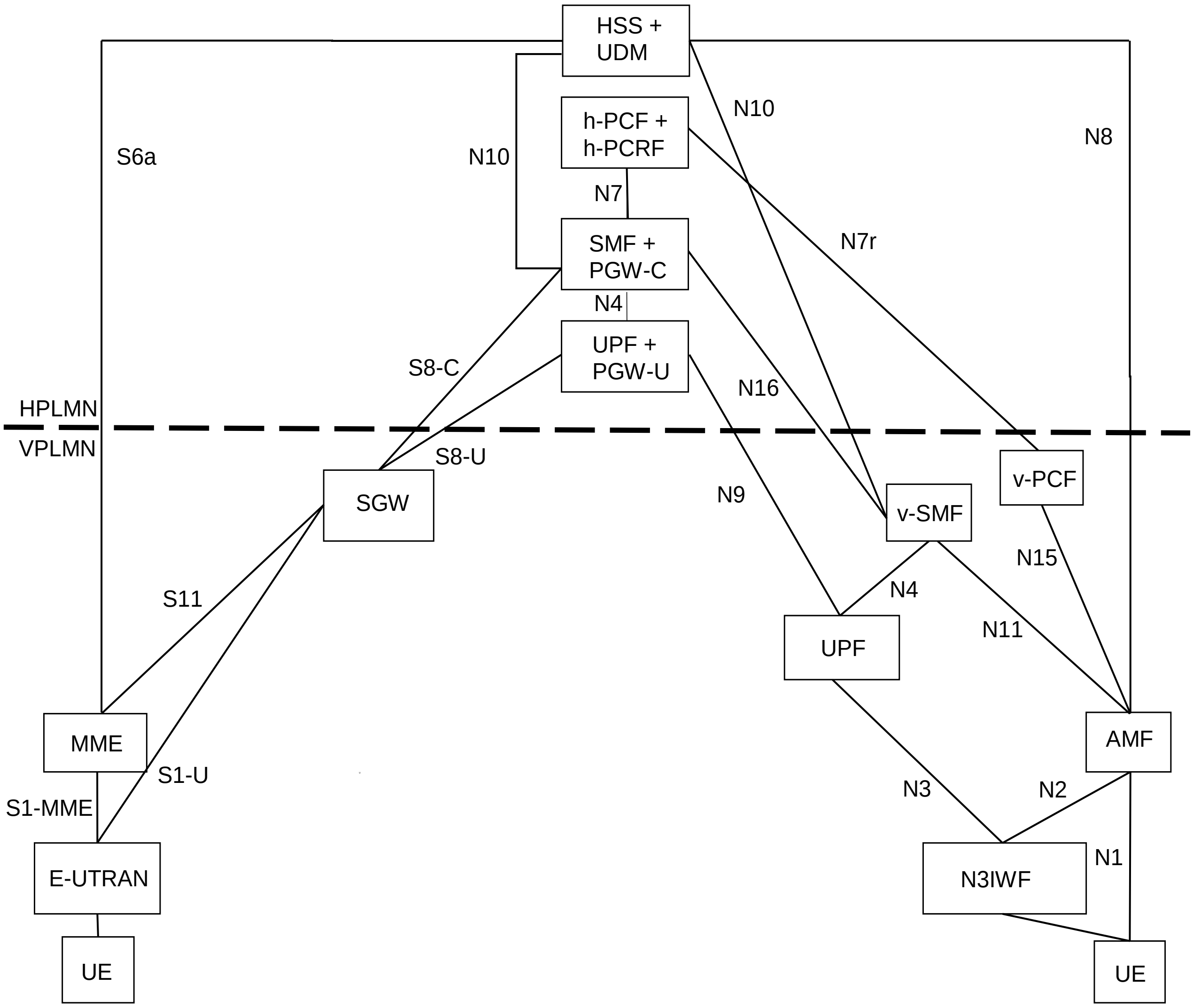


Figure 4.3.3.2-2: Home-routed roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 4: N26 interface is not precluded, but it not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

4.3.4 Interworking between ePDG connected to EPC and 5GS

4.3.4.1 Non-roaming architecture

Figure 4.3.4.1-1 represents the non-roaming architecture for interworking between ePDG/EPC and 5GS.

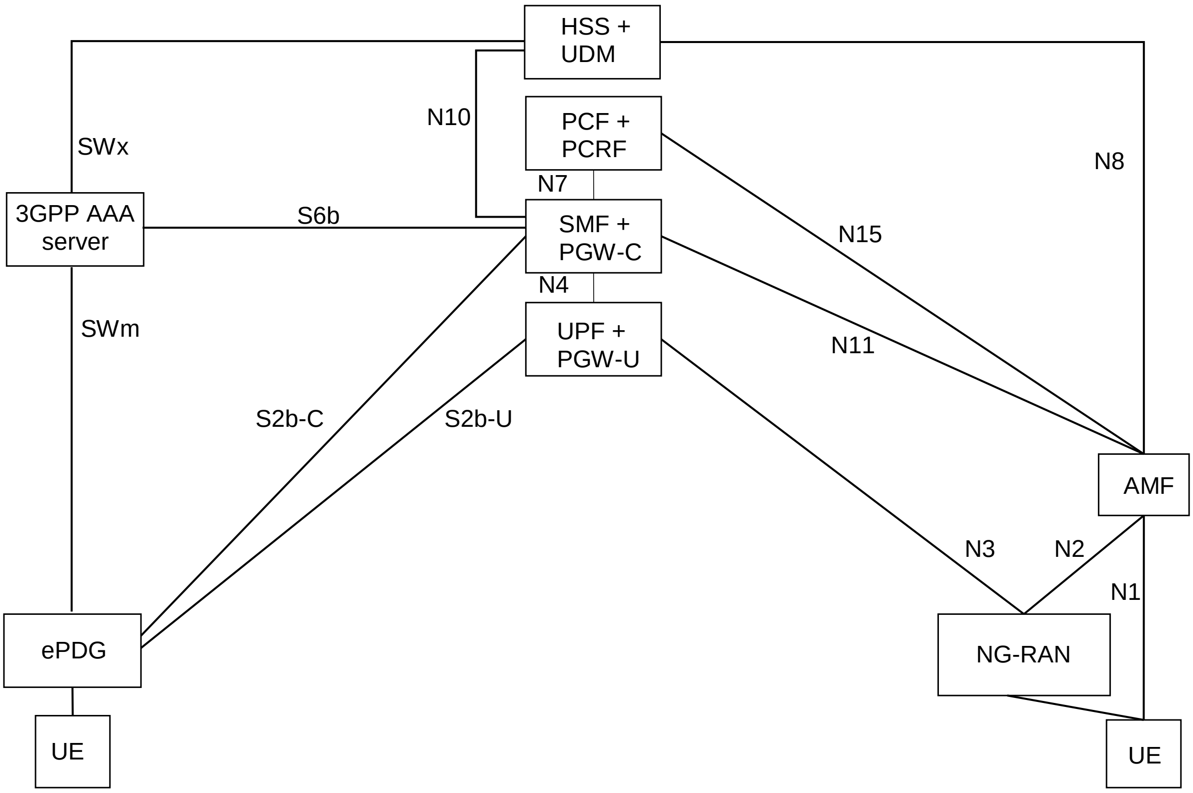


Figure 4.3.4.1-1: Non-roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 1: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWx, S2b and S6b), are documented in TS 23.402 [43].

4.3.4.2 Roaming architectures

Figure 4.3.4.2-1 represents the Roaming architecture with local breakout and Figure 4.3.4.2-2 represents the Roaming architecture with home-routed traffic for interworking between ePDG/EPC and 5GS.

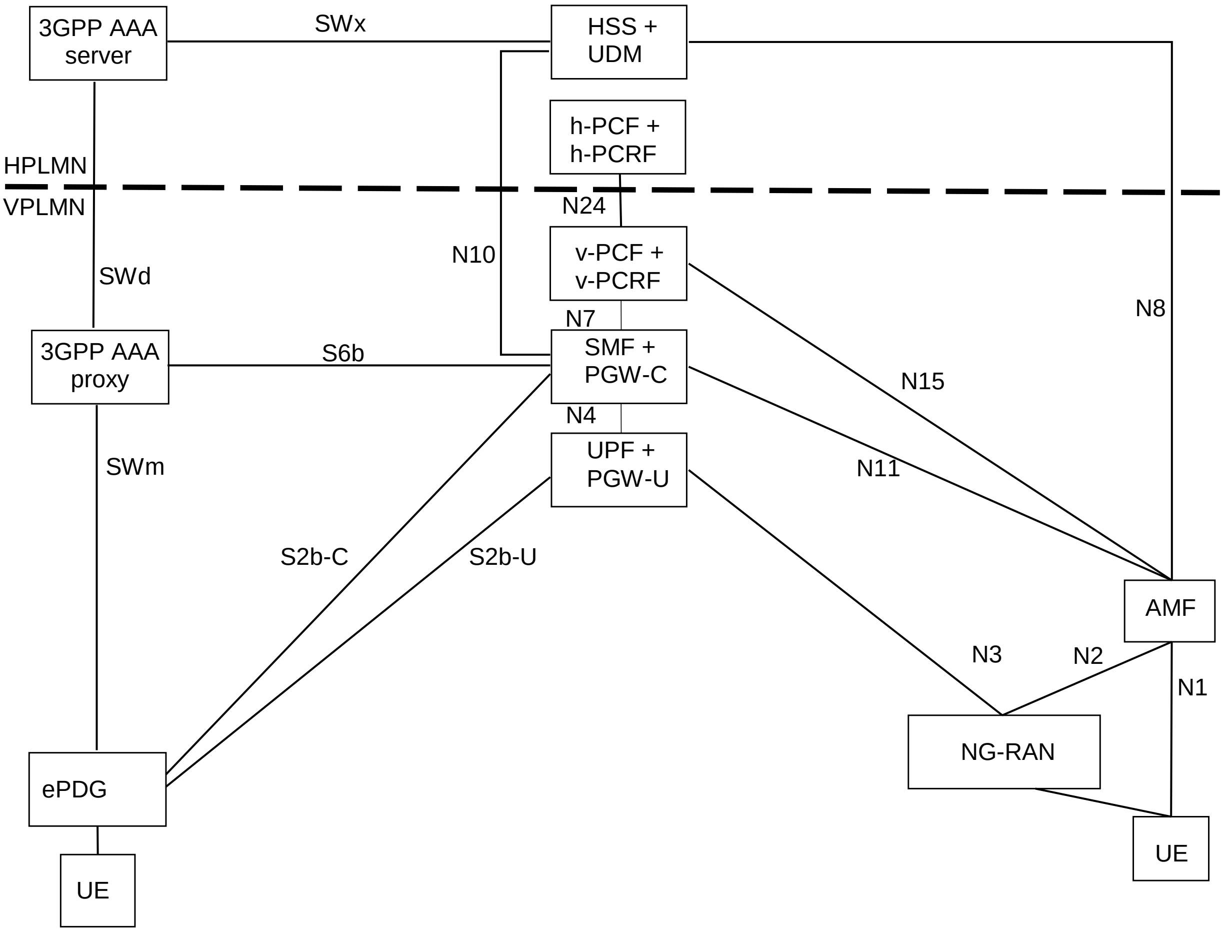


Figure 4.3.4.2-1: Local breakout roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 1: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWd, SWx, S2b and S6b), are documented in TS 23.402 [43].

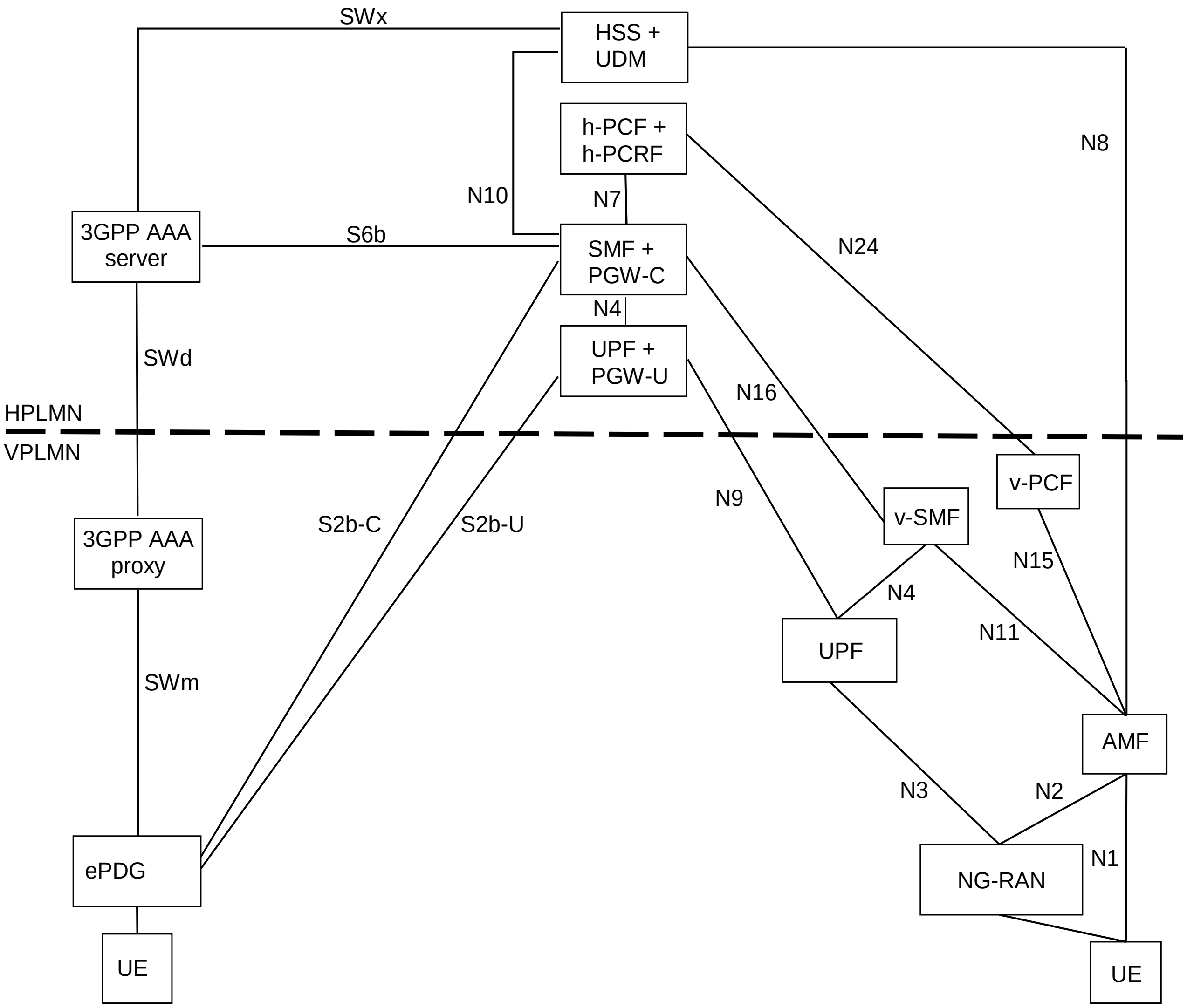


Figure 4.3.4.2-2: Home-routed roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 2: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWd, SWx, S2b and S6b), are documented in TS 23.402 [43].

4.4 Specific services

4.4.1 Public Warning System

The Public Warning System architecture for 5G System is specified in TS 23.041 [46].

4.4.2 SMS over NAS

4.4.2.1 Architecture to support SMS over NAS

Figure 4.4.2.1-1 shows the non-roaming architecture to support SMS over NAS using the Service-based interfaces within the Control Plane.

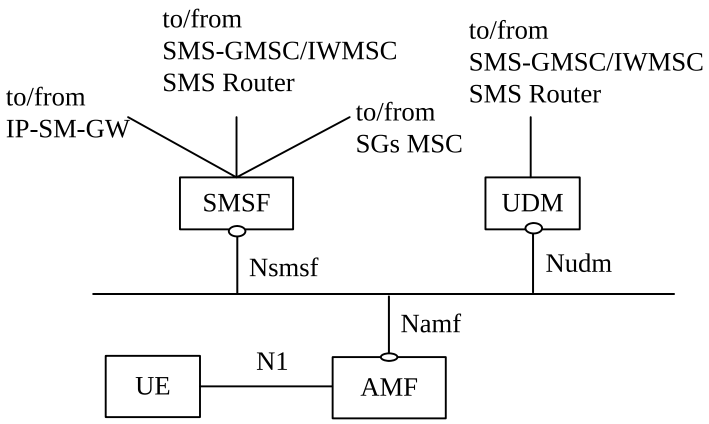


Figure 4.4.2.1-1: Non-roaming System Architecture for SMS over NAS

Figure 4.4.2.1-2 shows the non-roaming architecture to support SMS over NAS using the reference point representation.

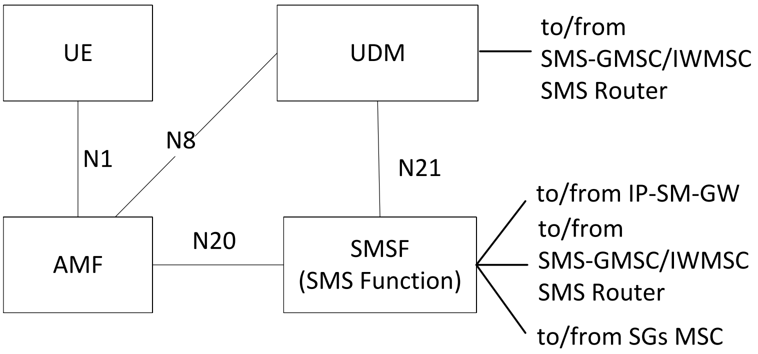


Figure 4.4.2.1-2: Non-roaming System Architecture for SMS over NAS in reference point representation

NOTE 1: SMS Function (SMSF) may be connected to the SMS-GMSC/IWMSC/SMS Router via one of the standardized interfaces as shown in TS 23.040 [5].

NOTE 2: UDM may be connected to the SMS-GMSC/IWMSC/SMS Router via one of the standardized interfaces as shown in TS 23.040 [5].

NOTE 3: Each UE is associated with only one SMS Function.

NOTE 4: SMSF re-allocation during UE is in RM-REGISTERED state is not supported in this release. When serving AMF is re-allocated for a given UE, the source AMF includes SMSF identifier as part of UE context transfer to target AMF.

NOTE 5: To support MT SMS domain selection, SMSF may connect to IP-SM-GW and SGs MSC via one of the standardized interfaces as shown in TS 23.040 [5].

Figure 4.4.2.1-3 shows the roaming architecture to support SMS over NAS using the Service-based interfaces within the Control Plane.

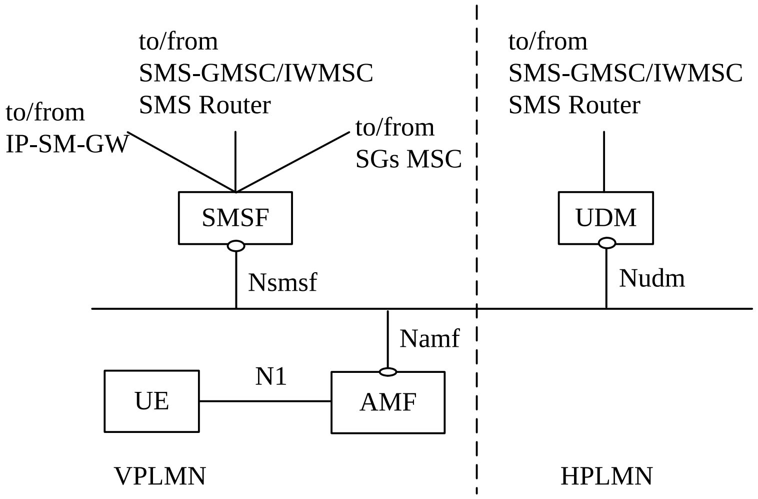


Figure 4.4.2.1-3: Roaming architecture for SMS over NAS

Figure 4.4.2.1-4 shows the roaming architecture to support SMS over NAS using the reference point representation.

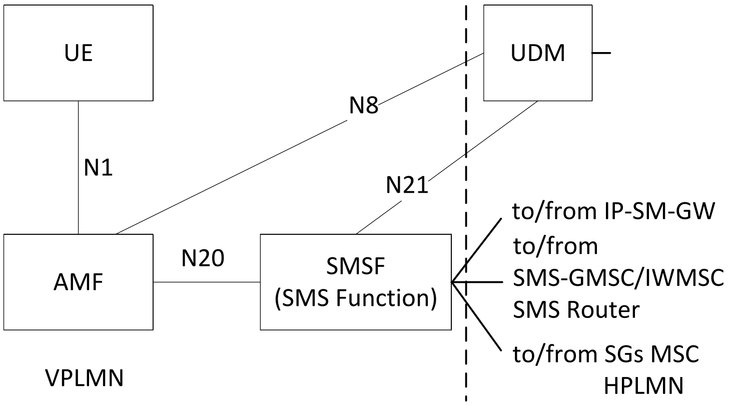


Figure 4.4.2.1-4: Roaming architecture for SMS over NAS in reference point representation

4.4.2.2 Reference point to support SMS over NAS

N1: Reference point for SMS transfer between UE and AMF via NAS.

Following reference points are realized by service based interfaces:

N8: Reference point for SMS function address retrieval and SMS over NAS service authorization between AMF and UDM.

N20: Reference point for SMS transfer between AMF and SMS Function.

N21: Reference point for SMS subscription retrieval between SMS Function and UDM.

4.4.2.3 Service based interface to support SMS over NAS

Nsmsf: Service-based interface exhibited by SMSF.

4.4.3 IMS support

IMS support for 5GC is defined in TS 23.228 [15].

The 5G System architecture supports Rx interface between PCF and P-CSCF to enable IMS service. See TS 23.228 [15] and TS 23.203 [4].

4.4.4 Location services

4.4.4.1 Architecture to support Location Services

Location Service feature is optional and restricted to regulatory services in this release of the specification. Figure 4.4.4.1-1 shows architectural support for location services for non-roaming scenarios using service-based interface representation, where applicable. Only entities directly relevant to location services are shown.

NOTE 1: The reference point Le is shown for completeness only.

NOTE 2: If an inter-GMLC scenario is required the reference points Lr defined in TS 23.271 [55] can be used.

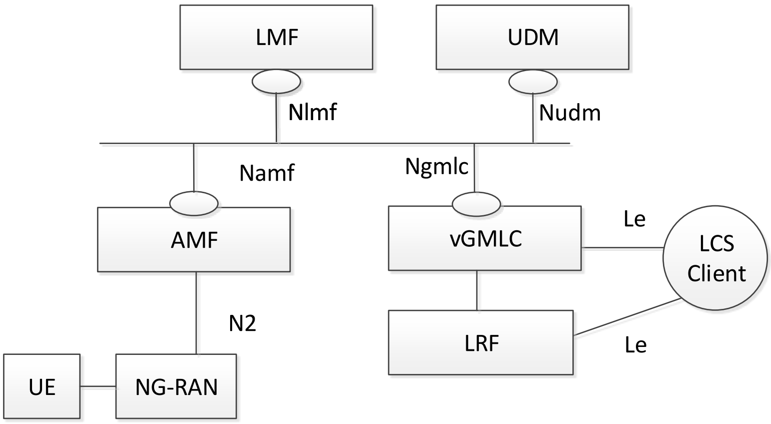


Figure 4.4.4.1-1: Non-roaming reference architecture for Location Services

Figure 4.4.4.1-2 shows architectural support for location services for non-roaming scenarios, using the reference point representation showing how various network functions interact with each other.

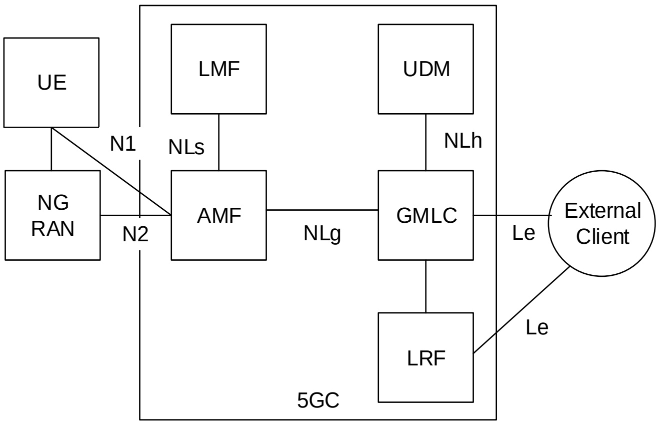


Figure 4.4.4.1-2: Non-roaming reference architecture for Location Services in reference point representation

4.4.4.2 Reference point to support Location Services

N1: Reference point between UE and AMF via NAS.

N2: Reference point between NG-RAN and AMF.

Le: Reference point between a GMLC and a LCS Client.

Following reference points are realized by service based interfaces:

NLg: Reference point between a GMLC and an AMF.

NLs: Reference point between an AMF and LMF.

NLh: Reference point between an GMLC and UDM.

4.4.4.3 Service Based Interfaces to support Location Services

Ngmlc: Service-based interface exhibited by GMLC.

Nlmf: Service-based interface exhibited by LMF.

Namf: Service-based interface exhibited by AMF.

Nudm: Service-based interface exhibited by UDM.

4.4.5 Application Triggering Services

See TS 23.502 [3] clause 5.2.6.1.

Application trigger message contains information that allows the network to route the message to the appropriate UE and the UE to route the message to the appropriate application. The information destined to the application, excluding the information to route it, is referred to as the Trigger payload. The Trigger payload is implementation specific.

NOTE: The application in the UE may perform actions indicated by the Trigger payload when the Triggered payload is received at the UE. For example initiation of immediate or later communication with the application server based on the information contained in the Trigger payload, which includes the PDU Session Establishment procedure if the related PDU Session is not already established.

5 High level features

5.1 General

Clause 5 specifies the high level functionality and features of the 5G System for both 3GPP and Non-3GPP access and for the interoperability with the EPC defined in TS 23.401 [26].

5.2 Network Access Control

5.2.1 General

Network access is the means for the user to connect to 5G CN. Network access control comprises the following functionality:

- Network selection,
- Identification and authentication,
- Authorisation,
- Access control and barring,
- Policy control,
- Lawful Interception.

5.2.2 Network selection

In order to determine to which PLMN to attempt registration, the UE performs network selection. The network selection procedure comprises two main parts, PLMN selection and access network selection. The requirements for the PLMN selection are specified in TS 22.011 [25] and the procedures are in TS 23.122 [17]. The access network selection part for the 3GPP access networks is specified in TS 36.300 [30] for E-UTRAN and in TS 38.300 [27] for the NR.

5.2.3 Identification and authentication

The network may authenticate the UE during any procedure establishing a signalling connection with the UE. The security architecture is specified in TS 33.501 [29]. The network may optionally perform an PEI check with 5G-EIR.

5.2.4 Authorisation

The authorisation for connectivity of the subscriber to the 5GC and the authorization for the services that the user is allowed to access based on subscription (e.g. Operator Determined Barrings, Roaming restrictions, Access Type and RAT Type currently in use) is evaluated once the user is successfully identified and authenticated. This authorization is executed during UE registration procedure.

5.2.5 Access control and barring

When the UE needs to transmit an initial NAS message, the UE shall request to establish an RRC connection first and the NAS shall provide the RRC establishment related information to the lower layer. The RAN handles the RRC connection with priority during and after RRC connection establishment procedure, when UE indicates priority in Establishment related information

Under high network load conditions, the network may protect itself against overload by limiting access attempts from UEs. Depending on network configuration, the network may determine whether certain access attempt should be allowed or blocked based on categorized criteria, as specified in TS 22.261 [2] and TS 24.501 [47].

5.2.6 Policy control

Network access control including service authorization may be influenced by Policy control, as specified in clause 5.14.

5.2.7 Lawful Interception

For definition and functionality of Lawful Interception, please see TS 33.106 [35].

5.3 Registration and Connection Management

5.3.1 General

The Registration Management is used to register or deregister a UE/user with the network, and establish the user context in the network. The Connection Management is used to establish and release the signalling connection between the UE and the AMF.

5.3.2 Registration Management

5.3.2.1 General

A UE/user needs to register with the network to receive services that requires registration. Once registered and if applicable the UE updates its registration with the network (see TS 23.502 [3]):

- periodically, in order to remain reachable (periodic registration update); or
- upon mobility (mobility registration update); or
- to update its capabilities or re-negotiate protocol parameters.

The initial Registration procedure involves execution of Network Access Control functions as defined in clause 5.2 (i.e. user authentication and access authorization based on subscription profiles in UDM). As result of the Registration procedure, the identifier of the serving AMF serving the UE in the access through which the UE has registered will be registered in UDM.

The registration management procedures are applicable over both 3GPP access and Non-3GPP access. The 3GPP and Non-3GPP RM states are independent of each other, see clause 5.3.2.4.

5.3.2.2 5GS Registration Management states

5.3.2.2.1 General

Two RM states are used in the UE and the AMF that reflect the registration status of the UE in the selected PLMN:

- RM-DEREGISTERED.
- RM-REGISTERED.

5.3.2.2.2 RM-DEREGISTERED state

In the RM-DEREGISTERED state, the UE is not registered with the network. The UE context in AMF holds no valid location or routing information for the UE so the UE is not reachable by the AMF. However, some parts of UE context may still be stored in the UE and the AMF e.g. to avoid running an authentication procedure during every Registration procedure.

In the RM-DEREGISTERED state, the UE shall:

- attempt to register with the selected PLMN using the initial registration procedure if it needs to receive service that requires registration (see TS 23.502 [3] clause 4.2.2.2).
- remain in RM-DEREGISTERED state if receiving a Registration Reject upon initial registration (see TS 23.502 [3] clause 4.2.2.2).
- enter RM-REGISTERED state upon receiving a Registration Accept (see TS 23.502 [3] clause 4.2.2.2).

When the UE RM state in the AMF is RM-DEREGISTERED, the AMF shall:

- when applicable, accept the initial registration of a UE by sending a Registration Accept to this UE and enter RM-REGISTERED state for the UE (see TS 23.502 [3] clause 4.2.2.2); or
- when applicable, reject the initial registration of a UE by sending a Registration Reject to this UE (see TS 23.502 [3] clause 4.2.2.2).

5.3.2.2.3 RM-REGISTERED state

In the RM-REGISTERED state, the UE is registered with the network. In the RM-REGISTERED state, the UE can receive services that require registration with the network.

In the RM-REGISTERED state, the UE shall:

- perform mobility Registration Update procedure if the current TAI of the serving cell (see TS 37.nnn [xx]) is not in the list of TAIs that the UE has received from the network in order to maintain the registration and enable the AMF to page the UE;
- perform periodic Registration Update procedure triggered by expiration of the periodic update timer to notify the network that the UE is still active.
- perform a Registration Update procedure to update its capability information or to re-negotiate protocol parameters with the network;
- perform Deregistration procedure (see TS 23.502 [3] clause 4.2.2.3.1), and enter RM-DEREGISTERED state, when the UE needs to be no longer registered with the PLMN. The UE may decide to deregister from the network at any time.

- enter RM-DEREGISTERED state when receiving a Registration Reject message or a Deregistration message. The actions of the UE depend upon the 'cause value' in the Registration Reject or Deregistration message. See TS 23.502 [3] clause 4.2.2.

When the UE RM state in the AMF is RM-REGISTERED, the AMF shall:

- perform Deregistration procedure (see TS 23.502 [3] clauses 4.2.2.3.2, 4.2.2.3.3), and enter RM-DEREGISTERED state for the UE, when the UE needs to be no longer registered with the PLMN. The network may decide to deregister the UE at any time;

- perform Implicit Deregistration at any time after the Implicit Deregistration timer expires. The AMF shall enter RM-DEREGISTERED state for the UE after Implicit Deregistration;

- when applicable, accept or reject Registration Requests or Service Requests from the UE.

5.3.2.2.4 5GS Registration Management State models

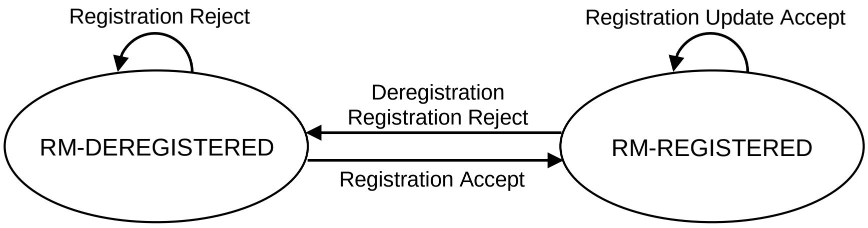


Figure 5.3.2.2.4-1: RM state model in UE

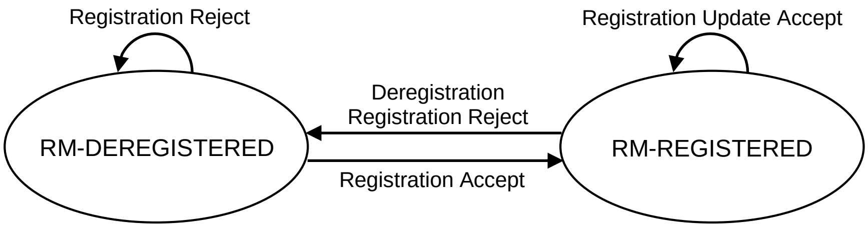


Figure 5.3.2.2.4-2: RM state model in AMF

5.3.2.3 Registration Area management

Registration Area management comprises the functions to allocate and reallocate a Registration area to a UE. Registration area is managed per access type i.e., 3GPP access or Non-3GPP access.

When a UE registers with the network over the 3GPP access, the AMF allocates a set of tracking areas in TAI List to the UE. When the AMF allocates registration area, i.e. the set of tracking areas in TAI List, to the UE it may take into account various information (e.g. Mobility Pattern and Allowed/Non-Allowed Area (refer to clause 5.3.4.1)). An AMF which has the whole PLMN as serving area may alternatively allocate the whole PLMN ("all PLMN") as registration area to a UE in MICO mode (refer to clause 5.4.1.3).

The 5G System shall support allocating a TAI List over different 5G-RATs in a single TAI List.

When a UE registers with the network over the Non-3GPP access, the registration area for Non-3GPP access corresponds to a unique reserved TAI value (i.e. dedicated to Non-3GPP access). There is thus a unique Tracking Area for the Non-3GPP access to 5GC, that is called the N3GPP TAI.

When generating the TAI list, the AMF shall include only TAIs that are applicable on the access where the TAI list is sent.

The additional aspects for registration management when a UE is registered over one access type while the UE is already registered over the other access type is further described in clause 5.3.2.4.

5.3.2.4 Support of a UE registered over both 3GPP and Non-3GPP access

For a given serving PLMN there is one RM context for a UE for each access, e.g. when the UE is consecutively or simultaneously served by a 3GPP access and by a non-3GPP access (via an N3IWF) of the same PLMN. UDM manages separate/independent UE Registration procedures for each access.

When served by the same PLMN for 3GPP and non-3GPP accesses, an UE is served by the same AMF except in the temporary situation described in clause 5.17 i.e. after a mobility from EPS while the UE has PDU Sessions associated with non-3GPP access.

An AMF associates multiple access-specific RM contexts for an UE with:

- a 5G-GUTI that is common to both 3GPP and Non-3GPP accesses. This 5G-GUTI is globally unique.
- a Registration state per access type (3GPP / Non-3GPP)
- a Registration Area per access type: one Registration Area for 3GPP access and another Registration Area for non 3GPP access. Registration Areas for the 3GPP access and the Non-3GPP access are independent.
- a Periodic Registration timer for 3GPP access.
- a Non-3GPP Implicit Deregistration timer.

The AMF shall not provide a Periodic Registration Timer for the UE over a Non-3GPP access. Consequently, the UE need not perform Periodic Registration Update procedure over Non-3GPP access. Instead, during the Initial Registration procedure and Re-registration, the UE is provided by the network with a UE Non-3GPP Deregistration timer that starts when the UE enters non-3GPP CM-IDLE state.

The 5G-GUTI may be assigned or re-assigned over any of the 3GPP and Non-3GPP accesses. The AMF assigns to the UE a single 5G-GUTI that is used over 3GPP and Non-3GPP access of the same PLMN or equivalent PLMN (which presumes that there is control and user plane connectivity between nodes of the registered PLMN and its equivalent PLMN). The 5G-GUTI is assigned upon a successful registration of the UE, and is valid over both 3GPP and Non-3GPP access to the same PLMN or equivalent PLMN for the UE. Upon performing any initial access over the Non-3GPP access or over the 3GPP access, the UE provides the 5G-GUTI it has received in an earlier successful registration over any access of the same PLMN or equivalent PLMN. This enables the AN to select an AMF that maintains the UE context created at the previous Registration procedure, and enables the AMF to correlate the UE request to the existing UE context.

If the UE is performing registration over one access and intends to perform registration over the other access in the same PLMN or equivalent PLMN (e.g. the 3GPP access and the selected N3IWF are located in the same PLMN), the UE shall not initiate the registration over the other access until the registration procedure over first access is completed.

NOTE: To which access the UE performs registration first is up to UE implementation.

When the UE is successfully registered to an access (3GPP access or Non-3GPP access respectively) and the UE registers via the other access:

- if the second access is located in the same PLMN or equivalent PLMN (e.g. the UE is registered via a 3GPP access and selects a N3IWF located in the same PLMN), the UE shall use for the registration to the PLMN associated with the new access the 5G-GUTI that the UE has been provided at the previous registration for the first access in the same PLMN or equivalent PLMN.
- if the second access is located in a PLMN different from the registered PLMN of the first access (i.e. not the registered PLMN or an equivalent PLMN of the registered PLMN), (e.g. the UE is registered to a 3GPP access and selects a N3IWF located in a PLMN different from the PLMN of the 3GPP access, or the UE is registered over Non-3GPP and registers to a 3GPP access in a PLMN different from the PLMN of the N3IWF), the UE shall use for the registration to the PLMN associated with the new access a 5G-GUTI only if it has got one previously received from the same PLMN. However, if the UE does not already have a 5G-GUTI from the PLMN to which it is attempting to register or from an equivalent PLMN, the SUCI shall be used for the new registration.

When a UE 5G-GUTI assigned during a Registration procedure over 3GPP (e.g. the UE registers first over a 3GPP access) is location-dependent, the same UE 5G-GUTI can be re-used over the Non-3GPP access when the selected N3IWF function is in the same PLMN as the 3GPP access. When an UE 5G-GUTI is assigned during a Registration procedure performed over a Non 3GPP access (e.g. the UE registers first over a non-3GPP access), the UE 5G-GUTI may not be location-dependent, so that the UE 5G-GUTI may not be valid for NAS procedures over the 3GPP access and, in this case, a new AMF is allocated during the Registration procedure over the 3GPP access.

When the UE is registered first via 3GPP access, if the UE registers to the same PLMN via Non-3GPP access, the UE shall send the GUAMI obtained via 3GPP access to the N3IWF, which uses the received GUAMI to select the same AMF as the 3GPP access.

The deregistration request indicates whether it applies to the 3GPP access the Non-3GPP access, or both.

If the UE is registered on both 3GPP and Non-3GPP accesses and it is in CM-IDLE over Non-3GPP access, then the UE or AMF may initiate a Deregistration procedure over the 3GPP access to deregister the UE only on the Non-3GPP access, in which case all the PDU Sessions which are associated with the Non-3GPP access shall be released.

If the UE is registered on both 3GPP and non-3GPP accesses and it is in CM-IDLE over 3GPP access and in CM-CONNECTED over non-3GPP access, then the UE may initiate a Deregistration procedure over the non-3GPP access to deregister the UE only on the 3GPP access, in which case all the PDU Sessions which are associated with the 3GPP access shall be released.

Registration Management over Non-3GPP access is further defined in clause 5.5.2.

5.3.3 Connection Management

5.3.3.1 General

Connection management comprises the functions of establishing and releasing a signalling connection between a UE and the AMF over N1. This signalling connection is used to enable NAS signalling exchange between the UE and the core network. It comprises both the AN signalling connection between the UE and the AN (RRC connection over 3GPP access or UE-N3IWF connection over N3GPP access) and the N2 connection for this UE between the AN and the AMF.

5.3.3.2 5GS Connection Management states

5.3.3.2.1 General

Two CM states are used to reflect the NAS signalling connectivity of the UE with the AMF:

- CM-IDLE
- CM-CONNECTED

The CM state for 3GPP access and Non-3GPP access are independent of each other, i.e. one can be in CM-IDLE state at the same time when the other is in CM-CONNECTED state.

5.3.3.2.2 CM-IDLE state

A UE in CM-IDLE state has no NAS signalling connection established with the AMF over N1. The UE performs cell selection/cell reselection according to TS 38.304 [50] and PLMN selection according to TS 23.122 [17].

There are no AN signalling connection, N2 connection and N3 connections for the UE in the CM-IDLE state.

If the UE is both in CM-IDLE state and in RM-REGISTERED state, the UE shall, unless otherwise specified in clause 5.3.4.1:

- Respond to paging by performing a Service Request procedure (see TS 23.502 [3] clause 4.2.3.2), unless the UE is in MICO mode (see clause 5.4.1.3);
- perform a Service Request procedure when the UE has uplink signalling or user data to be sent (see TS 23.502 [3] clause 4.2.3.2). Specific conditions apply for LADN, see clause 5.6.5.

The UE shall enter CM-CONNECTED state whenever an AN signalling connection is established between the UE and the AN (entering RRC Connected state over 3GPP access, or at the establishment of the UE-N3IWF connectivity over non-3GPP access). The transmission of an Initial NAS message (Registration Request, Service Request or Deregistration Request) initiates the transition from CM-IDLE to CM-CONNECTED state.

When the UE states in the AMF are CM-IDLE and RM-REGISTERED, the AMF shall:

- perform a network triggered Service Request procedure when it has signalling or mobile-terminated data to be sent to this UE, by sending a Paging Request to this UE (see TS 23.502 [3] clause 4.2.3.4), if a UE is not prevented from responding e.g. due to MICO mode or Mobility Restrictions.

The AMF shall enter CM-CONNECTED state for the UE whenever an N2 connection is established for this UE between the AN and the AMF. The reception of initial N2 message (e.g., N2 INITIAL UE MESSAGE) initiates the transition of AMF from CM-IDLE to CM-CONNECTED state.

The UE and the AMF may optimize the power efficiency and signalling efficiency of the UE when in CM-IDLE state e.g. by activating MICO mode (see clause 5.4.1.3).

5.3.3.2.3 CM-CONNECTED state

A UE in CM-CONNECTED state has a NAS signalling connection with the AMF over N1. A NAS signalling connection uses an RRC connection between the UE and the NG-RAN and an NGAP UE association between the AN and the AMF for 3GPP access. A UE can be in CM-CONNECTED state with an NGAP UE association that is not bound to any TNLA between the AN and the AMF. See clause 5.21.1.2 for details on the state of NGAP UE association for an UE in CM-CONNECTED state. Upon completion of a NAS signalling procedure, the AMF may decide to release the NAS signalling connection with the UE.

In the CM-CONNECTED state, the UE shall:

- enter CM-IDLE state whenever the AN signalling connection is released (entering RRC Idle state over 3GPP access or when the release of the UE-N3IWF connectivity over non-3GPP access is detected by the UE), see TS 38.331 [28] for 3GPP access.

When the UE CM state in the AMF is CM-CONNECTED, the AMF shall:

- enter CM-IDLE state for the UE whenever the logical NGAP signalling connection and the N3 user plane connection for this UE are released upon completion of the AN Releaseprocedure as specified in TS 23.502 [3].

The AMF may keep a UE CM state in the AMF in CM-CONNECTED state until the UE de-registers from the core network.

A UE in CM-CONNECTED state can be in RRC Inactive state, see TS 38.300 [27]. When the UE is in RRC Inactive state the following applies:

- UE reachability is managed by the RAN, with assistance information from core network;
- UE paging is managed by the RAN.
- UE monitors for paging with UE's CN (5G S-TMSI) and RAN identifier.

5.3.3.2.4 5GS Connection Management State models

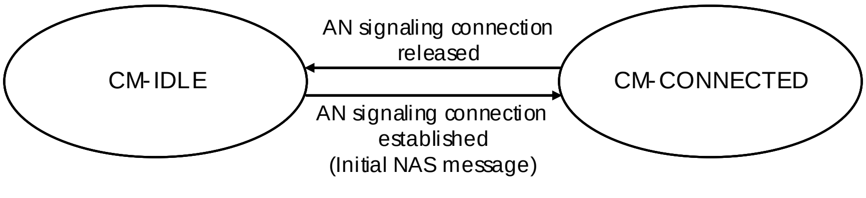

AN signaling connection released
CM-IDLE
CM-CONNECTED
AN signaling connection established
(Initial NAS message)

Figure 5.3.3.2.4-1: CM state transition in UE

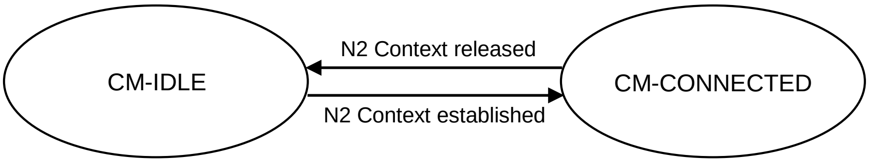


Figure 5.3.3.2.4-2: CM state transition in AMF

When a UE enters CM-IDLE state, the UP connection of the PDU Sessions that were active on this access are deactivated.

NOTE: The activation of UP connection of PDU Sessions is documented in clause 5.6.8.

5.3.3.2.5 CM-CONNECTED with RRC Inactive state

RRC Inactive state applies to NG-RAN.

The AMF, based on network configuration may provide assistance information to the NG-RAN, to assist the NG-RAN's decision whether the UE can be sent to RRC Inactive state.

Editor's note: It is FFS if the UE provides indication of support for RRC inactive state on NAS or AS layer.

The "RRC Inactive assistance information" includes:

- UE specific DRX values.
- the Registration Area provided to the UE;
- Periodic Registration Update timer
- If the AMF has enabled MICO mode for the UE, an indication that the UE is in MICO mode.
- Information from the UE permanent identifier, as defined in TS 38.304 [50], that allows the RAN to calculate the UE's RAN paging occasions.

The RRC Inactive assistance information mentioned above is provided by the AMF during N2 activation with the (new) serving NG-RAN node (i.e. during Registration, Service Request, handover) to assist the NG RAN's decision whether the UE can be sent to RRC Inactive state. RRC Inactive state is part of RRC state machine, and it is up to the RAN to determine the conditions to enter RRC Inactive state. If any of the parameters included in the RRC Inactive Assistance Information changes as the result of NAS procedure, the AMF shall update the RRC Inactive Assistance Information to the NG-RAN node.

When the UE is in CM-CONNECTED state, if the AMF has provided RRC Inactive assistance information, the RAN node may decide to move a UE to CM-CONNECTED with RRC Inactive state.

The state of the N2 and N3 reference points are not changed by the UE entering CM-CONNECTED with RRC Inactive state. A UE in RRC inactive state is aware of the RAN Notification area.

The 5GC network is not aware of the UE transitions between CM-CONNECTED with RRC Connected and CM-CONNECTED with RRC Inactive state, unless the 5GC network is notified via N2 notification procedure in TS 23.502 [3] clause 4.8.3.

At transition into CM-CONNECTED with RRC Inactive state, the NG-RAN configures the UE with a periodic RAN Notification Area Update timer taking into account the value of the Periodic Registration Update timer value indicated in the RRC Inactive Assistance Information, and uses a guard timer with a value longer than the RAN Notification Area Update timer value provided to the UE.

If the periodic RAN Notification Area Update guard timer expires in RAN, the RAN shall initiate AN Release procedure as specified in TS 23.502 [3].

When the UE is in CM-CONNECTED with RRC inactive state, the UE performs PLMN selection procedures as defined in TS 23.122 [17] for CM-IDLE.

When the UE is CM-CONNECTED with RRC Inactive state, the UE may resume the RRC connection due to:

- Uplink data pending;
- Mobile initiated NAS signalling procedure;
- As a response to RAN paging;
- Notifying the network that it has left the RAN Notification area;
- Upon periodic RAN update timer expiration.

If the UE resumes the connection in a different NG-RAN node within the same PLMN, the UE AS context is retrieved from the old NG-RAN node and a procedure is triggered towards the CN (see TS 23.502 [3]).

If the RAN paging procedure, as defined in TS 38.300 [27], is not successful in establishing contact with the UE the procedure shall be handled by the network as follows:

- If NG-RAN has at least one pending NAS PDU for transmission, the RAN node shall initiate the AN Release procedure (see clause 4.2.6, TS 23.502 [3]) to move the UE CM state in the AMF to CM-IDLE state and indicate to the AMF the NAS non-delivery.
- If NG RAN has only pending user plane data for transmission, the NG-RAN node may keep the N2 connection active or initiate the AN Release procedure (see clause 4.2.6, TS 23.502 [3]) based on local configuration in NG-RAN.

NOTE: The user plane data which triggers the RAN paging can be lost, e.g. in case of RAN paging failure.

If a UE in CM-CONNECTED with RRC Inactive state performs cell selection to GERAN/UTRAN/E-UTRAN, it shall enter CM-IDLE and follow idle mode procedures of the selected RAT.

In addition, a UE in CM-CONNECTED state with RRC Inactive state shall enter CM-IDLE state and initiates the NAS recovery procedure in the following cases:

- If RRC resume procedure fails,

  If the UE receives Core Network paging,
- If the periodic RAN Notification Area Update timer expires and the UE cannot successfully resume the RRC connection.
- in any other failure scenario that cannot be resolved in RRC Inactive state and requires the UE to move to CM-IDLE state.

When UE is in CM-CONNECTED with RRC Inactive state, if RAN has received Location Reporting Control message from AMF with the reporting type indicating single stand-alone report, the RAN shall perform RAN paging before reporting the location to AMF.

When UE is in CM-CONNECTED with RRC Inactive state, if RAN has received Location Reporting Control message from AMF with the reporting type indicating continuously reporting whenever the UE changes cell, the RAN shall send a Location Report message to AMF including UE's last known location with time stamp.

When the UE is CM-CONNECTED with RRC Inactive state. If the AMF receives Nudm_UEContextManagement_DeregistrationNotification from UDM, the AMF shall initiate AN Release procedure as specified in TS 23.502 [3].

5.3.3.3 NAS signalling connection management

5.3.3.3.1 General

NAS signalling connection management includes the functions of establishing and releasing a NAS signalling connection.

5.3.3.3.2 NAS signalling connection establishment

NAS signalling connection establishment function is provided by the UE and the AMF to establish a NAS signalling connection for a UE in CM-IDLE state. The AMF shall provide the list of recommended cells/ TAs / NG-RAN node identifiers for paging, if the NG-RAN had provided that information in an earlier AN Release Procedure in the AN (see clause 4.2.6 of 3GPP TS 23.502 [3]).

When the UE in CM-IDLE state needs to transmit an NAS message, the UE shall initiate a Service Request or a registration or Deregistration procedure to establish a signalling connection to the AMF as specified in TS 23.502 [3], clauses 4.2.2 and 4.2.3. If the NAS signalling connection is to be established via a NG-RAN node, but the AMF detects that this UE has already established a NAS signalling connection via old NG-RAN node, the AMF shall release the old established NAS signalling connection by triggering AN Release Procedure.

Based on UE preferences, UE subscription, UE mobility pattern and network configuration, the AMF may keep the NAS signalling connection until the UE de-registers from the network.

5.3.3.3.3 NAS signalling connection Release

The procedure of releasing a NAS signalling connection is initiated by the AN node (either 5G (R)AN node or N3IWF) or the AMF. The NG-RAN node may include the list of recommended cells/ TAs / NG-RAN node identifiers for paging, during the AN Release Procedure in the AN (see clause 4.2.6 of 3GPP TS 23.502 [3]). The AMF stores this information, if provided by the NG-RAN.

The UE considers the NAS signalling connection is released if it detects the AN signalling connection is released. The AMF considers the NAS signalling connection is released if it detects the N2 context is released.

5.3.3.4 Support of a UE connected over both 3GPP and Non-3GPP access

The AMF manages two CM states for an UE: a CM state for 3GPP access and a CM state for Non-3GPP access. An N2 interface can serve the UE for either 3GPP access or for Non 3GPP access. UE connected over both 3GPP and Non-3GPP has got two N2 interfaces, one for each access. A UE may be in any combination of the CM states between 3GPP and Non-3GPP access, e.g. a UE may be CM-IDLE for one access and CM-CONNECTED for the other access, CM-IDLE for both accesses or CM-CONNECTED for both accesses.

When the UE CM state in the AMF is CM-IDLE for 3GPP access and CM-CONNECTED for Non-3GPP access, the AMF shall perform a network triggered service request procedure, when it has downlink data to be sent to this UE for 3GPP access, by sending either the Paging Request via 3GPP access or the NAS notification via Non-3GPP access to this UE (see TS 23.502 [3] clause 4.2.3.4).

Connection Management over Non-3GPP access is further defined in clause 5.5.2.

5.3.4 UE Mobility

5.3.4.1 Mobility Restrictions

5.3.4.1.1 General

Mobility Restrictions restrict mobility handling or service access of a UE in the 5G System. The Mobility Restriction functionality is provided by the UE, the radio access network and the core network.

Mobility Restrictions only apply to 3GPP access, they do not apply to non-3GPP access.

Mobility Restrictions for CM-IDLE state and, for CM-CONNECTED state when in RRC Inactive state are executed by the UE based on information received from the core network. Mobility Restrictions for CM-CONNECTED state when in RRC-Connected state are executed by the radio access network and the core network.

In CM-CONNECTED state, the core network provides Mobility Restrictions to the radio access network within Handover Restriction List.

Mobility Restrictions consists of RAT restriction, Forbidden Area, Service area restrictions and Core Network type restriction as follows:

- RAT restriction:

  Defines the 3GPP Radio Access Technology(ies), a UE is not allowed to access in a PLMN. In a restricted RAT a UE is based on subscription not permitted to initiate any communication for this PLMN. For CM-

CONNECTED state, when radio access network determines target RAT and target PLMN during handover procedure, it should take per PLMN RAT restriction into consideration.

- Forbidden Area:

  In a Forbidden Area under a given RAT, the UE is based on subscription not permitted to initiate any communication with the network for this PLMN. The UE behaviour in terms of cell selection, RAT selection and PLMN selection depends on the network response that informs the UE of Forbidden Area.

NOTE 1: The UE reactions to specific network responses are described in TS 24.501 [47].

- Service area restrictions:

  Defines areas in which the UE may or may not initiate communication with the network as follows:

  - Allowed Area:

    In an Allowed Area under a given RAT, the UE is permitted to initiate communication with the network as allowed by the subscription.

  - Non-Allowed Area:

    In a Non-Allowed Area under a given RAT a UE is service area restricted based on subscription. The UE and the network are not allowed to initiate Service Request or SM signalling to obtain user services (both in CM-IDLE and in CM-CONNECTED states). The RRC procedures while the UE is in CM-CONNECTED with RRC Inactive state are unchanged compared to when the UE is in an Allowed Area. The RM procedures are unchanged compared to when the UE is in an Allowed Area. The UE in a Non-Allowed Area shall respond to core network paging with Service Request and RAN paging.

- Core Network type restriction:

  Defines whether UE is allowed to connect to 5GC for this PLMN.

NOTE 2: The Core Network type restriction can be used e.g. in network deployments where the E-UTRAN connects to both EPC and 5GC as described in clause 5.17.

For a given UE, the core network determines the Mobility restrictions based on UE subscription information, UE location and local policy. The Mobility Restriction may change due to e.g. UE's subscription, location change and local policy. Optionally the Service area restrictions or the Non-Allowed Area may in addition be fine-tuned by the PCF e.g. based on UE location, PEI and network policies. Service area restrictions may be updated during a Registration procedure or UE Configuration Update procedure.

If the network sends Service area restrictions to the UE, the network sends only either an Allowed Area, or a Non-Allowed Area, but not both at the same time, to the UE. If the UE has received an Allowed Area from the network, any TA not part of the Allowed Area is considered by the UE as non-allowed. If the UE has received a Non-Allowed Area from the network, any TA not part of the Non-Allowed Area is considered by the UE as allowed. If the UE has not received any Service area restrictions, any TA in the PLMN is considered as allowed.

If the UE has overlapping areas between RAT restrictions, Forbidden Areas, Service Area Restrictions, or any combination of them, the UE shall proceed in the following precedence order:

- The evaluation of RAT restrictions shall take precedence over the evaluation of any other Mobility Restrictions; and

- The evaluation of Forbidden Areas shall take precedence over the evaluation of Service Area Restrictions.

A UE shall override any RAT restrictions, Forbidden Area and Non-Allowed area restrictions whenever access to the network for regulatory prioritized services like Emergency services and MPS. Also the network shall override any Non-Allowed Area restrictions and RAT restrictions for regulatory prioritized services like Emergency services and MPS.

5.3.4.1.2 Management of service area restrictions

A service area restriction may contain one or more (e.g. up to 16) entire tracking areas. The UE's subscription data in the UDM includes a service area restriction which may contain either Allowed or Non-Allowed Areas–specified by using explicit tracking area identities and/or other geographical information (e.g., longitude/latitude, zip code, etc). The geographical information used to specify allowed or non-allowed area is only managed in the network, and the network will map it to a list of TAs before sending service area restriction information to the UE. The Allowed Area may also be limited by a maximum allowed number of tracking areas, or the allowed area may alternatively be configured as unlimited i.e. it may contain all tracking areas of the PLMN. The registration area of a UE in the non-allowed area should consist of a set of TAs which belongs to a non-allowed area of the UE. The registration area of a UE in the allowed area should consist of a set of TAs which belongs to an allowed area of the UE. The AMF provides the service area restriction in the form of TA(s), which may be a subset of full list stored in UE's subscription data, to the UE during the Registration procedure.

NOTE: As the finest granularity for Service area restrictions is at TA level, subscriptions with limited geographical extent, like subscriptions for Fixed Wireless Access, will be allocated one or a few TAs and will consequently be allowed to access services in a larger area than in e.g. a FWA system.

The UDM stores the service area restrictions of a UE as part of the UE's subscription data. The PCF in the serving network may (e.g. due to varying conditions such as UE's location, application in use, time and date) further adjust service area restrictions of a UE, either by expanding an allowed area or by reducing a non-allowed area or by increasing the maximum allowed number of tracking areas. The UDM and the PCF may update the service area restrictions of a UE at any time. For the UE in CM-CONNECTED state the AMF updates the UE and RAN immediately. For UE in CM-IDLE state the AMF may page the UE immediately or store the updated service area restriction and update the UE upon next signalling interaction with the UE.

During registration, if the service area restrictions of the UE is not present in the AMF, the AMF fetches from the UDM the service area restrictions of the UE that may be further adjusted by the PCF. The serving AMF shall enforce the service area restrictions of a UE. A limited allowed area given by a maximum allowed number of tracking areas, may be dynamically assigned by the AMF adding, any not yet visited (by the UE) tracking areas to the Allowed area until the maximum allowed number of tracking areas is reached. When the AMF assigns a limited allowed area to the UE, then the AMF shall provide the UE with any pre-configured and/or dynamically assigned allowed area. For a UE in CM-CONNECTED state the AMF shall indicate the service area restrictions of this UE to the RAN. The UE shall store the received Service Area Restrictions, and if there is previously stored Service Area Restrictions. The UE stores either Allowed Area or Non-Allowed Area, but not both of them.

Upon change of serving AMF due to mobility, the old AMF may provide the new AMF with the service area restrictions of the UE that may be further adjusted by the PCF.

The network may perform paging for a UE to update service area restrictions with Generic UE Configuration Update procedure (see in TS 23.502 [3] clause 4.2.4).

In case of roaming, the service area restrictions are transferred from the UDM via the serving AMF to the serving PCF in the visited network. The serving PCF in the visited network may further adjust the service area restrictions.

5.3.4.2 Mobility Pattern

The Mobility Pattern is a concept that may be used by the AMF to characterise and optimise the UE mobility. The AMF determines and updates Mobility Pattern of the UE based on subscription of the UE, statistics of the UE mobility, network local policy, and the UE assisted information, or any combination of them. The statistics of the UE mobility can be historical or expected UE moving trajectory.

UE mobility pattern can be used by the AMF to optimize mobility support provided to the UE, for example, Registration area Allocation.

5.3.4.3 Radio Resource Management functions

To support radio resource management in RAN the AMF provides the parameter 'Index to RAT/Frequency Selection Priority' (RFSP Index) to RAN across N2. The RFSP Index is mapped by the RAN to locally defined configuration in order to apply specific RRM strategies. The RFSP Index is UE specific and applies to all the Radio Bearers. Examples of how this parameter may be used by the RAN:

- to derive UE specific cell reselection priorities to control idle mode camping.
- to decide on redirecting active mode UEs to different frequency layers or RATs.

The AMF receives the subscribed RFSP Index from the UDM (e.g., during the Registration procedure). For non-roaming subscribers, the AMF chooses the RFSP Index in use according to one of the following procedures, depending on operator's configuration:

- the RFSP Index in use is identical to the subscribed RFSP Index, or
- the AMF chooses the RFSP Index in use based on the subscribed RFSP Index, the locally configured operator's policies and the UE related context information available at the AMF, including UE's usage setting, if received during Registration procedures (see clause TS 23.502 [3]).

NOTE: One example of how the AMF can use the "UE's usage setting," is to select an RFSP value that enforces idle mode camping on E-UTRA for a UE acting in a "Voice centric" way, in case voice over NR is not supported in the specific Registration Area and it contains NR cells.

The AMF may report to the PCF the subscribed RFSP Index received from the UDM for further evaluation as described in clause 6.1.2.1 in TS 23.503 [45]. When receiving the authorized RFSP Index from the PCF, the AMF shall replace the subscribed RFSP Index with the authorized RFSP Index.

For roaming subscribers the AMF may alternatively choose the RFSP Index in use based on the visited network policy, but can take input from the HPLMN into account (e.g., an RFSP Index value pre-configured per HPLMN, or a single RFSP Index value to be used for all roamers independent of the HPLMN).

The RFSP Index in use is also forwarded from source to target RAN node when Xn or N2 is used for intra-NG-RAN handover.

The AMF stores the subscribed RFSP Index value received and the RFSP Index value in use. During the Registration Update procedure, the AMF may update the RFSP Index value in use (e.g. the AMF may need to update the RFSP Index value in use if the UE related context information in the AMF has changed). When the RFSP Index value in use is changed, the AMF immediately provides the updated RFSP Index value in use to NG-RAN node by modifying an existing UE context or by establishing a new UE context in RAN or by being configured to include the updated RFSP Index value in use in the DOWNLINK NAS TRANSPORT message if the user plane establishment is not needed. During inter-AMF mobility procedures, the source AMF forwards both RFSP Index values to the target AMF. The target AMF may replace the received RFSP Index value in use with a new RFSP Index value in use that is based on the operator's policies and the UE related context information available at the target AMF.

5.4 3GPP access specific aspects

5.4.1 UE reachability in CM-IDLE

5.4.1.1 General

Reachability management is responsible for detecting whether the UE is reachable and providing UE location (i.e. access node) for the network to reach the UE. This is done by paging UE and UE location tracking. The UE location tracking includes both UE registration area tracking (i.e. UE registration area update) and UE reachability tracking ((i.e. UE periodic registration area update)). Such functionalities can be either located at 5GC (in case of CM-IDLE state) or NG-RAN (in case of CM-CONNECTED state).

The UE and the AMF negotiate UE reachability characteristics for CM-IDLE state during registration and registration update procedures.

Two UE reachability categories are negotiated between UE and AMF for CM-IDLE state:

1. UE reachability allowing Mobile Terminated data while the UE is CM-IDLE state.
    - The UE location is known by the network on a Tracking Area List granularity
    - Paging procedures apply to this category.
    - Mobile originating and mobile terminated data apply in this category for both CM-CONNECTED and CM-IDLE state.
2. Mobile Initiated Connection Only (MICO) mode:

- Mobile originated data applies in this category for both CM-CONNECTED and CM-IDLE state.
- Mobile terminated data is only supported when the UE is in CM-CONNECTED state.

Whenever a UE in RM-REGISTERED state enters CM-IDLE state, it starts a periodic registration timer according to the periodic registration timer value received from the AMF during a registration procedure.

The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of the periodic registration timer, the UE shall perform a periodic registration. If the UE moves out of network coverage when its periodic registration timer expires, the UE shall perform a registration update when it next returns to the coverage.

The AMF runs a Mobile Reachable timer for the UE. The timer is started with a value longer than the UE's periodic registration timer whenever the CM state for the UE in RM-REGISTERED state changes to CM-IDLE. If the AMF receives an elapsed time from RAN when RAN initiate UE context release indicating UE unreachable, the AMF should deduce a Mobile Reachable timer value based on the elapsed time received from RAN and the normal Mobile Reachable timer value. The AMF stops the Mobile Reachable timer, if the UE CM state in the AMF moves to CM-CONNECTED state. If the Mobile Reachable timer expires, the AMF determines that the UE is not reachable.

However, the AMF does not know for how long the UE remains not reachable, thus the AMF shall not immediately de-register the UE. Instead, after the expiry of the Mobile Reachable timer, the AMF should clear the PPF flag and shall start an Implicit De-registration timer, with a relatively large value. The AMF shall stop the Implicit Deregistration timer and set the PPF flag if the AMF moves the UE CM state in the AMF to CM-CONNECTED state.

NOTE: If the UE CM state in the AMF is CM-IDLE, then AMF considers the UE always unreachable if the UE is in MICO mode (refer to clause 5.4.1.3).

If the PPF is not set, the AMF does not page the UE and shall reject any request for delivering DL signalling or data to this UE.

If the Implicit De-registration timer expires before the UE contacts the network, the AMF implicitly de-register the UE.

As part of deregistration for a particular access (3GPP or non-3GPP), the AMF shall request the UE's related SMF to release the PDU Sessions established on that access.

5.4.1.2 UE reachability allowing mobile terminated data while the UE is CM-IDLE

The AMF considers a UE in RM-REGISTERED state to be reachable by CN paging if the UE CM state in the AMF is CM-IDLE state unless the UE applies MICO mode.

5.4.1.3 Mobile Initiated Connection Only (MICO) mode

A UE may indicate preference for MICO mode during Initial Registration or Registration Update procedure. The AMF, based on local configuration, Expected UE Behaviour if available, UE indicated preferences, UE subscription information and network policies, or any combination of them, determines whether MICO mode is allowed for the UE and indicates it to the UE during Registration procedure. If the UE does not indicate preference for MICO mode during Registration procedure, the AMF shall not activate MICO mode for this UE.

The UE and the AMF re- negotiate the MICO mode at every subsequent Registration procedure. When the UE is in CM-CONNECTED, the AMF may deactivate MICO mode by triggering Registration Update procedure through UE Configuration Update procedure as described in clause 4.2.4 in TS 23.502 [3].

The AMF assigns a registration area to the UE during the registration procedure. When the AMF indicates MICO mode to a UE, the registration area is not constrained by paging area size. If the AMF serving area is the whole PLMN, based on local policy, and subscription information, may decide to provide an "all PLMN" registration area to the UE. In that case, re-registration to the same PLMN due to mobility does not apply.

If Mobility Restrictions are applied to a UE in MICO mode, the AMF needs to allocate an Allowed Area/Non-Allowed Area to the UE as specified in clause 5.3.4.1.

When the AMF indicates MICO mode to a UE, the AMF considers the UE always unreachable while the UE CM state in the AMF is CM-IDLE. The AMF rejects any request for downlink data delivery for UE in MICO mode and whose UE CM state in the AMF is CM-IDLE with an appropriate cause. For MT-SMS over NAS, the AMF notifies the SMSF that UE is not reachable, then the procedure of the unsuccessful Mobile terminating SMS delivery described in clause 4.13.3.9 in TS 23.502 [3] is performed. The AMF also defers location services, etc. The UE in MICO mode is only reachable for mobile terminated data or signalling when the UE is in CM-CONNECTED.

A UE in MICO mode need not listen to paging while in CM-IDLE. A UE in MICO mode may stop any access stratum procedures in CM-IDLE, until the UE initiates transition from CM-IDLE to CM-CONNECTED due to one of the following triggers:

- A change in the UE (e.g. change in configuration) requires an update of its registration with the network.
- Periodic registration timer expires.
- MO data pending.
- MO signalling pending (e.g. SM procedure initiated).

If a registration area that is not the "all PLMN" registration area is allocated to a UE in MICO mode, then the UE determines if it is within the registration area or not when it has MO data or MO signalling and performs Registration Update if it is not within the registration area.

A UE initiating emergency service shall not indicate MICO preference during Registration procedure. When the MICO mode is already activated in the UE, the UE shall request deactivation of MICO mode via Registration procedure while the UE is in CM-CONNECTED state after PDU Establishment procedure for Emergency Services is completed.

5.4.2 UE reachability in CM-CONNECTED

For a UE in CM-CONNECTED state:

- the AMF knows the UE location on a serving (R)AN node granularity.
- the NG-RAN notifies the AMF when UE becomes unreachable from RAN point of view.

UE RAN reachability management is used by RAN for UEs in RRC Inactive state, see TS 38.300 [27]. The location of a UE in RRC Inactive state is known by the RAN on a RAN Notification area granularity. A UE in RRC Inactive state is paged in cells of the RAN Notification area that is assigned to the UEs. The RAN Notification area can be a subset of cells configured in UE's Registration Area or all cells configured in the UE's Registration Area. UE in RRC Inactive state performs Paging Area Update when entering a cell that is not part of the RAN Notification area that is assigned to the UE.

At transition into RRC Inactive state RAN configures the UE with a periodic RAN Notification Area Update timer value and the timer is restarted in the UE with this initial timer value. After the expiry of the periodic RAN Notification Area Update timer in the UE, the UE in RRC Inactive state performs periodic RAN Notification Area Update, as specified in TS 38.300 [27].

To aid the UE reachability management in the AMF, RAN uses a guard timer with a value longer than the RAN Notification Area Update timer value provided to the UE. Upon the expiry of the periodic RAN Notification Area Update guard timer in RAN, the RAN shall initiate the AN Release procedure as specified in TS 23.502 [3]. The RAN may provide the elapsed time since RAN's last contact with the UE to AMF.

5.4.3 Paging strategy handling

5.4.3.1 General

Based on operator configuration, the 5GS supports the AMF and NG-RAN to apply different paging strategies for different types of traffic.

In case of UE in CM-IDLE state, the AMF performs paging and determines the paging strategy based on e.g. local configuration, what NF triggered the paging and information available in the request that triggered the paging.

In case of UE in CM-CONNECTED with RRC Inactive state, the NG-RAN performs paging and determines the paging strategy based on e.g. local configuration, and information received from AMF as described in clause 5.4.6.3 and SMF as described in clause 5.4.3.2.

In case of Network Triggered Service Request from SMF, the SMF determines the 5QI and ARP based on the downlink data or the notification of downlink data received from UPF. The SMF includes the 5QI and ARP corresponding to the received downlink PDU in the request sent to the AMF. If the UE is in CM IDLE, the AMF uses e.g. the 5QI and ARP to derive different paging strategies as described in TS 23.502, clause 4.2.3.4.

NOTE: The 5QI is used by AMF to determine suitable paging strategies.

5.4.3.2 Paging Policy Differentiation

Paging policy differentiation is an optional feature that allows the AMF, based on operator configuration, to apply different paging strategies for different traffic or service types provided within the same PDU Session. In this release this feature applies only to PDU Session of IP type.

When the 5GS supports the Paging Policy Differentiation (PPD) feature, the DSCP value (TOS in IPv4 / TC in IPv6) is set by the application to indicate to the 5GS which Paging Policy should be applied for a certain IP packet. For example, as defined in TS 23.228 [15], the P-CSCF may support Paging Policy Differentiation by marking packet(s) to be sent towards the UE that relate to a specific IMS services (e.g. conversational voice as defined in IMS multimedia telephony service).

It shall be possible for the operator to configure the SMF in such a way that the Paging Policy Differentiation feature only applies to certain HPLMNs, DNNs and 5QIs. In case of HR roaming, this configuration is done in the SMF in the VPLMN.

NOTE 1: Support of Paging Policy Differentiation in case of HR roaming requires inter operator agreements including on the DSCP value associated with this feature.

In case of Network Triggered Service Request and UPF buffering downlink data packet, the UPF shall include the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the downlink data packet and an indication of the corresponding QoS Flow in the data notification message sent to the SMF.

When PPD applies, the SMF determines the Paging Policy Indicator (PPI) based on the information received from the UPF. In case of Network Triggered Service Request and SMF buffering downlink data packet, when PPD applies, the SMF determines the PPI based on the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the received downlink data packet and an indication of the corresponding QoS Flow. The SMF includes the PPI, the ARP and the 5QI in the N11 message sent to the AMF. If the UE is in CM IDLE, the AMF uses this information to derive a paging strategy, and sends paging messages to NG-RAN over N2. The paging messages sent to NG-RAN may include the PPI.

NOTE 2: Network configuration needs to ensure that the information used as a trigger for Paging Policy Indication is not changed within the 5GS.

NOTE 3: Network configuration needs to ensure that the specific DSCP in TOS (IPv4) / TC (IPv6) value, used as a trigger for Paging Policy Indication, is managed correctly in order to avoid the accidental use of certain paging policies.

The SMF configures the UPF to put in different QoS Flows traffic with different paging differentiation requirements and may indicate over N2 to the NG-RAN the Paging Policy Indicator (PPI) for a QoS Flow (QFI) of a PDU Session. For a UE in RRC Inactive state the NG-RAN may, based on 5QI, ARP and this PPI associated with the QFI of an incoming DL PDU enforce specific paging policies applied in case of NG-RAN paging.

5.4.3.3 Paging Priority

Paging Priority is a feature that allows the AMF to include an indication in the Paging Message sent to NG-RAN that the UE be paged with priority. The decision by the AMF whether to include Paging Priority in the Paging Message is based on the ARP value in the message received from the SMF for an IP packet waiting to be delivered in the UPF. If the ARP value is associated with select priority services (e.g., MPS, MCS), the AMF includes Paging Priority in the Paging Message. When the NG-RAN receives a Paging Message with Paging Priority, it handles the page with priority.

The AMF while waiting for the UE to respond to a page sent without priority receives another message from the SMF with an ARP associated with select priority services (e.g., MPS, MCS), the AMF sends another Paging message to the (R)AN including the Paging Priority.

For a UE in RRC Inactive state, the NG-RAN determines Paging Priority based on the ARP associated with the QoS Flow as provisioned by the operator policy, and the Core Network Assisted RAN paging information from AMF as described in clause 5.4.6.3.

5.4.4 UE Radio Capability handling

5.4.4.1 UE radio capability information storage in the AMF

The UE Radio Capability information contains information on RATs that the UE supports (e.g. power class, frequency bands, etc). Consequently, this information can be sufficiently large that it is undesirable to send it across the radio interface at every transition of UE CM state in the AMF from CM-IDLE to CM-CONNECTED. To avoid this radio overhead, the AMF shall store the UE Capability information during CM-IDLE state for the UE and RM-REGISTERED state for the UE and the AMF shall if it is available, send its most up to date UE Radio Capability information to the RAN in the N2 REQUEST message.

The AMF deletes the UE radio capability when the UE RM state in the AMF transitions to RM-DEREGISTERED.

The UE Radio Capability is maintained in the core network, even during AMF reselection.

The RAN stores the UE Radio Capability information, received in the N2 message or obtained from the UE, for the duration of the UE staying in RRC connected or RRC Inactive state.

5.4.4.2 Feature specific UE/RAN Radio information and Compatibility Request

If the AMF requires specific information on the UE radio capabilities support to be able to enable a specific feature or set a specific NAS parameter, then the AMF may send a Feature specific UE/RAN information and Compatibility Request message to the NG-RAN node. This request may be transmitted standalone or included during N2 activation.

In this release of the specification, this procedure is used for UE radio capabilities support to be able to set the IMS voice over PS Session Supported Indication in AMF.

The AMF includes a list of features, including for each of the features:

- The Specific Feature for which it needs information.

The response from the RAN includes for each requested feature:

- Feature compatibility at the NG-RAN

5.4.4.3 Paging assistance information

The paging assistance information contains UE radio related information that assists the RAN for efficient paging. The Paging assistance information contains:

- UE radio capability for paging information:
    - The UE Radio Capability for Paging Information may contain UE Radio Paging Information provided by the UE to the NG-RAN node, and other information derived by the NG-RAN node (e.g. band support information) from the UE Radio Capability information.
- Information On Recommended Cells And RAN nodes For Paging
    - Information sent by the NG-RAN, and used by the AMF when paging the UE to help determining the NG RAN nodes to be paged as well as to provide the information on recommended cells to each of these RAN nodes, in order to optimize the probability of successful paging while minimizing the signalling load on the radio path.

The RAN provides this information during N2 release.

5.4.5 DRX (Discontinuous Reception) framework

The 5G System supports DRX architecture which allows Idle mode DRX cycle is negotiated between UE and the AMF. The Idle mode DRX cycle applies in CM-IDLE state. During the registration procedure, a UE may provide DRX parameters (i.e. Idle mode DRX cycle) that the UE wants to use and the AMF returns the DRX parameters to be used. For details of DRX parameters, see TS 38.300 [27].

If the UE does not provide any DRX parameters during registration procedure to the AMF, the DRX cycle broadcasted by the RAN is applied to the UE.

The UE specific DRX Parameters are sent from the old AMF to the new AMF as part of the MM context information during the AMF change mobility

5.4.6 Core Network assistance information for RAN optimization

5.4.6.1 General

Core Network assistance information for RAN aids the RAN to optimize the UE state transition steering and the RAN paging strategy formulation in RRC-Inactive state. The core network assistance information includes the information set, Core Network assisted RAN parameters tuning, which assist RAN optimize the UE RRC state transition and CM state transition decision. It also includes the information set, Core Network assisted RAN paging information, which assist RAN to formulate an optimized paging strategy when RAN paging is triggered.

5.4.6.2 Core Network assisted RAN parameters tuning

Core Network assisted RAN parameters tuning aids the RAN to minimize the UE state transitions and achieve optimum network behaviour. How the RAN uses the CN assistance information is not defined in this specification.

CN assistance information may be derived by the AMF per UE in the AMF based on collection of UE behaviour statistics and/or other available information about the expected UE behaviour (such as subscribed DNN, SUPI ranges, or other information). If the Expected UE Behaviour parameters of the UE is available, the AMF may use this information for selecting the CN assisted RAN parameter values. If the AMF is able to derive the Mobility Pattern of the UE (as described in clause 5.3.4.2), the AMF may take the Mobility Pattern information into account when selecting the CN assisted RAN parameter values.

The Expected UE Behaviour parameters and the Mobility Pattern information are used by the AMF as input to derive the CN-assisted RAN parameter values. The Expected UE Behaviour parameters can be provisioned by external party via the NEF, as described in clause 5.20. For the case of statistics-based CN assistance information collection, this may be enabled based on local configuration (e.g. subscribed DNN, SUPI ranges or other subscription information).

The CN assistance information provides the RAN with a way to understand the UE behaviour for these aspects:

- "Expected UE activity behavior", i.e. the expected pattern of the UE's changes between CM-CONNECTED and CM-IDLE states. This may be derived e.g. from the statistical information, or Expected UE Behaviour or from subscription information.

- "Expected HO behavior", i.e. the expected interval between inter-RAN handovers. This may be derived by the AMF e.g. from the Mobility Pattern information

The AMF decides when to send this information to the RAN as "Expected UE behaviour" carried in N2 signalling over the N2 interface.

NOTE: The calculation of the CN assistance information, i.e. the algorithms used and related criteria, and the decision when it is considered suitable and stable to send to the RAN are vendor specific.5.4.6.3 Core Network assisted RAN paging information

Core Network assisted RAN paging information aids the RAN to formulate a RAN paging policy and strategy in RRC-Inactive state, besides the PPI and QoS information associated to the QoS Flows as indicated in clause 5.4.3.

CN assisted RAN paging information may be derived by the AMF per UE and/or per PDU Session based on collection of UE behaviour statistics and/or other available information about the expected UE behaviour (such as subscribed DNN, SUPI ranges, Multimedia priority service), and/or information received from other network functions when downlink signalling is triggered.

The CN assisted RAN paging information consists of a service priority (values 1-256) which provides AN with a way to understand how important the downlink signalling is. The AMF derives this service priority based on available information as described above. The method to derive the service priority is implementation depended and can be controlled by operator.

The Core Network may provide the CN assisted RAN paging information to RAN in different occasions, e.g. during downlink N1 and N2 message delivery, etc.

5.5 Non-3GPP access specific aspects

5.5.1 Registration Management

The UE shall enter RM-DEREGISTERED state and the AMF shall enter RM-DEREGISTERED state for the UE on non-3GPP access as follows:

- at the UE and at the AMF, after performing an Explicit Deregistration procedure;
- at the AMF, after the Network non-3GPP Implicit Deregistration timer has expired.
- at the UE, after the UE non-3GPP Deregistration timer has expired.

NOTE: This is assumed to leave sufficient time to allow the UE to re-activate UP connections for the established PDU Sessions over 3GPP or non-3GPP access.

Whenever a UE registered over non-3GPP access enters CM-IDLE state for the non-3GPP access, it starts the UE non-3GPP Deregistration timer according to the value received from the AMF during a Registration procedure.

Over non-3GPP access, the AMF runs the Network non-3GPP Implicit Deregistration timer. The Network non-3GPP Implicit Deregistration timer is started with a value longer than the UE's non-3GPP Deregistration timer, whenever the CM state for the UE registered over non-3GPP access changes to CM-IDLE for the non-3GPP access.

For an UE that is registered over Non-3GPP access, a change of the point of attachment (e.g. change of WLAN AP) shall not lead the UE to perform a registration update procedure.

A UE shall not provide 3GPP-specific parameters (e.g. indicate a preference for MICO mode) during registration over a non-3GPP access.

5.5.2 Connection Management

A UE that successfully establishes an NWu connection over an Untrusted Non-3GPP access transitions to CM-CONNECTED state for the Untrusted Non-3GPP access.

In case of Untrusted Non-3GPP access to 5GC, the NWu signalling is released either as a result of an Explicit Deregistration procedure or an AN Release procedure. In addition, the N3IWF may explicitly release the NWu signalling connection due to NWu connection failure, as determined by the "dead peer detection" mechanism in IKEv2 defined in RFC 7296 [60]. Further details on how NWu connection failure is detected is out of scope of 3GPP specifications. The release of the NWu signalling connection between the UE and the N3IWF shall be interpreted as follows:

- By the N3IWF as a criterion to release the N2 connection.
- By the UE as a criterion for the UE to transition to CM-IDLE. A UE registered over non-3GPP access remains in RM-REGISTERED state, unless the NWu connection release occurs as part of a Deregistration procedure over non-3GPP access in which case the UE enters the RM-DEREGISTERED state. When the UE in RM-REGISTERED transitions to CM-IDLE, the UE non-3GPP Deregistration timer starts running in the UE. The UE non-3GPP Deregistration timer stops when the UE moves to CM-CONNECTED state or to the RM-DEREGISTERED state.

NOTE 1: When moved to CM-IDLE state over one access, the UE can attempt to re-activate UP connections for the PDU Sessions over other access, per UE policies and depending on the availability of these accesses.

NOTE 2: The release of the NWu at the UE can occur as a result of explicit signalling from the N3IWF, e.g. IKE INFORMATION EXCHANGE or as a result of the UE detecting NWu connection failure, e.g. as determined by the "dead peer detection" mechanism in IKEv2 as defined in RFC 7296 [60]. Further details on how the UE detects NWu connection failure is out of scope of 3GPP specifications.

In case of Untrusted Non-3GPP access, when the AMF releases the N2 interface, the N3IWF shall release all the resources associated with the UE including the NWu connection with the UE. A release of the N2 connection by the AMF shall set the CM state for the UE in the AMF to CM-IDLE.

NOTE 3: It is assumed that a UE configured to receive services from a 5GC over non-3GPP access that is RM-DEREGISTERED or CM-IDLE over the non-3GPP access will attempt to establish an NWu connection and transition to CM-CONNECTED mode whenever the UE successfully connects to a non-3GPP access unless prohibited by the network to make a NWu connection (e.g. due to network congestion).

An UE cannot be paged on Untrusted Non-3GPP access.

When a UE registered simultaneously over a 3GPP access and a non-3GPP access moves all the PDU Sessions to one of the accesses, whether the UE initiates a Deregistration procedure in the access that has no PDU Sessions is up to the UE implementation.

Release of PDU Sessions over the non-3GPP access does not imply the release of N2 connection.

When the UE has PDU Sessions routed over the non-3GPP access and the UE state becomes CM-IDLE for the non-3GPP access, these PDU Sessions are not released to enable the UE to move the PDU Sessions over the 3GPP access based on UE policies. The core network maintains the PDU Sessions but deactivates the N3 user plane connection for such PDU Sessions.

5.5.3 UE Reachability

5.5.3.1 UE reachability in CM-IDLE

An UE cannot be paged over Untrusted Non-3GPP access.

If the UE states in the AMF are CM-IDLE and RM-REGISTERED for the non-3GPP access, there may be PDU Sessions that were last routed over the non-3GPP access and without user plane resources. If the AMF receives a data notification with a Non-3GPP Access Type indication from an SMF for a PDU Session corresponding to a UE that is CM-IDLE for non-3GPP access, and the UE is registered over 3GPP access in the same PLMN as the one registered over non-3GPP access, a Network Triggered Service Request may be performed over the 3GPP access independently of whether the UE is CM-IDLE or CM-CONNECTED over the 3GPP access. In this case, the AMF provides an indication that the procedure is related to pending down link data for non-3GPP access. If the UE is in CM-IDLE over the 3GPP access, the AMF does not include the PDU Session ID of the specific PDU Session for which Access Type is set to non-3GPP access, as specified in clause 5.6.8.

NOTE: The UE behaviour upon such network triggered Service Request is specified in clause 5.6.8.

5.5.3.2 UE reachability in CM-CONNECTED

For a UE in CM-CONNECTED state:

- the AMF knows the UE location on a N3IWF node granularity.
- the N3IWF releases the N2 connection when UE becomes unreachable from N3IWF point of view, i.e. upon NWu release.

5.6 Session Management

5.6.1 Overview

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

Subscription Information may include multiple DNNs and may contain a Default DNN. The UE is assigned to a default DNN if it does not provide a valid DNN in a PDU Session Establishment Request sent to the network.

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

NOTE 1: In this release the 5GC does not support dual stack PDU Session (PDU Session type IPv4v6): The 5GC supports dual Stack UEs by using separate PDU Sessions for IPv4 and IPv6.

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

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

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

- The allowed PDU Session Types and the default PDU Session Type.
- The allowed SSC modes and the default SSC mode.
- QoS Information (refer to clause 5.7): the subscribed Session-AMBR, Default 5QI and Default ARP.
- The static IP address/prefix.

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

NOTE 2: In this release, at a given time, a PDU Session is routed over only a single access network.

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

In a PDU Session establishment request sent to the network, the UE shall provide a PDU Session Identifier. PDU Session ID is unique per UE and is the identifier used to uniquely identify one of an UE's PDU Sessions. PDU Session ID shall be stored in the UDM to support handover between 3GPP and non-3GPP access when different PLMNs are used for the two accesses. The UE may also provide:

- A PDU Session Type.
- S-NSSAI.
- The DNN (Data Network Name).
- The SSC mode (Service and Session Continuity mode defined in clause 5.6.9.2).

Table 5.6.1-1: Attributes of a PDU Session

PDU Session attribute	May be modified later during the lifetime of the PDU Session	Notes
S-NSSAI	No	(Note 2)
DNN (Data Network Name)	No	(Note 1)(Note 2)
PDU Session Type	No	(Note 1)
SSC mode	No	(Note 1) The semantics of Service and Session Continuity mode is defined in clause 5.6.9.2
PDU Session Id	No	
NOTE 1: If it is not provided by the UE, the network determines the parameter based on default information received in user subscription. Subscription to different DNN(s) and S-NSSAI(s) may correspond to different default SSC modes and different default PDU Session Types NOTE 2: S-NSSAI and DNN are used by AMF to select a SMF to handle a new session. Refer to clause 6.3.2.		

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

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

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

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

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

NOTE 3: User Plane resources for PDU Sessions of a UE, except for regulatory prioritized service like Emergency Services and MPS, can be deactivated by the SMF if the UE is only reachable for regulatory prioritized services.

NOTE 4: The handling if the UE goes out of the SMF service area is not specified in this release.

5.6.2 Interaction between AMF and SMF

The AMF and SMF are separate Network Functions.

N1 related interaction with SMF is as follows:

- The single N1 termination point is located in AMF. The AMF forwards SM related NAS information to the SMF based on the PDU Session ID in the NAS message. Further SM NAS exchanges (e.g. SM NAS message responses) for N1 NAS signalling received by the AMF over an access (e.g. 3GPP access or non-3GPP access) are transported over the same access.
- The serving PLMN ensures that subsequent SM NAS exchanges (e.g. SM NAS message responses) for N1 NAS signalling received by the AMF over an access (e.g. 3GPP access or non-3GPP access) are transported over the same access.
- SMF handles the Session management part of NAS signalling exchanged with the UE.
- The UE shall only initiate PDU Session establishment in RM-REGISTERED state.
- When a SMF has been selected to serve a specific PDU Session, AMF has to ensure that all NAS signalling related with this PDU Session is handled by the same SMF instance.
- Upon successful PDU Session establishment, the AMF and SMF stores the Access Type that the PDU Session is associated.

N11 related interaction with SMF is as follows:

- The AMF reports the reachability of the UE based on a subscription from the SMF, including:

  - The UE location information with respect to the area of interest indicated by the SMF.

- The SMF indicates to AMF when a PDU Session has been released.
- Upon successful PDU Session establishment, AMF stores the identification of serving SMF of UE and SMF stores the identification of serving AMF of UE including the AMF set. When trying to reach the AMF serving the UE, the SMF may need to apply the behaviour described for "the other CP NFs" in clause 5.21.

N2 related interaction with SMF is as follows:

- Some N2 signalling (such as Handover related signalling) may require the action of both AMF and SMF. In such case, the AMF is responsible to ensure the coordination between AMF and SMF. The AMF may forward the SM N2 signalling towards the corresponding SMF based on the PDU Session ID in N2 signalling.
- SMF shall provide PDU Session Type together with PDU Session ID to NG-RAN, in order to facilitate NG-RAN to apply suitable header compression mechanism to packet of different PDU type. Details refer to TS 38.413 [34].

N3 related interaction with SMF is as follows:

- Selective activation and deactivation of UP connection of existing PDU Session is defined in clause 5.6.8.

N4 related interaction with SMF is as follows:

- When it is made aware by the UPF that some DL data has arrived for a UE without downlink N3 tunnel information, the SMF interacts with the AMF to initiate Network Triggered Service Request procedure. In this case, if the SMF is aware that the UE is unreachable or if the UE is reachable only for regulatory prioritized service and the PDU Session is not for regulatory prioritized service, then the SMF shall not inform DL data notification to the AMF

The AMF is responsible of selecting the SMF per procedures described in clause 6.3.2. For this purpose, it gets subscription data from the UDM that are defined in that clause. Furthermore, it retrieves the subscribed UE-AMBR from the UDM to send it to the (R)AN as defined in clause 5.7.2

AMF-SMF interactions to support LADN are defined in clause 5.6.5.

In order to support charging data collection and to fulfill regulatory requirement (in order to provide NPLI - Network Provided Location Information- as defined in TS 23.228 [15]) related with with the set-up, modification and release of IMS Voice calls or with SMS transfer the following applies

- At the time of the establishment of a PDU Session, the AMF provides the SMF with the PEI of the UE if the PEI is available at the AMF.
- When it forwards UL NAS or N2 signalling to a peer NF (e.g. to SMF or to SMSF) or during the UP connection activation of a PDU Session, the AMF provides any User Location Information it has received from the 5G-AN as well as the Access Type (3GPP - Non 3GPP) of the AN over which it has received the UL NAS or N2 signalling. The AMF also provides the corresponding UE Time Zone.

The User Location Information, the access type and the UE Time Zone may be further provided by SMF to PCF. The PCF may get this information from the SMF in order to provide NPLI to applications (such as IMS) that have requested it.

The User Location Information may correspond to

- In case of a NG-RAN: a Cell-Id.
- In case of a N3IWF: an UE local IP address (used to reach the N3IWF) and optionally UDP or TCP source port number (if NAT is detected).

5.6.3 Roaming

In case of roaming the 5GC supports following possible deployments scenarios for a PDU Session:

- "Local Break Out" (LBO) where the SMF and all UPF(s) involved by the PDU Session are under control of the VPLMN.

- "Home Routed" (HR) where the PDU Session is supported by a SMF function under control of the HPLMN, by a SMF function under control of the VPLMN, by at least one UPF under control of the HPLMN and by at least one UPF under control of the VPLMN. In this case the SMF in HPLMN selects the UPF(s) in the HPLMN and the SMF in VPLMN selects the UPF(s) in the VPLMN. This is further described in clause 6.3.

NOTE 1: The use of an UPF in the VPLMN e.g. enables VPLMN charging, VPLMN LI and minimizes the impact on the HPLMN of the UE mobility within the VPLMN (e.g. for scenarios where SSC mode 1 applies).

Different simultaneous PDU Sessions of an UE may use different modes: Home Routed and LBO. The HPLMN can control via subscription data per DNN and per S-NSSAI whether a PDU Session is to be set-up in HR or in LBO mode.

In case of PDU Sessions per Home Routed deployment:

- NAS SM terminates in the SMF in VPLMN.
- The SMF in VPLMN forwards to the SMF in the HPLMN SM related information.
- The SMF in the HPLMN receives the SUPI of the UE from the SMF in the VPLMN during the PDU Session Establishment procedure.
- The SMF in HPLMN is responsible to check the UE request with regard to the user subscription and to possibly reject the UE request in case of mismatch. The SMF in HPLMN obtains subscription data directly from the UDM.
- The SMF in HPLMN may send QoS requirements associated with a PDU Session to the SMF in VPLMN. This may happen at PDU Session establishment and after the PDU Session is established. The interface between SMF in HPLMN and SMF in VPLMN is also able to carry (N9) User Plane forwarding information exchanged between SMF in HPLMN and SMF in VPLMN. The SMF in the VPLMN may check QoS requests from the SMF in HPLMN with respect to roaming agreements.

In home routed roaming case, the AMF selects an SMF in the VPLMN and a SMF in the HPLMN, and provides the identifier of the selected SMF in the HPLMN to the selected SMF in the VPLMN.

In roaming with LBO, the AMF selects a SMF in the VPLMN. In this case, when handling a PDU Session establishment request, the SMF in the VPLMN may reject the N11 message (related with a PDU Session establishment request) with a proper N11 cause. This triggers the AMF to select both a new SMF in the VPLMN and a SMF in the HPLMN in order to handle the PDU Session using home routed roaming.

5.6.4 Single PDU Session with multiple PDU Session Anchors

5.6.4.1 General

In order to support selective traffic routing to the DN or to support SSC mode 3 as defined in clause 5.6.9.2.3, the SMF may control the data path of a PDU Session so that the PDU Session may simultaneously correspond to multiple N6 interfaces. The UPF that terminates each of these interfaces is said to support PDU Session Anchor functionality. Each PDU Session Anchor supporting a PDU Session provides a different access to the same DN. Further, the PDU Session Anchor assigned at the establishment of a PDU Session is associated with the SSC mode of the PDU Session and the additional PDU Session Anchor(s) assigned within the same PDU Session e.g. for selective traffic routing to the DN are independent of the SSC mode of the PDU Session.

NOTE: Selective traffic routing to the DN supports, for example, deployments where some selected traffic is forwarded on an N6 interface to the DN that is "close" to the AN serving the UE.

This may correspond to

- The Usage of UL Classifier functionality for a PDU Session defined in clause 5.6.4.2.
- The Usage of an IPv6 multi-homing for a PDU Session defined in clause 5.6.4.3.

5.6.4.2 Usage of an UL Classifier for a PDU Session

In case of PDU Sessions of type IPv4 or IPv6 or Ethernet, the SMF may decide to insert in the data path of a PDU Session an "UL CL" (Uplink classifier). The UL CL is a functionality supported by an UPF that aims at diverting (locally) some traffic matching traffic filters provided by the SMF. The insertion and removal of an UL CL is decided by the SMF and controlled by the SMF using generic N4 and UPF capabilities. The SMF may decide to insert in the data path of a PDU Session a UPF supporting the UL CL functionality during or after the PDU Session establishment, or to remove from the data path of a PDU Session a UPF supporting the UL CL functionality after the PDU Session establishment. The SMF may include more than one UPF supporting the UL CL functionality in the data path of a PDU Session.

The UE is unaware of the traffic diversion by the UL CL, and does not involve in both the insertion and the removal of UL CL. In case of a PDU Session of IPv4 or IPv6 type, the UE associates the PDU Session with either a single IPv4 address or a single IPv6 Prefix allocated by the network.

When an UL CL functionality has been inserted in the data path of a PDU Session, there are multiple PDU Session Anchors for this PDU Session. These PDU Session Anchors provide different access to the same DN. In case of a PDU Session of IPv4 or IPv6 type, only one PDU Session Anchor is IP anchor point for the IPv4 address / IPv6 prefix of the PDU Session provided to the UE.

NOTE 0: The mechanisms for packet forwarding on the N6 reference point between the PDU Session Anchor providing local access and the DN are outside the scope of this specification.

The UL CL provides forwarding of UL traffic towards different PDU Session Anchors and merge of DL traffic to the UE i.e. merging the traffic from the different PDU Session Anchors on the link towards the UE. This is based on traffic detection and traffic forwarding rules provided by the SMF.

The UL CL applies filtering rules (e.g. to examine the destination IP address/Prefix of UL IP packets sent by the UE) and determines how the packet should be routed. The UPF supporting an UL CL may also be controlled by the SMF to support traffic measurement for charging, traffic replication for LI and bit rate enforcement (per PDU Session AMBR).

NOTE 1: The UPF supporting an UL CL may also support a PDU Session Anchor for connectivity to the local access to the data network (including e.g. support of tunnelling or NAT on N6). This is controlled by the SMF.

Additional UL CLs (and thus additional PDU Session Anchors) can be inserted in the data path of a PDU Session to create new data paths for the same PDU Session. The way to organize the data path of all UL CLs in a PDU Session is up to operator configuration and SMF logic and there is only one UPF supporting UL CL connecting to the (R)AN via N3 interface.

The insertion of an ULCL in the data path of a PDU Session is depicted in Figure 5.6.4.2-1.

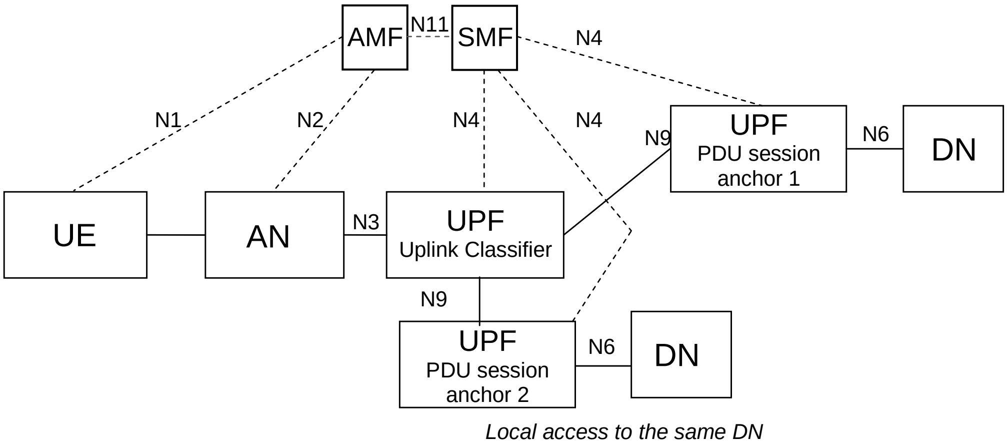


Figure 5.6.4.2-1 User plane Architecture for the Uplink Classifier

NOTE 2: It is possible for a given UPF to support both the UL CL and the PDU Session Anchor functionalities.

5.6.4.3 Usage of IPv6 multi-homing for a PDU Session

A PDU Session may be associated with multiple IPv6 prefixes. This is referred to as multi-homed PDU Session. The multi-homed PDU Session provides access to the Data Network via more than one PDU Session Anchor. The different user plane paths leading to the different PDU Session Anchors branch out at a "common" UPF referred to as a UPF supporting "Branching Point" functionality. The Branching Point provides forwarding of UL traffic towards the different PDU Session Anchors and merge of DL traffic to the UE i.e. merging the traffic from the different PDU Session Anchors on the link towards the UE.

The UPF supporting a Branching Point functionality may also be controlled by the SMF to support traffic measurement for charging, traffic replication for LI and bit rate enforcement (per PDU Session AMBR). The insertion and removal of a UPF supporting Branching Point is decided by the SMF and controlled by the SMF using generic N4 and UPF capabilities. The SMF may decide to insert in the data path of a PDU Session a UPF supporting the Branching Point functionality during or after the PDU Session establishment, or to remove from the data path of a PDU Session a UPF supporting the Branching Point functionality after the PDU Session establishment.

Multi homing of a PDU Session applies only for PDU Sessions of IPv6 type. The request of PDU Session type "IP" or "IPv6" implies the support of multi-homed PDU Session for IPv6 in the UE.

The use of multiple IPv6 prefixes in a PDU Session is characterised by the following:

- The UPF supporting a Branching Point functionality is configured by the SMF to spread the UL traffic between the IP anchors based on the Source Prefix of the PDU (which may be selected by the UE based on routing information and preferences received from the network).

- IETF RFC 4191 [8] is used to configure routing information and preferences into the UE to influence the selection of the source Prefix.

NOTE 1: This corresponds to Scenario 1 defined in IETF RFC 7157 [7] "IPv6 Multi-homing without Network Address Translation". This allows to make the Branching Point unaware of the routing tables in the Data Network and to keep the first hop router function in the IP anchors.

- The multi-homed PDU Session may be used to support make-before-break service continuity to support SSC mode 3. This is illustrated in Figure 5.6.4.3-1.

- The multi-homed PDU Session may also be used to support cases where UE needs to access both a local service (e.g. local server) and a central service (e.g. the internet), illustrated in Figure 5.6.4.3-2.

- The UE shall use the method specified in TS 23.502 [3], clause 4.3.5.3, to determine if a multi-homed PDU Session is used to support the service continuity case shown in Figure 5.6.4.3-1, or if it is used to support the local access to DN case shown in Figure 5.6.4.3-2.

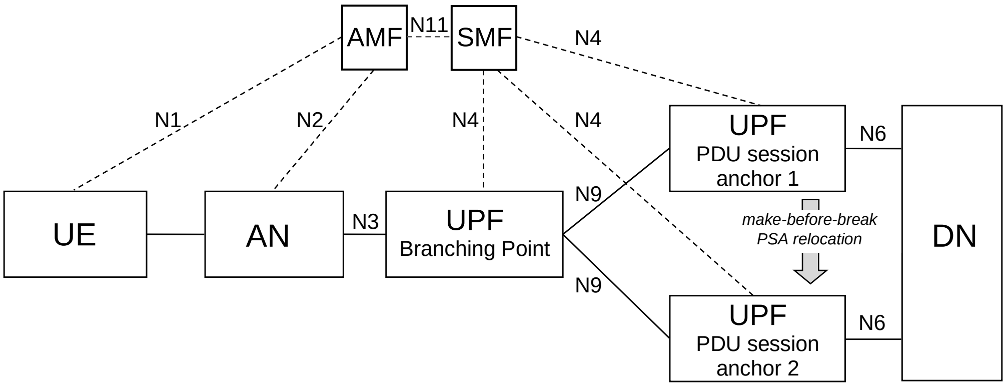


Figure 5.6.4.3-1: Multi-homed PDU Session: service continuity case

NOTE 2: It is possible for a given UPF to support both the Branching Point and the PDU Session Anchor functionalities.

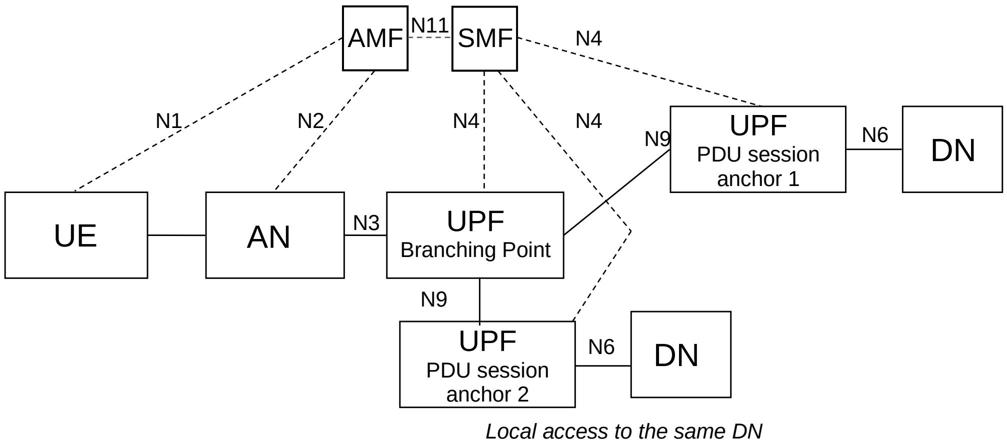


Figure 5.6.4.3-2: Multi-homed PDU Session: local access to same DN

NOTE 3: It is possible for a given UPF to support both the Branching Point and the PDU Session Anchor functionalities.

5.6.5 Support for local area data network

The access to a DN via a PDU Session for a LADN is only available in a specific LADN service area. A LADN service area is a set of Tracking Areas.

The LADN Information (i.e. LADN service area information and LADN DNN) is configured in the AMF on a per DN basis, i.e. for different UEs accessing the same LADN, the configured LADN service area is the same regardless of other factors (e.g. UE's Registration Area). The SMF subscribes to AMF about "UE location change notification" corresponding to a LADN DNN. The AMF tracks UE's location and notifies the SMF about the relationship between UE location and a LADN service area (i.e. IN, OUT, UNKNOWN).

The LADN information is provided by AMF to the UE during the registration procedure or UE Configuration Update procedure. For each LADN DNN, the corresponding LADN service area information includes a set of Tracking Areas that belong to the current Registration Area of the UE (i.e. the intersection of the LADN service area and the current Registration Area). The AMF does not create Registration Area based on the availability of LADNs.

NOTE 1: It is thus possible that the LADN service area information sent by the AMF to the UE contains only a sub-set of the full LADN service area as the LADN service area can contain TA(s) outside of the registration area of the UE

When the UE performs a successful (Re)registration procedure, the AMF shall provide to the UE, based on local configuration information (e.g. via OAM) about LADN Information, UE location, UE subscription information received from the UDM about DNNs that is subscribed as LADN, the LADN Information for the LADNs available to the UE in that RA in the Registration Accept message. During the subsequent Registration Update procedure, if the network does not provides LADN information, the UE deletes the LADN information.

When the LADN Information for the UE in the 5GC is changed, the AMF shall update LADN Information to the UE through UE Configuration Update/Registration procedure as described in clause 4.2.4/4.2.2.2.2 in TS 23.502 [3].

Editor's note: How UE knows whether a DNN is a LADN DNN is FFS.

Based on the LADN Information in the UE, the UE takes actions as follows:

a) When the UE is out of a LADN service area, the UE:

  - shall not request to activate UP connection of a PDU Session for this LADN DNN;
  - shall not establish/modify a PDU Session for this LADN DNN;
  - needs not release any existing PDU Session for this LADN DNN unless UE receives explicit PDU Session release request from network.

b) When the UE is in a LADN service area, the UE:

- may request a PDU Session establishment/modification for this LADN DNN;
- may request to activate UP connection of the existing PDU Session for this LADN DNN.

The SMF subscribes to "UE location change notification" as described in clause 5.6.11. In the network deployment where a UE may leave or enter an LADN service area without any notification to the 5GC in CM-CONNECTED state, the AMF needs to initiate the Location reporting as described in clause 5.6.11 to track the correct location of the UE related to the LADN service area in CM-CONNECTED state.

Based on the notification whether the UE is in or out of the LADN service area notified by AMF (i.e. IN, OUT, UNKNOWN), the SMF takes actions as follows based on operator's policy:

a) When SMF is informed that the UE moves out of the LADN service area, the SMF shall:

- release the PDU Session immediately; or
- deactivate the user plane connection for the PDU Session with maintaining the PDU Session and ensure the Downlink Data Notification is disabled The SMF may release the PDU Session later.

b) When SMF is informed that the UE moves in the LADN service area, the SMF shall:

- ensure that Downlink Data Notification is enabled.
- trigger the Network triggered Service Request procedure for a LADN PDU Session to active the UP connection when the SMF receives downlink data or Data Notification from UPF.

c) When the SMF is informed that the UE location is unknown, the SMF may:

- ensure that Downlink Data Notification is enabled.
- trigger the Network triggered Service Request procedure for a LADN PDU Session to active the UP connection when the SMF receives downlink data or Data Notification from UPF.

In this release, LADNs apply only to 3GPP accesses.

5.6.6 Secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session

At the establishment of a PDU Session to a DN:

- The DN-specific identity (TS 33.501 [29]) of a UE may be authenticated/authorized by the DN.

NOTE 1: the DN-AAA server may belong to the 5GC or to the DN.

- If the UE provides authentication/authorization information corresponding to a DN-specific identity during the establishment of the PDU Session, and the SMF determines that authentication/authorization of the PDU Session establishment is required based on the SMF policy associated with the DN, the SMF passes the authentication/authorization information of the UE to the DN-AAA server via the UPF if the DN-AAA server is located in the DN. If the SMF determines that authentication of the PDU Session establishment is required but the UE has not provided authentication/authorization information, then the SMF rejects the PDU Session establishment.

NOTE 2: If the DN-AAA server is located in the 5GC and reachable directly, then the SMF may communicate with it directly without involving the UPF.

- The DN-AAA server may authenticate/authorize the PDU Session establishment.
- When DN-AAA server authorizes the PDU Session establishment, it may send DN authorization data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:
  - a reference to a locally configured authorization data in the SMF
  - a DN profile index to retrieve the SM or QoS policy from the PCF

- a list of allowed MAC addresses for the PDU Session ; this may apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2
- PDU Session AMBR

SMF policies may require DN authorization without DN authentication. In that case, when contacting the DN-AAA server for authorization, the SMF provides the Public UE Identifier (PUI) of the UE if available.

Such DN authentication and/or authorization takes place for the purpose of PDU Session authorization in addition to:

- The 5GC access authentication handled by AMF and described in clause 5.2.
- The PDU Session authorization enforced by SMF with regard to subscription data retrieved from UDM.

Based on local policies the SMF may initiate DN authentication and/or authorization at PDU Session establishment.

The UE provides information required to support user authentication by the DN over NAS SM.

NOTE 3: The way for the UE to acquire such information is not defined.

When SMF adds an PDU Session Anchor (such as defined in clause 5.6.4) to a PDU Session DN authentication and / or authorization is not carried out, but SMF policies may require SMF to notify the DN when a new prefix or address has been added to or removed from a PDU Session.

Indication of PDU Session establishment rejection is transferred by SMF to the UE via NAS SM.

If the DN-AAA sends DN authorization data for the established PDU Session to the SMF and dynamic PCC applies to the PDU Session, the SMF requests the PCF to validate the DN authorization data for the established PDU Session. If the DN-AAA does not send DN authorization data for the established PDU Session, the SMF may use locally configured information.

At any time, a DN-AAA server may revoke the authorization for a PDU Session or update DN authorization data for a PDU Session. According to the request from DN-AAA server, the SMF may release or update the PDU Session.

5.6.7 Application Function influence on traffic routing

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

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

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

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

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

The AF requests are sent to the PCF via N5 (in case of requests regarding on-going PDU Sessions of individual UEs, for an AF allowed to interact directly with the 5GC NFs) or via the NEF. Requests that target multiple UE(s) are sent via the NEF and may target multiple PCF(s). The PCF(s) transform(s) the AF requests into policies that apply to PDU Sessions. When the AF has subscribed to UP path management event notifications from SMF(s), such notifications are sent either directly to the AF or via an NEF (without involving the PCF)

Such AF requests may contain at least:

1) Information to identify the traffic. The traffic can be identified in the AF request by
   - Either a DNN and possibly slicing information (S-NSSAI) or an AF-Service-Identifier

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

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

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

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

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

2) Information about the N6 traffic routing requirements for traffic identified as defined in 1). This is provided implicitly by reference, in the form of a list of routing profile IDs, corresponding each to a DNAI, if the details of the N6 routing requirements are preconfigured in the 5GC. Otherwise, it is provided explicitly by value, in the form of a list of DNAIs and associated N6 traffic routing information. Based on the information about the N6 traffic routing requirements the PCF determines traffic steering policy IDs sent to SMF that each corresponds to a steering behaviour which is preconfigured on the SMF or UPF.

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

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

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

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

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

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

- any UE the request applies to any UE accessing the combination of DNN, S-NSSAI and DNAI(s).

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

  Otherwise the request shall apply to any existing or future PDU Session that matches the parameters in the AF request.

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

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

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

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

5) Indication that for the traffic related with an application, no DNAI change shall take place once selected for this application;

NOTE 3: This could result in the traffic for this application being handled by a less optimum DNAI /application instance over time.

6) Temporal validity condition.

NOTE 4: This allows to provide a time interval or duration during which the AF request is valid.

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

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

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

When the AF request is for influencing SMF routing decisions, the spatial validity condition indicates where the UE(s) are to be when the traffic routing applies.

When the AF request is for subscription to notifications about UP path management events, the spatial validity condition indicates where the UE(s) are to be when the subscription applies.

8) Type of notifications regarding UP path management events.

The AF subscription can be for early notification and/or late notification. In case of a subscription for early notification, the SMF sends the notification before executing the UPF (re)selection. In case of a subscription for late notification, the SMF sends the notification when the UPF (re)selection has completed.

9) An AF transaction identifier referring to the AF request. This allows the AF to update or remove the AF request to influence traffic routing.

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

The AF may subscribe to notifications about UP path management events, e.g., when the request becomes active or inactive, or when a change of DNAI occurs for the PDU Session. The corresponding notification about a change from source DNAI (or no DNAI) to target DNAI (or no DNAI) sent by the SMF to the AF includes type of notification (i.e. early notification or late notification), the Identity of the source and/or target DNAI, the IP address/prefix of the UE, the SUPI and the N6 routing information related to the 5GC UP. The UE identity information and the N6 routing information related to the 5GC UP are optional if the PDU Session type is IP. The nature of the N6 traffic routing information related to the 5GC UP is described in clause 5.6.10.

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

The PCF, based on information received from the AF, operator's policy, etc. authorizes the request received from the application function and determines the traffic steering policy. The traffic steering policy indicates the list of suitable traffic steering policy IDs configured in SMF and if the N6 routing information associated to the application is explicitly provided by the AF, the N6 routing information. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN.

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

The PCF acknowledges the request to the AF or to the NEF.

For PDU Session that corresponds to the AF request, the PCF provides the SMF with PCC rules that are generated based on the AF request and taking into account UE location presence in area of interest. The PCC rules may contain information to identify the traffic to be routed and/or information about the DNAI(s) towards which the traffic routing should apply and/or a list of traffic steering policy IDs and/or information on AF subscription to SMF events. If the N6 routing information associated to the application is explicitly provided in the AF request, the PCF also provides the N6 routing information to the SMF as part of PCC rules. This is done by providing policies at PDU session set-up or by initiating a PDU Session Modification procedure. When initiating a PDU Session set-up or PDU Session Modification procedure, the PCF considers the latest known UE location to determine the PCC rules provided to the SMF. The PCF evaluates the temporal validity condition of the AF request and informs the SMF to activate or deactivate the corresponding PCC rules according to the evaluation result. When policies specific to the PDU Session and policies general to multiple PDU Sessions exist, the PCF gives precedence to the PDU Session specific policies over the general policies.

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

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

- (re)select UPF(s) for PDU Sessions. The SMF is responsible for handling the mapping between the UE location (TAI / Cell-Id) and DNAI(s) associated with UPF and applications and of the selection of the UPF(s) that serve a PDU Session. This is described in clause 6.3.3.
- activate mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL). Such mechanisms are defined in clause 5.6.4. This may include providing the UPF with traffic forwarding (e.g. break-out) rules and the associated N6 routing information if the N6 routing information is part of the PCC rules.
- inform the Application Function of the (re)selection of the UP path (change of DNAI).

5.6.8 Selective activation and deactivation of UP connection of existing PDU Session

This clause applies to the case when a UE has established multiple PDU Sessions. The activation of a UP connection of an existing PDU Session causes the activation of its UE-CN User Plane connection (i.e. data radio bearer and N3 tunnel).

For the UE in the CM-IDLE state in 3GPP access, either UE or Network-Triggered Service Request procedure may support independent activation of UP connection of existing PDU Session. For the UE in the CM-IDLE state in non-3GPP access, UE-Triggered Service Request procedure allows the re-activation of UP connection of existing PDU Sessions, and may support independent activation of UP connection of existing PDU session.

A UE in the CM-CONNECTED state invokes a Service Request (see TS 23.502 [3] clause 4.2.3.3) procedure to request the independent activation of the UP connection of existing PDU Sessions.

Network Triggered re-activation of UP connection of existing PDU Sessions is handled as follows:

- If the UE CM state in the AMF is already CM-CONNECTED on the access (3GPP, non-3GPP) associated to the PDU Session in the SMF, the network may re-activate the UP connection of a PDU Session using a Network Initiated Service Request procedure.

  Otherwise:

- If the UE is registered in both 3GPP and non-3GPP accesses and the UE CM state in the AMF is CM-IDLE in non-3GPP access, the UE can be paged or notified through the 3GPP access for a PDU Session associated in the SMF (i.e. last routed) to the 3GPP access or to the non-3GPP access:
  - If the UE CM state in the AMF is CM-IDLE in 3GPP access, the paging message may include the access type associated with the PDU Session in the SMF. The UE, upon reception of the paging message containing an access type, shall reply to the 5GC via the 3GPP access using the NAS Service Request message, which shall contain the list of PDU Sessions associated with the received access type and whose UP connections can be re-activated over 3GPP (i.e. the list does not contain the PDU Sessions whose UP connections cannot be re-activated on 3GPP based on UE policies). If the PDU Session for which the UE has been paged is in the

list of the PDU Sessions provided in the NAS Service Request, the 5GC shall re-activate the PDU Session UP connection over 3GPP access;

- If the UE CM state in the AMF is CM-CONNECTED in 3GPP access, the notification message may include the PDU Session ID. The UE, upon reception of the notification message, shall reply to the 5GC via the 3GPP access using the NAS Service Request message, which shall contain an indication on whether the PDU Session UP connection can be re-activated over 3GPP.

NOTE: A UE that is in a coverage of a non-3GPP access and has PDU Session(s) that are associated in the UE (i.e. last routed) to non-3GPP access, is assumed to attempt to connect to it without the need to be paged.

- If the UE is registered in both 3GPP and non-3GPP accesses served by the same AMF and the UE CM state in the AMF is CM-IDLE in 3GPP access and is in CM-CONNECTED in non 3GPP access, the UE can be notified through the non-3GPP for a PDU Session associated in the SMF (i.e. last routed) to the 3GPP access. The notification message includes the PDU Session ID. Upon reception of the notification message, when 3GPP access is available, the UE shall reply to the 5GC via the 3GPP access using the NAS Service Request message.

The deactivation of the UP connection of an existing PDU Session causes the corresponding data radio bearer and N3 tunnel to be deactivated. The UP connection of different PDU Sessions can be deactivated independently when a UE is in CM-CONNECTED state in 3GPP access or non-3GPP access.

5.6.9 Session and Service Continuity

5.6.9.1 General

The support for session and service continuity in 5G System architecture enables to address the various continuity requirements of different applications/services for the UE. The 5G System supports different session and service continuity (SSC) modes defined in this clause. The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session. The following three modes are specified with further details provided in the next clause:

- With SSC mode 1, the network preserves the connectivity service provided to the UE. For the case of PDU Session of IPv4 or IPv6 type, the IP address is preserved.

- With SSC mode 2, the network may release the connectivity service delivered to the UE and release the corresponding PDU Session. For the case of IPv4 or IPv6 type, the network may release IP address(es) that had been allocated to the UE.

- With SSC mode 3, changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. For the case of IPv4 or IPv6 type, the IP address is not preserved in this mode when the PDU Session Anchor changes.

NOTE: In this Release, the addition/removal procedure of additional PDU Session Anchor in a PDU Session for local access to a DN is independent from the SSC mode of the PDU Session.

5.6.9.2 SSC mode

5.6.9.2.1 SSC Mode 1

For a PDU Session of SSC mode 1, the UPF acting as PDU Session Anchor at the establishment of the PDU Session is maintained regardless of the access technology (e.g. Access Type and cells) a UE is successively using to access the network.

In case of a PDU Session of IPv4 or IPv6 type, IP continuity is supported regardless of UE mobility events.

In this release, when IPv6 multihoming or UL CL applies to a PDU Session of in SSC mode 1, and the network allocates (based on local policies) additional PDU Session Anchors to such a PDU Session, these additional PDU Session Anchors may be released or allocated, and the UE does not expect that the additional IPv6 prefix is maintained during the lifetime of PDU Session.

SSC mode 1 may apply to any PDU Session type and to any access type.

5.6.9.2.2 SSC Mode 2

If a PDU Session of SSC mode 2 has a single PDU Session Anchor, the network may trigger the release of the PDU Session and instruct the UE to establish a new PDU Session to the same data network immediately. The trigger condition depends on operator policy e.g. request from Application Function, based on load status, etc. At establishment of the new PDU Session, a new UPF acting as PDU Session Anchor can be selected.

Otherwise, if a PDU Session of SSC mode 2 has multiple PDU Session Anchors (i.e., in case of multi-homed PDU Sessions or in case UL CL applies to a PDU Session of SSC mode 2), the additional PDU Session Anchors may be released or allocated.

SSC mode 2 may apply to any PDU Session type and to any access type.

NOTE: In UL CL mode, the UE is not involved in PDU Session Anchor re-allocation, so that the existence of multiple PDU Session Anchors is not visible to the UE.

5.6.9.2.3 SSC Mode 3

For PDU Session of SSC mode 3, the network allows the establishment of UE connectivity via a new PDU Session Anchor to the same data network before connectivity between the UE and the previous PDU Session Anchor is released. When trigger conditions apply, the network decides whether to select a PDU Session Anchor UPF suitable for the UE's new conditions (e.g. point of attachment to the network).

SSC mode 3 may apply to any PDU Session type and to any access type.

In the case of a PDU Session of IPv4 or IPv6 type, during the procedure of change of PDU Session Anchor, the following applies:

a. The new IP prefix anchored on the new PDU Session Anchor may be allocated within the same PDU Session (relying on IPv6 multi-homing specified in clause 5.6.4.3), or

b. The new IP address/prefix may be allocated within a new PDU Session that the UE is triggered to establish.

After the new IP address/prefix has been allocated, the old IP address/prefix is maintained during some time indicated to the UE and then released.

If a PDU Session of SSC mode 3 has multiple PDU Session Anchors (i.e., in case of multi-homed PDU Sessions or in case UL CL applies to a PDU Session of SSC mode 3), the additional PDU Session Anchors may be released or allocated.

5.6.9.3 SSC mode selection

The SSC mode selection policy shall be used to determine the type of session and service continuity mode associated with an application or group of applications for the UE.

It shall be possible for the operator to provision the UE with SSC mode selection policy. This policy includes one or more SSC mode selection policy rules which can be used by the UE to determine the type of SSC mode associated with an application or group of applications. The policy may include a default SSC mode selection policy rule that matches all applications of the UE.

When an application requests data transmission (e.g. opens a network socket) and the application itself does not specify the required SSC mode, the UE determines the SSC mode associated with this application by using the SSC mode selection policy; . In addition, the following behaviour applies for the UE and network:

a) If the UE has already an established PDU Session that matches the SSC mode associated with the application, then the UE routes the data of the application within this PDU Session unless other conditions in the UE do not permit the use of this PDU Session. Otherwise, the UE requests the establishment of a new PDU Session with an SSC mode that matches the SSC mode associated with the application.

b) The SSC mode associated with the application is either the SSC mode included in a non-default SSCMSP rule that matches the application or the SSC mode included in the default SSC mode selection policy rule, if present. If the SSCMSP does not include a default SSCMP rule and no other rule matches the application, then the UE requests the PDU Session without providing the SSC mode. In this case, the network determines the SSC mode of the PDU Session.

The SSC mode selection policy rules provided to the UE can be updated by the operator.

The SMF receives from the UDM the list of supported SSC modes and the default SSC mode per DNN per S-NSSAI as part of the subscription information.

If a UE provide an SSC mode when requesting a new PDU Session, the SMF selects the SSC mode by either accepting the requested SSC mode or modifying the requested SSC mode or rejecting the PDU session establishment request with the cause value back to UE based on subscription and/or local configuration.

If a UE does not provide an SSC mode when requesting a new PDU Session, then the SMF selects the default SSC mode for the data network listed in the subscription or applies local configuration to select the SSC mode.

SSC mode 1 shall be assigned to the PDU Session when static IP address/prefix is allocated to the PDU Session based on the static IP address/prefix subscription for the DNN and S-NSSAI. The SMF shall inform the UE of the selected SSC mode for a PDU Session.

5.6.10 Specific aspects of different PDU Session types

5.6.10.1 Support of IP PDU Session type

The IP address allocation is defined in clause 5.8.1

5.6.10.2 Support of Ethernet PDU Session type

For a PDU Session set up with the Ethernet PDU Session type, the SMF and the UPF acting as PDU Session Anchor can support specific behaviours related with the fact the PDU Session carries Ethernet frames. Based on operator configuration, the SMF may request the UPF acting as the PDU Session Anchor to proxy ARP/IPv6 Neighbour Solicitation or to redirect the ARP traffic from the UPF to the SMF.

Ethernet Preamble and Start of Frame delimiter are not sent over 5GS:

- For UL traffic the UE strips the preamble and frame check sequence (FCS) from the Ethernet frame.
- For DL traffic the PDU Session Anchor strips the preamble and frame check sequence (FCS) from the Ethernet frame.

Neither a MAC nor an IP address is allocated by the 5GC to the UE for this PDU Session. The UPF shall store the MAC addresses, received from the UE, and associate those with the appropriate PDU Session.

NOTE 1: The UE may operate in bridge mode with regard to a LAN it is connecting to the 5GS, thus different MAC addresses may be used as source address of different frames sent UL over a single PDU Session (and destination MAC address of different frames sent DL over the same PDU Session)

NOTE 2: Entities on the LAN connected to the 5GS by the UE may have an IP address allocated by the DN but the IP layer is considered as an application layer which is not part of the Ethernet PDU Session.

NOTE 3: In this release, only the UE connected to the 5GS is authenticated, not the devices behind such UE

Different Frames exchanged on a PDU Session of Ethernet type may be served with different QoS over the 5GS. Thus, the SMF may provide to the UPF Ethernet Packet Filter Set and forwarding rule(s) based on the Ethernet frame structure and UE MAC address(es). The UPF detects and forwards Ethernet frames based on the Ethernet Packet Filter Set and forwarding rule(s) received from the SMF. This is further defined in clauses 5.7 and 5.8.2.

When a PDU Session of Ethernet PDU type is authorized by a DN as described in clause 5.6.6, the DN-AAA server may, as part of authorization data, provide the SMF with a list of allowed MAC addresses for this PDU Session; this list is limited to a maximum of 16 MAC addresses. When such a list has been provided for a PDU Session, the SMF sets corresponding filtering rules in the UPF(s) acting as PDU Session Anchor for the PDU Session and the UPF discards any UL traffic that does not contains one of these MAC addresses as a source address.

5.6.10.3 Support of Unstructured PDU Session type

Different Point-to-Point (PtP) tunnelling techniques may be used to deliver Unstructured PDU Session type data to the destination (e.g. application server) in the Data Network via N6.

Point-to-point tunnelling based on UDP/IP encapsulation as described below may be used. Other techniques may be supported. Regardless of addressing scheme used from the UPF to the DN, the UPF shall be able to map the address used between the UPF and the DN to the PDU Session.

When Point-to-Point tunnelling based on UDP/IPv6 is used, the following considerations apply:

- IPv6 prefix allocation for PDU Sessions are performed locally by the (H-)SMF without involving the UE.
- The UPF(s) acts as a transparent forwarding node for the payload between the UE and the destination in the DN.
- For uplink, the UPF forwards the received Unstructured PDU Session type data to the destination in the data network over the N6 PtP tunnel using UDP/IPv6 encapsulation.
- For downlink, the destination in the data network sends the Unstructured PDU Session type data using UDP/IPv6 encapsulation with the IPv6 address of the PDU Session and the 3GPP defined UDP port for Unstructured PDU Session type data. The UPF acting as PDU Session Anchor decapsulates the received data (i.e. removes the UDP/IPv6 headers) and forwards the data identified by the IPv6 prefix of the PDU Session for delivery to the UE.
- The (H-)SMF performs the IPv6 related operations but the IPv6 prefix is not provided to the UE, i.e. Router Advertisements and DHCPv6 are not performed. The SMF assigns an IPv6 Interface Identifier for the PDU Session. The allocated IPv6 prefix identifies the PDU Session of the UE.

In this release of the specification there is support for maximum one 5G QoS Flow per PDU Session of Type Unstructured.

5.6.11 UE Location change notification

When a PDU Session is established or modified, or when the user plane path has been changed (e.g. UPF re-allocation/addition/removal), SMF may determine an area of interest, e.g. based on UPF Service Area, etc., and subscribe to AMF notifications. When the AMF detects that the UE has moved in or out of that area, it needs to notify SMF of the UE's new location.

For 3GPP access, the area of interest is defined by a list of Tracking Areas.

SMF subscribes to "UE mobility event Notification" service provided by AMF. During subscription, SMF provides the area of interest to AMF. The AMF sends UE's new location to SMF when AMF detects that the UE has moved in or out of that area. Upon reception of new UE location notification from AMF, the SMF determines how to deal with the PDU Session, e.g. reallocate UPF.

If the AMF is subscribed to an area of interest by the SMF, the AMF may construct an area of interest (e.g. a list of TAIs) based on SMF's subscribed area of interest and provide this area of interest information to NG-RAN via the location reporting procedure specified in TS 23.502 [3]. If the NG-RAN detects the UE moves out of or into the area of interest provided by the AMF, NG-RAN notifies the latest UE location to AMF.

In the case of LADN, the SMF only provides the LADN DNN to the AMF to subscribe to notifications when the UE enters or leaves the LADN service area. The AMF notifies the SMF when the AMF detects that the UE has moved in or out of an area where the LADN is available. Upon reception of a notification from the AMF that the UE has moved in or out of an LADN area, the SMF determines how to deal with the PDU Session, e.g. release the PDU Session, deactivate UP connection for the PDU Session, etc. The AMF may send the UE location to the SMF along with the notification, e.g. for UPF selection.

The subscription may be maintained during the life of PDU Session, regardless of the UP activation state of PDU Session (i.e. whether UP connection of the PDU Session is activated or not). When the AMF is changed, the subscription of mobility event is transferred from the old AMF to the new AMF and the new AMF notifies the SMF with the current status related to the subscription of mobility event.

SMF may determine a new area of interest, and send a new subscription to the AMF with the new area of interest.

SMF unsubscribes to "UE mobility event Notification" service when PDU Session is released.

The UE location change notification may also be subscribed by other NF.

5.7 QoS model

5.7.1 General Overview

5.7.1.1 QoS Flow

The 5G QoS model is based on QoS Flows. The 5G QoS model supports both QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require guaranteed flow bit rate (non-GBR QoS Flows). The 5G QoS model also supports reflective QoS (see clause 5.7.5).

The QoS Flow is the finest granularity of QoS differentiation in the PDU Session. A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System. User Plane traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment (e.g. scheduling, admission threshold). The QFI is carried in an encapsulation header on N3 (and N9) i.e. without any changes to the e2e packet header. QFI shall be used for all PDU Session Types. The QFI shall be unique within a PDU Session. The QFI may be dynamically assigned or may be equal to the 5QI (see clause 5.7.2.1).

NOTE 1: Policing of User Plane traffic (e.g. MFBR enforcement) is not regarded as QoS differentiation and is done by UPFs on an SDF level granularity.

Within the 5GS, a QoS Flow is controlled by the SMF and may be preconfigured, or established via the PDU Session establishment procedure (see TS 23.502 [3], clause 4.3.2), or the PDU Session Modification procedures (see TS 23.502 [3].

Any QoS Flow is characterised by:

- A QoS profile provided by the SMF to the AN via the AMF over the N2 reference point or preconfigured in the AN;
- One or more QoS rule(s) which can be provided by the SMF to the UE via the AMF over the N1 reference point and/or derived by the UE by applying reflective QoS control; and
- One or more SDF templates provided by the SMF to the UPF.

Within the 5GS, a QoS Flow associated with the default QoS rule is required to be established for a PDU Session and remains established throughout the lifetime of the PDU Session. This QoS Flow should be a Non-GBR QoS Flow.

NOTE 2: The above QoS Flow provides the UE with connectivity throughout the lifetime of the PDU Session. Possible interworking with EPS motivates the restriction of this QoS Flow to be of type Non-GBR.

5.7.1.2 QoS Profile

A QoS Flow may either be 'GBR' or 'Non-GBR' depending on its QoS profile. The QoS profile of a QoS Flow contains QoS parameters as described below (details of QoS parameters are described in clause 5.7.2):

- For each QoS Flow, the QoS profile shall include QoS parameters:
  - A 5G QoS Identifier (5QI); and.
  - An Allocation and Retention Priority (ARP).
- For each Non-GBR QoS Flow, the QoS profile may also include the QoS parameter:
  - Reflective QoS Attribute (RQA).
- For each GBR QoS Flow, the QoS profile shall also include the QoS parameters:
  - Guaranteed Flow Bit Rate (GFBR) - UL and DL; and
  - Maximum Flow Bit Rate (MFBR) - UL and DL; and
- In case of a GBR QoS Flow only, the QoS parameters may also include:
  - Notification control.

- Maximum Packet Loss Rate - UL and DL.

NOTE: In this Release, the Maximum Packet Loss Rate (UL, DL) is only provided for a GBR QoS flow belonging to voice media.

Each QoS profile has one corresponding QoS Flow identifier (QFI) which is not included in the QoS profile itself.

The 5QI value may indicate that a QoS Flow have signalled QoS characteristics, and if so, the QoS characteristics are included in the QoS profile. Details of QoS characteristics are described in clause 5.7.3.

5.7.1.3 Control of QoS Flows

The following options are supported to control QoS Flows:

1) For non-GBR QoS Flows, and when standardized 5QIs or pre-configured 5QIs are used, the 5QI value can be used as the QFI of the QoS Flow.

   (a) A default ARP shall be pre-configured in the AN; or

NOTE 1: The above 1a option is intended to be used for non-3GPP ANs (e.g. Fixed AN) scenarios when there is no need for any N1 signalling including PDU Session Establishment, nor any N2 signalling.

   (b) The ARP and the QFI shall be sent to RAN over N2 at PDU Session Establishment or at PDU Session Modification and when NG-RAN is used every time the User Plane of the PDU Session is activated; and

2) For all other cases (including GBR and non-GBR QoS Flows), a dynamically assigned QFI shall be used. The 5QI value may be a standardized, pre-configured or dynamically assigned. The QoS profile and the QFI of a QoS Flow shall be provided to the (R)AN over N2 at PDU Session Establishment/Modification and when NG-RAN is used every time the User Plane of the PDU Session is activated.

NOTE 2: The options 1b and 2 are intended to be used for 3GPP ANs.

NOTE 3: Pre-configured 5QI values cannot be used when the UE is roaming.

5.7.1.4 QoS Rules

The UE performs the classification and marking of UL User plane traffic, i.e. the association of UL traffic to QoS Flows, based on QoS rules. These QoS rules may be explicitly provided to the UE (using the PDU Session Establishment/Modification procedure), pre-configured in the UE or implicitly derived by UE by applying reflective QoS (see clause 5.7.5). A QoS rule contains a QoS rule identifier which is unique within the PDU Session, the QFI of the associated QoS Flow and except for the default QoS rule (see below) a Packet Filter Set (see clause 5.7.6) for UL and optionally for DL and a precedence value (see clause 5.7.1.9). Additionally, for a dynamically assigned QFI, the QoS rule contains the QoS parameters relevant to the UE (e.g. 5QI, GBR and MBR and the Averaging Window). There can be more than one QoS rule associated with the same QoS Flow (i.e. with the same QFI).

A default QoS rule is required for every PDU Session and associated with the QoS Flow of the default QoS rule. The default QoS rule is the only QoS rule of a PDU Session that may contain no Packet Filter Set in which case, the highest precedence value shall be used. If the default QoS rule does not contain a Packet Filter Set, the default QoS rule defines the treatment of packets that do not match any other QoS rule in a PDU Session.

As long as the default QoS rule does not contain any packet filter, reflective QoS should not be applied for the QoS Flow which the default QoS rule is associated with and the RQA should not be sent for this QoS Flow.

5.7.1.5 QoS Flow mapping

The SMF performs the binding of SDFs to QoS Flows based on the QoS and service requirements (e.g. the received PCC rules). The SMF assigns the QFI for a new QoS Flow and derives its QoS profile from the information provided by the PCF. When applicable, the SMF provides the QFI together with the QoS profile to the (R)AN, and optionally a transport level packet marking value (e.g. the DSCP value of the outer IP header over N3 tunnel) to the (R)AN for the UL traffic. The SMF provides the SDF template i.e. Packet Filter Set (see clause 5.7.6) associated with the SDF received from the PCF) together with the SDF template precedence value (see clause 5.7.1.9) included in the PCC rule as defined in TS 23.503 [45], the QoS related information, and the corresponding packet marking information, i.e. the QFI, the transport level packet marking value (e.g. the DSCP value of the outer IP header over N3 tunnel) for downlink traffic and optionally the Reflective QoS Indication to the UPF enabling classification, bandwidth enforcement and marking of User Plane traffic. For each SDF, when applicable, the SMF generates a QoS rule Each of these QoS rules contain the QoS rule identifier, the QFI of the QoS Flow the Packet Filter Set of the UL part of the SDF template, optionally the Packet Filter Set for the DL part of the SDF template, and the QoS rule precedence value set to the precedence value of the PCC rule from which the QoS rule is generated. The QoS rules are then provided to the UE.

The principle for classification and marking of User Plane traffic and mapping of QoS Flows to AN resources is illustrated in Figure 5.7.1.5-1.

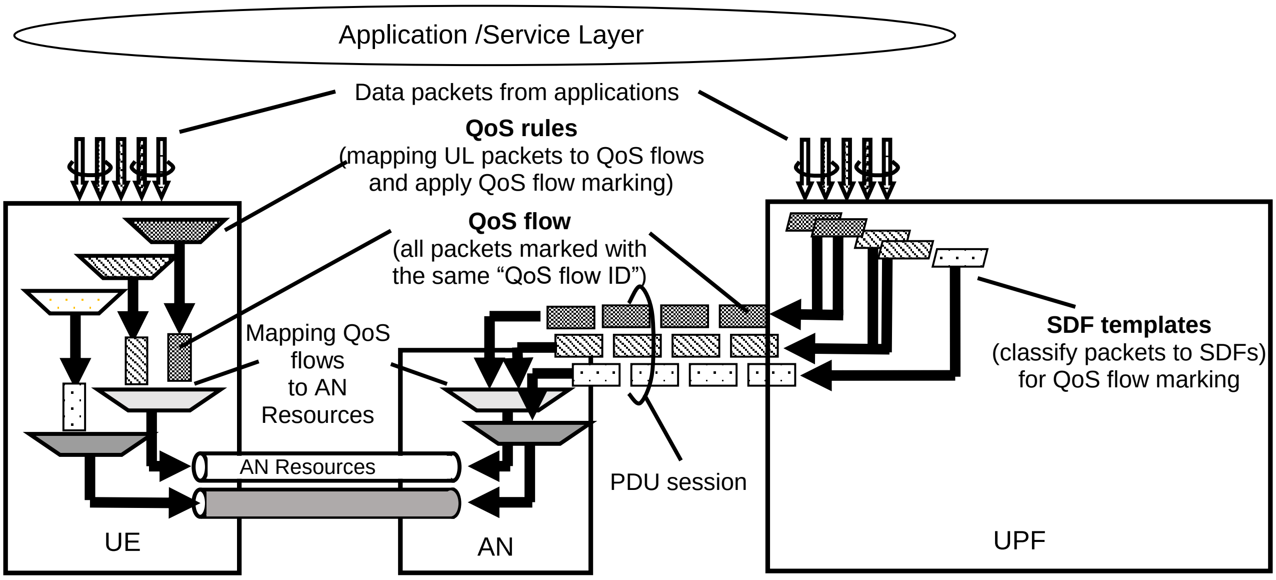

Application /Service Layer
Data packets from applications
QoS rules
(mapping UL packets to QoS flows and apply QoS flow marking)
QoS flow
(all packets marked with the same "QoS flow ID")
Mapping QoS flows to AN Resources
AN Resources
PDU session
SDF templates
(classify packets to SDFs) for QoS flow marking
UE
AN
UPF

Figure 5.7.1.5-1: The principle for classification and User Plane marking for QoS Flows and mapping to AN Resources

In DL, incoming data packets are classified by the UPF based on SDF templates according to the precedence of the PCC rule authorizing the service data flow, (without initiating additional N4 signalling). The UPF conveys the classification of the User Plane traffic belonging to a QoS Flow through an N3 (and N9) User Plane marking using a QFI. The AN binds QoS Flows to AN resources (i.e. Data Radio Bearers of in case of 3GPP RAN). There is no strict 1:1 relation between QoS Flows and AN resources. It is up to the AN to establish the necessary AN resources that QoS Flows can be mapped to, and to release them. The AN shall indicate to the SMF when the AN resources onto which a QoS flow is mapped are released.

If no match is found and all QoS Flows are related with a DL Packet Filter Set, the UPF shall discard the DL data packet.

In UL, the UE evaluates UL packets against the Packet Filter Set in the QoS rules based on the precedence value of QoS rules in increasing order until a matching QoS rule (i.e. whose packet filter matches the UL packet) is found. The UE uses the QFI in the corresponding matching QoS rule to bind the UL packet to a QoS Flow. The UE then binds QoS Flows to AN resources.

If no match is found and the default QoS rule contains an UL Packet Filter Set, the UE shall discard the UL data packet.

The MBR (and if applicable GBR) per SDF, if received from PCF over N7, is signalled on N4. For further information regarding MBR and GBR over N7, see TS 23.503 [45].

5.7.1.6 DL traffic

The following characteristics apply for processing of DL traffic:

- UPF maps User Plane traffic to QoS Flows based on the SDF templates
- UPF performs Session-AMBR enforcement and counting of packets for charging.

- UPF transmits the PDUs of the PDU Session in a single tunnel between 5GC and (R)AN, the UPF includes the QFI in the encapsulation header. In addition, UPF may include an indication for reflective QoS activation in the encapsulation header.

- UPF performs transport level packet marking in DL, e.g. setting the DiffServ Code point in outer IP header. Transport level packet marking may be based on the 5QI and ARP of the associated QoS Flow.

- (R)AN maps PDUs from QoS Flows to access-specific resources based on the QFI and the associated 5G QoS profile, also taking into account the N3 tunnel associated with the DL packet.

NOTE: Packet filters are not used for the mapping of QoS Flows onto access-specific resources in (R)AN.

- If reflective QoS applies, the UE creates a new derived QoS rule. The packet filter set in the derived QoS rule is derived from the header of the) DL packet, and the QFI of the UE derived QoS rule is set according to the QFI of the DL packet.

5.7.1.7 UL Traffic

Following characteristics apply for processing of UL traffic:

- UE uses the stored QoS rules to determine mapping between UL User Plane traffic and QoS Flows. UE marks the UL PDU with the QFI of the QoS rule containing the matching packet filter and transmits the UL PDUs using the corresponding access specific resource for the QoS Flow based on the mapping provided by RAN.

- (R)AN transmits the PDUs over N3 tunnel towards UPF. When passing an UL packet from (R)AN to CN, the (R)AN includes the QFI value, in the encapsulation header of the UL PDU, and selects the N3 tunnel.

- (R)AN performs transport level packet marking in the UL, transport level packet marking may be based on the 5QI and ARP of the associated QoS Flow. When applicable, (R)AN uses the transport level packet marking value (e.g. the DSCP value) if it is provided by the SMF during the PDU Session establishment/modification.

- UPF verifies whether QFIs in the UL PDUs are aligned with the QoS Rules provided to the UE or implicitly derived by the UE in case of reflective QoS).

- UPF performs Session-AMBR enforcement and counting of packets for charging.

5.7.1.8 AMBR/MFBR enforcement and rate limitation

For UL Classifier PDU Sessions, UL and DL Session-AMBR shall be enforced in the SMF selected UPF that supports the UL Classifier functionality. In addition, the DL Session-AMBR shall be enforced separately in every UPF that terminates the N6 interface (i.e. without requiring interaction between the UPFs) (see clause 5.6.4).

For multi-homed PDU Sessions, UL and DL Session-AMBR shall be enforced in the UPF that supports the Branching Point functionality. In addition, the DL Session-AMBR shall be enforced separately in every UPF that terminates the N6 interface (i.e. without requiring interaction between the UPFs) (see clause 5.6.4).

NOTE: The DL Session-AMBR is enforced in every UPF terminating the N6 interface to reduce unnecessary transport of traffic which may be discarded by the UPF performing the UL Classifier/Branching Point functionality due to the amount of the DL traffic for the PDU Session exceeding the DL Session-AMBR. Discarding DL packets in the UL Classifier/Branching Point could cause erroneous PDU counting for support of charging

The (R)AN shall enforce Max Bit Rate (UE-AMBR) limit in UL and DL per UE for non-GBR QoS Flows. The UE shall perform UL rate limitation on PDU Session basis for non-GBR traffic using Session-AMBR, if the UE receives a session-AMBR.

Rate limit enforcement per PDU Session applies for flows that do not require guaranteed flow bit rate. MBR per SDF is mandatory for GBR QoS Flows but optional for non-GBR QoS Flows. The MBR is enforced in the UPF.

The QoS control for Unstructured PDUs is performed at the PDU Session level and in this release of the specification there is only support for maximum of one 5G QoS Flow per PDU Session of Type Unstructured.

When a PDU Session is set up for transferring unstructured PDUs, SMF provides the QFI which will be applied to any packet of the PDU Session to the UPF and UE.

5.7.1.9 Precedence Value

The QoS rule precedence value and the SDF template precedence value determine the order in which a QoS rule or an SDF template, respectively, shall be evaluated. The evaluation of the QoS rules or SDF templates is performed in increasing order of their precedence value.

5.7.2 5G QoS Parameters

5.7.2.1 5QI

A 5QI is a scalar that is used as a reference to 5G QoS characteristics defined in clause 5.7.4, i.e. access node-specific parameters that control QoS forwarding treatment for the QoS Flow (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

Standardized 5QI values have one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in Table 5.7.4-1.

The 5G QoS characteristics for pre-configured 5QI values are pre-configured in the AN. The 5G QoS characteristics for dynamically assigned 5QI values are signalled as part of the QoS profile.

NOTE: On N3, each PDU (i.e. in the tunnel used for the PDU Session) is associated with one 5QI via the QFI carried in the encapsulation header.

5.7.2.2 ARP

The QoS parameter ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The priority level defines the relative importance of a resource request. This allows deciding whether a new QoS Flow may be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). It may also be used to decide which existing QoS Flow to pre-empt during resource limitations.

The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority. The pre-emption capability information defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. The pre-emption vulnerability information defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. The pre-emption capability and the pre-emption vulnerability shall be either set to 'yes' or 'no'.

The ARP priority levels 1-8 should only be assigned to resources for services that are authorized to receive prioritized treatment within an operator domain (i.e. that are authorized by the serving network). The ARP priority levels 9-15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.

NOTE: This ensures that future releases may use ARP priority level 1-8 to indicate e.g. emergency and other priority services within an operator domain in a backward compatible manner. This does not prevent the use of ARP priority level 1-8 in roaming situation in case appropriate roaming agreements exist that ensure a compatible use of these priority levels.

5.7.2.3 RQA

The Reflective QoS Attribute (RQA) is an optional parameter. which indicates that certain traffic (not necessarily all) carried on this QoS Flow is subject to Reflective QoS. Only when the RQA is signalled for a QoS Flow, the (R)AN enables the transfer of the RQI for AN resource corresponding to this QoS Flow. The RQA may be signalled to NG-RAN via the N2 reference point at UE context establishment in NG-RAN and at QoS Flow establishment or modification.

5.7.2.4 Notification control

In addition, a GBR QoS Flow may be associated with the parameter:

- Notification control.

The Notification control indicates whether notifications are requested from the RAN when the GFBR can no longer (or again) be fulfilled for a QoS Flow during the lifetime of the QoS Flow. If, for a given GBR QoS Flow, notification control is enabled and the NG-RAN determines that the GFBR cannot be fulfilled, RAN shall send a notification towards SMF. The RAN shall keep the QoS Flow, and should try to fulfil the GFBR. Upon receiving a notification from the RAN that the GFBR cannot be fulfilled, the 5GC may initiate N2 signalling to modify or remove the QoS Flow. When applicable, NG-RAN sends a new notification, informing SMF that the GFBR can be fulfilled again. After a configured time, the NG-RAN may send a subsequent notification that the GFBR cannot be fulfilled.

5.7.2.5 Flow Bit Rates

For GBR QoS Flows, the 5G QoS profile additionally include the following QoS parameters:

- Guaranteed Flow Bit Rate (GFBR) - UL and DL;

- Maximum Flow Bit Rate (MFBR) -- UL and DL.

The GFBR denotes the bit rate that may be expected to be provided by a GBR QoS Flow. The MFBR limits the bit rate that may be expected to be provided by a GBR QoS Flow (e.g. excess traffic may get discarded by a rate shaping function).

GFBR and MFBR are signalled on N2 and N11 for each of the GBR QoS Flows.

5.7.2.6 Aggregate Bit Rates

Each PDU Session of a UE is associated with the following aggregate rate limit QoS parameter:

- per Session Aggregate Maximum Bit Rate (Session-AMBR).

The subscribed Session-AMBR is a subscription parameter which is retrieved by the SMF from UDM. SMF may use the subscribed Session-AMBR or modify it based on local policy or use the authorized Session-AMBR received from PCF to get the Session-AMBR, which is signalled to the appropriate UPF entity/ies to the UE and to the (R)AN (to enable the calculation of the UE-AMBR). The Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows for a specific PDU Session. The Session-AMBR is measured over an AMBR averaging window which is a standardized value. The Session-AMBR is not applicable to GBR QoS Flows. In downlink direction, the Session-AMBR is enforced by the UPF. In uplink, the Session-AMBR is enforced by both the UE and the UPF.

Each UE is associated with the following aggregate rate limit QoS parameter:

- per UE Aggregate Maximum Bit Rate (UE-AMBR).

The UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE. Each (R)AN shall set its UE-AMBR to the sum of the Session-AMBR of all PDU Sessions with active user plane to this (R)AN up to the value of the subscribed UE-AMBR. The subscribed UE-AMBR is a subscription parameter which is retrieved from UDM and provided to the (R)AN by the AMF. The UE-AMBR is measured over an AMBR averaging window which is a standardized value. The UE-AMBR is not applicable to GBR QoS Flows. The (R)AN enforces the UE-AMBR in both downlink and uplink.

NOTE: The AMBR averaging window is only applied to Session-AMBR and UE-AMBR measurement and the AMBR averaging windows for Session-AMBR and UE-AMBR are standardised to the same value.

5.7.2.7 Default values

For each PDU Session Setup, SMF retrieves the subscribed default 5QI and ARP values from UDM. The SMF may change the subscribed default 5QI/ARP values based on local configuration or interaction with the PCF to retrieve the authorized default 5QIand ARP values which overrides the subscribed default 5QI and ARP values. The authorized default 5QI and ARP values are used by SMF to set QoS parameters for the QoS Flow which the default QoS rule is associated with. The default 5QI value shall be from the standardized value range for non-GBR 5QIs.

5.7.2.8 Maximum Packet Loss Rate

The Maximum Packet Loss Rate (UL, DL) indicates the maximum rate for lost packets of the QoS flow that can be tolerated in the uplink and downlink direction.

NOTE 1: In this Release, the Maximum Packet Loss Rate (UL, DL) can only be provided for a GBR QoS flow belonging to voice media.

NOTE 2: How the (R)AN uses the Maximum Packet Loss Rate (UL, DL) for handover threshold decisions is described in (R)AN specification.

5.7.3 5G QoS characteristics

5.7.3.1 General

This clause specifies the 5G QoS characteristics associated with 5QI. The characteristics describe the packet forwarding treatment that a QoS Flow receives edge-to-edge between the UE and the UPF in terms of the following performance characteristics:

1 Resource Type (GBR, delay critical GBR or Non-GBR);

2 Priority level;

3 Packet Delay Budget;

4 Packet Error Rate;

5 Averaging window.

6 Maximum Data Burst Volume (for 5QIs with 5G Access Network PDB <=20ms).

The 5G QoS characteristics should be understood as guidelines for setting node specific parameters for each QoS Flow e.g. for 3GPP radio access link layer protocol configurations.

Standardized or pre-configured 5G QoS characteristics, are indicated through the 5QI value, and are not signalled on any interface.

Signalled QoS characteristics are included as part of the QoS profile.

5.7.3.2 Resource Type

The Resource Type determines if dedicated network resources related QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated (e.g. by an admission control function in a radio base station). GBR QoS Flow are therefore typically authorized "on demand" which requires dynamic policy and charging control. A Non-GBR QoS Flow may be pre-authorized through static policy and charging control. There are two kinds of GBR resource types, GBR and Delay critical GBR. Both resource types are treated the same, except that the definition of PDB and PER are different.

5.7.3.3 Priority Level

The Priority level indicate a priority in scheduling resources among QoS Flows. The Priority levels shall be used to differentiate between QoS Flows of the same UE, and it shall also be used to differentiate between QoS Flows from different UEs. Once all QoS requirements are fulfilled for the GBR QoS Flows, spare resources can be used for any remaining traffic in an implementation specific manner. The lowest Priority level value corresponds to the highest Priority.

The priority level may be signalled with standardized 5QIs, and if it is received, it overwrites the default value specified in QoS characteristics Table 5.7.4.1.

5.7.3.4 Packet Delay Budget

The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the UPF that terminates the N6 interface. For a certain 5QI the value of the PDB is the same in UL and DL. In the case of 3GPP access, the PDB is used to support the configuration of scheduling and link layer functions (e.g. the setting of scheduling priority weights and HARQ target operating points). For a delay critical GBR QoS flows, a packet delayed more than PDB is counted as lost if the transmitted data burst is less than Maximum Data Burst Volume within the period of PDB. For all other flows, the PDB shall be interpreted as a maximum delay with a confidence level of 98 percent.

The PDB denotes a "soft upper bound" in the sense that an "expired" packet, e.g. a link layer SDU that has exceeded the PDB, does not need to be discarded and is not added to the PER. However, for a delay critical GBR resource type, packets delayed more than the PDB are added to the PER.

5.7.3.5 Packet Error Rate

The Packet Error Rate (PER) defines an upper bound for the rate of PDUs (e.g. IP packets) that have been processed by the sender of a link layer protocol (e.g. RLC in RAN of a 3GPP access) but that are not successfully delivered by the corresponding receiver to the upper layer (e.g. PDCP in RAN of a 3GPP access). Thus, the PER defines an upper bound for a rate of non-congestion related packet losses. The purpose of the PER is to allow for appropriate link layer protocol configurations (e.g. RLC and HARQ in RAN of a 3GPP access). For some 5QI the value of the PER is the same in UL and DL. For QoS Flows with delay critical GBR resource type, a packet which is delayed more than PDB (but which comply with the GBR and Maximum Data Burst Volume requirements) is counted as lost, and included in the PER. If the burst for a delay critical GBR QoS flow is greater than the Maximum Data Burst Volume, delayed packet is not included in the PER.

Editor's note: Whether for non-standardized 5QI value range "allowed boundaries" for the 5G QoS characteristics needs to be specified e.g. minimum allowed PDB< X ms, PLR < 10^-X, etc. is FFS.

5.7.3.6 Averaging Window

The Averaging window is defined only for GBR QoS Flows. The Averaging window represents the duration over which the GFBR and MFBR shall be calculated (e.g. (R)AN, UPF, UE). The averaging window may be signalled with 5QIs to the (R)AN and UPF, and if it is not received a standardized value applies (for standardized 5QIs the value in the QoS characteristics Table 5.7.4-1 applies).

5.7.3.7 Maximum Data Burst Volume

Each QoS flow with a 5QI with 5G-AN PDB value equal to 20 ms or lower shall be associated with:

- Maximum Data Burst Volume.

Maximum Data Burst Volume denotes the largest amount of data that the 5G-AN is required to serve within a period of 5G-AN PDB (i.e. 5G-AN part of the PDB). The Maximum Data Burst Volume may be signalled with 5QIs to the (R)AN, and if it is not received, a standardized value applies (for standardized 5QIs the value in the QoS characteristics Table 5.7.4) applies.

5.7.4 Standardized 5QI to QoS characteristics mapping

The one-to-one mapping of standardized 5QI values to 5G QoS characteristics is specified in table 5.7.4-1.

Table 5.7.4-1: Standardized 5QI to QoS characteristics mapping

5QI Value	Resource Type	Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume (NOTE 2)	Default Averaging Window	Example Services
B	Delay Critical GBR	11	5 ms	10^{-5}	160 B	TBD	Remote control (see TS 22.261 [2])
C NOTE 4		12	10 ms NOTE 5	10^{-6}	320 B	TBD	Intelligent transport systems
D		13	20 ms	10^{-5}	640 B	TBD	
1	GBR NOTE 1	20	100 ms	10^{-2}	N/A	TBD	Conversational Voice
2		40	150 ms	10^{-3}	N/A	TBD	Conversational Video (Live Streaming)
3		30	50 ms	10^{-3}	N/A	TBD	Real Time Gaming, V2X messages Electricity distribution – medium voltage, Process automation - monitoring
4		50	300 ms	10^{-6}	N/A	TBD	Non-Conversational Video (Buffered Streaming)
65		7	75 ms	10^{-2}	N/A	TBD	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		20	100 ms	10^{-2}	N/A	TBD	Non-Mission-Critical user plane Push To Talk voice
75		25	50 ms	10^{-2}	N/A	TBD	V2X messages
E NOTE 4		18	10 ms	10^{-4}	255 B	TBD	Discrete Automation
F NOTE 4		19	10 ms	10^{-4}	1358 B NOTE 3	TBD	Discrete Automation
5	Non-GBR NOTE 1	10	100 ms	10^{-6}		N/A	IMS Signalling
6		60	300 ms	10^{-6}		N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms	10^{-3}		N/A	Voice, Video (Live Streaming) Interactive Gaming
8		80	300 ms	10^{-6}		N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file
9		90				N/A	sharing, progressive video, etc.)
69		5	60 ms	10^{-6}		N/A	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70		55	200 ms	10^{-6}		N/A	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)
79		65	50 ms	10^{-2}		N/A	V2X messages

						N/A	
G		66	10 ms	10^{-6}	N/A	N/A	Low Latency eMBB applications Augmented Reality

NOTE 1: a packet which is delayed more than PDB is not counted as lost, thus not included in the PER.

NOTE 2: it is required that default Maximum Data Burst Volume is supported by a PLMN supporting the related 5QIs.

NOTE 3: This Maximum Burst Size value is intended to avoid IP fragmentation on an IPv6 based, IPSec protected, GTP tunnel to the 5G-AN node.

NOTE 4: A delay of 1 ms for the delay between a PCEF and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.

NOTE 5:The jitter for this service is assumed to be 20 msec as per TS 22.261 [2].

NOTE: For Standardized 5QI to QoS characteristics mapping, the table will be extended/updated to support service requirements for 5G, e.g. ultralow latency service.

Editor's note: need to support a 5QI with PDB 1ms is FFS.

Editor's note: The PDB and parameters in this table have to be aligned based on the outcome of discussions between RAN WG2 and SA WG1.

5.7.5 Reflective QoS

5.7.5.1 General

Reflective QoS enables the UE to map UL User Plane traffic to QoS Flows without SMF provided QoS rules and it applies for IP PDU Session and Ethernet PDU Session. This is achieved by creating UE derived QoS rules in the UE based on the received DL traffic. It shall be possible to apply reflective QoS and non-reflective QoS concurrently within the same PDU Session.

For a UE supporting reflective QoS functionality, the UE shall create a derived QoS rule for the uplink traffic based on the received DL traffic if reflective QoS function is used by the 5GC for some traffic flows. The UE shall use the derived QoS rules to determine mapping of UL traffic to QoS Flows.

If the 3GPP UE supports Reflective QoS functionality, the UE shall indicate support of reflective QoS to the network (i.e. SMF) during the PDU Session establishment.

5.7.5.2 UE Derived QoS Rule

The UE derived QoS rule contains following parameters:

- One Packet Filter (in the Packet Filter Set as defined in clause 5.7.6.2 or 5.7.6.3;
- QFI;
- Precedence value(see clause 5.7.1.9).

For PDU Session of IP type the UL packet filter is derived based on the received DL packet as follows:

- When Protocol ID / Next Header is set to TCP or UDP, by using the source and destination IP addresses, source and destination port numbers, and the Protocol ID / Next Header field itself.
- When Protocol ID / Next Header is set to ESP, by using the source and destination IP addresses, the Security Parameter Index, and the Protocol ID / Next Header field itself. If the received DL packet is an IPSec protected packet, and an uplink IPSec SA corresponding to a downlink IPSec SA of the SPI in the DL packet exists, then the UL packet filter contains an SPI of the uplink IPSec SA.

NOTE 1: In this release of the specification for PDU Sessions of IP type the use of Reflective QoS is restricted to service data flows for which Protocol ID / Next Header is set to TCP, UDP or ESP.

NOTE 2: The UE does not verify whether the downlink packets with RQI indication match the restrictions on Reflective QoS.

For PDU Session of Ethernet type the UL packet filter is derived based on the received DL packet by using the source and destination MAC addresses, the Ethertype on received DL packet is used as Ethertype for UL packet. In case of presence of 802.1Q, the VID and PCP in IEEE 802.1Q header(s) of the received DL packet is also used as the VID and PCP field for the UL packet filter. When double 802.1Q tagging is used, only the outer (S-TAG) is taken into account for the UL packet filter derivation.

NOTE 3: In this release of the specification for PDU Sessions of Ethernet type the use of Reflective QoS is restricted to service data flows for which 802.1Q tagging is used.

The QFI of the derived QoS rule is set to the value received in the DL packet.

When Reflective QoS is activated the precedence value for all derived QoS rules is set to a standardised value.

5.7.5.3 Reflective QoS Control

Reflective QoS is controlled on per-packet basis by using the Reflective QoS Indication (RQI) in the encapsulation header on N3 reference point together with the QFI, together with a Reflective QoS Timer (RQ Timer) value that is either signalled to the UE upon PDU Session establishment or set to a default value.

When the 5GC determines that Reflective QoS has to be used for a specific SDF belonging to a QoS Flow, the SMF shall provide the RQA (Reflective QoS Attribute) within the QoS Flow's QoS profile to the NG-RAN on N2 reference point unless it has been done so before. When the RQA has been provided to the NG-RAN for a QoS Flow and the 5GC determines that the QoS Flow carries no more SDF for which Reflective QoS has to be used, the SMF should signal the removal of the RQA (Reflective QoS Attribute) from the QoS Flow's QoS profile to the NG-RAN on N2 reference point.

NOTE 1: The SMF could have a timer to delay the sending of the removal of the RQA. This would avoid signalling to the RAN in case new SDFs subject to Reflective QoS are bound to this QoS Flow in the meantime.

When the 5GC determines to use reflective QoS for a specific SDF, the SMF shall include an indication to use reflective QoS for this SDF in the corresponding SDF information provided to the UPF via N4 interface.

When the UPF receives this indication for an SDF, the UPF shall set the RQI bit in the encapsulation header on the N3 reference point for every DL packet corresponding to this SDF.

When an RQI is received by (R)AN in a DL packet on N3 reference point, the (R)AN shall indicate to the UE the QFI and the RQI of that DL packet.

Upon reception of a DL packet with RQI:

- if a UE derived QoS rule with a packet filter corresponding to the DL packet does not already exist,
    - the UE shall create a new UE derived QoS rule with a packet filter corresponding to the DL packet; and
    - the UE shall start, for this UE derived QoS rule, a timer set to the RQ Timer value.
- otherwise,
    - if the QFI associated with the downlink packet is different from the QFI associated with derived QoS rule, the UE shall update the derived QoS rule with the new QFI; and
    - the UE shall restart the timer associated to this UE derived QoS rule.

NOTE 2: Non-3GPP ANs does not need N2 signalling to enable Reflective QoS. Non 3GPP accesses are expected to send transparently the QFI and RQI to the UE. If the UPF does not include the RQI, no UE derived QoS rule will be generated. If RQI is included to assist the UE to trigger an update of the UE derived QoS rule, the reception of PDU for a QFI restarts the RQ Timer.

Upon timer expiry associated with a UE derived QoS rule the UE deletes the corresponding UE derived QoS rule.

When the 5GC determines to no longer use reflective QoS for a specific SDF, the SMF shall remove the indication to use reflective QoS in the corresponding SDF information provided to the UPF via N4 interface.

When the UPF receives this instruction for this SDF, the UPF shall no longer set the RQI bit in the encapsulation header on the N3 reference point.

The UPF shall continue to accept the UL traffic of the SDF for the originally authorized QoS Flow for an operator configurable time.

NOTE 3: This means that the detection and QoS enforcement instructions which were applied before the SMF removed the indication to use reflective QoS remain active in UL direction while the accounting of the UL traffic is done according to the new instructions.

NOTE 4: The operator configurable time has to be at least as long as the RQ Timer value to ensure that no UL packet would be dropped until the UE derived QoS rule is deleted by the UE.

5.7.6 Packet Filter Set

5.7.6.1 General

Packet Filter Set is used in the QoS rules or SDF template to identify a QoS Flow. The Packet Filter Set may contain packet filters for the DL direction, the UL direction or packet filters that are applicable to both directions.

There are two types of Packet Filter Set, i.e. IP Packet Filter Set, and Ethernet Packet Filter Set, corresponding to those PDU Session Types.

5.7.6.2 IP Packet Filter Set

For IP PDU Session Type, the Packet Filter Set shall support packet filtering based on at least any combination of:

- Source/destination IP address or IPv6 prefix.
- Source / destination port number.
- Protocol ID of the protocol above IP/Next header type.
- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.
- Flow Label (IPv6).
- Security parameter index.
- Packet filter direction.

NOTE 1: A value left unspecified in a filter matches any value of the corresponding information in a packet.

NOTE 2: An IP address or Prefix may be combined with a prefix mask.

NOTE 3: Port numbers may be specified as port ranges.

5.7.6.3 Ethernet Packet Filter Set

For Ethernet PDU Session Type, the Packet Filter Set shall support packet filtering based on at least any combination of:

- Source/destination MAC address
- Ethertype as defined in IEEE 802.3 [yy]
- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) VID fields as defined in IEEE 802.1Q
- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) PCP/DEI fields as defined in IEEE 802.1Q
- IP Packet Filter Set, in case Ethertype indicates IPv4/IPv6 payload.
- Packet filter direction.

NOTE 1: The MAC address may be specified as address ranges.

NOTE 2: A value left unspecified in a filter matches any value of the corresponding information in a packet.

5.8 User Plane Management

5.8.1 General

User Plane Function(s) handle the user plane path of PDU Sessions. 3GPP specifications support deployments with a single UPF or multiple UPFs for a given PDU Session. UPF selection is performed by SMF. The details of UPF selection is described in clause 6.3.3. The number of UPFs supported for a PDU Session is unrestricted.

For IPv4 or IPv6 type PDU Sessions, the PDU Session Anchor may be IP anchor point of the IP address/prefix allocated to the UE. For an IPv4 type PDU Session or an IPv6 type PDU Session without multi-homing, when multiple PDU Session Anchors are used (due to UL CL being inserted), only one PDU Session Anchor is the IP anchor point for the PDU Session. For an IPv6 multi-homed PDU Session there are multiple IP (IPv6) anchor points as described in clause 5.6.4.3.

If the SMF had requested the UPF to proxy ARP or IPv6 Neighbour Solicitation for an Ethernet DNN, the UPF should respond to the ARP or IPv6 Neighbour Solicitation Request, itself.

Deployments with one single UPF used to serve a PDU Session do not apply to the Home Routed case and may not apply to the cases described in clause 5.6.4.

Deployments where a UPF is controlled either by a single SMF or multiple SMFs (for different PDU Sessions) are supported.

UPF traffic detection capabilities may be used by the SMF in order to control at least following features of the UPF:

- Traffic detection (e.g. classifying traffic of IP type, Ethernet type, or unstructured type)
- Traffic reporting (e.g. allowing SMF support for charging).
- QoS enforcement (The corresponding requirements are defined in clause 5.7).
- Traffic routing (e.g. as defined in clause 5.6.4. for UL CL or IPv6 multi-homing).

5.8.2 Functional Description

5.8.2.1 General

This clause contains detailed functional descriptions for some of the functions provided by the UPF. It is described how the SMF instructs it's corresponding UP function and which control parameters are used.

5.8.2.2 UE IP Address Management

5.8.2.2.1 General

The UE IP address management includes allocation and release of the UE IP address as well as renewal of the allocated IP address, where applicable.

The UE sets the requested PDU Session Type during the PDU Session Establishment procedure based on its IP stack capabilities as follows:

- A UE which supports IPv6 and IPv4 shall set the requested PDU Session Type to "IP".
- A UE which supports only IPv4 shall request for PDU Session Type "IPv4".
- A UE which supports only IPv6 shall request for PDU Session Type "IPv6".
- When the IP version capability of the UE is unknown in the UE (as in the case when the MT and TE are separated and the capability of the TE is not known in the MT), the UE shall request for PDU Session Type "IP".

The SMF selects PDU Session Type of the PDU Session as follows:

- If the SMF receives a request with PDU Session Type set to "IP", the SMF selects either PDU Session Type "IPv4" or "IPv6" based on DNN configuration and operator policies. A SMF also provides a cause value to the UE to indicate only the assigned PDU Session type is allowed. In this case, the UE shall not request another PDU Session to the same DNN for the other IP version that is not allowed by the network.

- If the SMF receives a request for PDU Session Type "IPv4" or "IPv6" and the requested IP version is supported by the DNN the SMF selects the requested PDU Session type.

An SMF shall perform IP address management procedure based on the selected PDU Session Type. If IPv4 PDU Session Type is selected, an IPv4 address is allocated to the UE. Similarly, if IPv6 PDU Session type is selected, an IPv6 prefix is allocated. For Roaming case, the SMF in this clause refers to the SMF controlling the UPF acting as IP anchor point. i.e. H-SMF in home routed case and V-SMF in local breakout case. . The SMF shall process the UE IP address management related messages, maintain the corresponding state information and provide the response messages to the UE. In case the UE IP address is obtained from the external data network, additionally, the SMF shall also send the allocation, renewal and release related request messages to the external data network and maintain the corresponding state information.

The 5GC elements and UE support the following mechanisms:

a. During PDU Session Establishment procedure, the SMF sends the IP address to the UE via SM NAS signalling. The IPv4 address allocation and/or IPv4 parameter configuration via DHCPv4 (according to RFC 2131 [9]) can also be used once PDU Session is established.

b. /64 IPv6 prefix allocation shall be supported via IPv6 Stateless Auto-configuration according to RFC 4862 [10], if IPv6 is supported. The details of Stateless IPv6 Address Autoconfiguration are described in clause 5.8.2.2.3. IPv6 parameter configuration via Stateless DHCPv6 (according to RFC 3736 [14]) may also be supported.

To allocate the IP address via DHCPv4, the UE may indicate to the network within the Protocol Configuration Options element that the UE requests to obtain the IPv4 address with DHCPv4, or obtain the IP address during the PDU Session Establishment procedure. This implies the following behaviour both for static and dynamic address allocation:

- The UE may indicate that it requests to obtain an IPv4 address as part of the PDU Session Establishment procedure. In such a case, the UE relies on the 5GC network to provide IPv4 address to the UE as part of the PDU Session Establishment procedure.

- The UE may indicate that it requests to obtain the IPv4 address after the PDU Session Establishment procedure by DHCPv4. That is, when the 5GC network supports DHCPv4 and allows that, it does not provide the IPv4 address for the UE as part of the PDU Session Establishment procedures. The network may respond to the UE by setting the allocated IPv4 Address to 0.0.0.0. After the PDU Session Establishment procedure is completed, the UE uses the connectivity with the 5GC and initiates the IPv4 address allocation on its own using DHCPv4. However, if the 5GC network provides IPv4 address to the UE as part of the PDU Session Establishment procedure, the UE should accept the IPv4 address indicated in the PDU Session Establishment procedure.

- If the UE sends no IP Address Allocation request, the SMF determines whether DHCPv4 is used between the UE and the SMF or not, based on per DNN configuration.

If dynamic policy provisioning is deployed, and the PCF was not informed of the IPv4 address at PDU Session Establishment procedure, the SMF shall inform the PCF about an allocated IPv4 address. If the IPv4 address is released, the SMF shall inform the PCF about the de-allocation of an IPv4 address.

In order to support DHCP based IP address configuration, the SMF shall act as the DHCP server towards the UE. The PDU Session Anchor UPF does not have any DHCP functionality. The SMF instructs the PDU Session Anchor UPF serving the PDU Session to forward DHCP packets between the UE and the SMF over the user plane.

When DHCP is used for external data network assigned addressing and parameter configuration, the SMF shall act as the DHCP client towards the external DHCP server. The UPF does not have any DHCP functionality. In case of DHCP server on the external data network, the SMF instructs a UPF with N6 connectivity to forward DHCP packets between the UE and the SMF and the external DHCP server over the user plane.

The IP address/prefix is released by the SMF upon release of the PDU Session.

The 5GC may also support the allocation of a static IPv4 address and/or a static IPv6 prefix based on subscription information in the UDM or based on the configuration on a per-subscriber, per-DNN basis and per-S-NSSAI.

If the static IP address/prefix is stored in the UDM, during PDU Session Establishment procedure, the SMF retrieves this static IP address/prefix from the UDM. If the static IP address/prefix is not stored in the UDM subscription record, it may be configured on a per-subscriber, per-DNN and per-S-NSSAI basis in the DHCP/DN-AAA server and the SMF retrieves the IP address/prefix for the UE from the DHCP/DN-AAA server. This IP address/prefix is delivered to the UE in the same way as a dynamic IP address/prefix. It is transparent to the UE whether the PLMN or the external data network allocates the IP address and whether the IP address is static or dynamic.

For IPv4 or IPv6 PDU Session Type, during PDU Session Establishment, the SMF may receive a Subscribers IP Index from the PCF, the SMF may use this to assist in selecting how the IP address is to be allocated when multiple allocation methods, or multiple instances of the same method are supported. In the case of roaming, it is the SMF controlling the UPF acting as IP anchor that is responsible for IP allocation, therefore it is this SMF that may receive the IP index from the PCF (in its own network).

5.8.2.2.2 Routing rules configuration

When the UE has an IPv6 multi-homed PDU Session the UE selects the source IPv6 prefix according to routing rules pre-configured in the UE or received from network. Routing rules received from the network have a higher priority than routing rules pre-configured in the UE

The SMF can decide the routing rules for a UE based on local configuration or dynamic policy received from the PCF. The SMF can send routing rules to the UE to influence the source IP prefix selection in IPv6 Router Advertisement (RA) messages according to RFC 4191 [8] at any time during the lifetime of the IPv6 multi-homed PDU Session. Such messages are sent via the UPF.

NOTE: For multiple IPv4 PDU Session and multiple IPv6 PDU Session cases, routing rule based PDU Session selection is not specified in this release.

5.8.2.2.3 The procedure of Stateless IPv6 Address Autoconfiguration

If Stateless IPv6 Address Autoconfiguration is used for IPv6 address allocation to the UE, after PDU Session establishment the UE may send a Router Solicitation message to the SMF to solicit a Router Advertisement message. The SMF sends a Router Advertisement message (solicited or unsolicited) to the UE. The Router Advertisement messages shall contain the IPv6 prefix.

After the UE has received the Router Advertisement message, it constructs a full IPv6 address via IPv6 Stateless Address Autoconfiguration in accordance with RFC 4862 [10]. To ensure that the link-local address generated by the UE does not collide with the link-local address of the UPF and the SMF, the SMF shall provide an interface identifier (see RFC 4862 [10]) to the UE and the UE shall use this interface identifier to configure its link-local address. For Stateless Address Autoconfiguration however, the UE can choose any interface identifier to generate IPv6 addresses, other than link-local, without involving the network. However, the UE shall not use any identifiers defined in TS 23.003 [19] as the basis for generating the interface identifier. For privacy, the UE may change the interface identifier used to generate full IPv6 address, as defined in TS 23.221 [23] without involving the network. Any prefix that the SMF advertises to the UE is globally unique. The SMF shall also record the relationship between the UE's identity (SUPI) and the allocated IPv6 prefix. Because any prefix that the SMF advertises to the UE is globally unique, there is no need for the UE to perform Duplicate Address Detection for any IPv6 address configured from the allocated IPv6 prefix. Even if the UE does not need to use Neighbor Solicitation messages for Duplicate Address Detection, the UE may, for example, use them to perform Neighbor Unreachability Detection towards the SMF, as defined in RFC 4861 [54]. Therefore, the SMF shall respond with a Neighbor Advertisement upon receiving a Neighbor Solicitation message from the UE.

The above IPv6 related messages (e.g. Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement) are transferred between the SMF and UE via the UPF(s).

5.8.2.3 CN Tunnel Info Allocation

5.8.2.3.1 General

CN Tunnel Info is the Core Network address of the N3/N9 tunnel corresponding to the PDU Session. It comprises the TEID and the IP address which is used by the UPF for the PDU Session.

Allocation and release of CN Tunnel Info is performed when a new PDU Session is established or released. This functionality is supported either by SMF or UPF, based on operator's configuration on the SMF. The SMF should indicate the UPF if the UPF is required to allocate/release CN Tunnel Info.

When both CN Tunnel Info allocation in SMF and CN Tunnel Info allocation in UPF coexist in the same network, the same CN Tunnel Info allocation option shall be used by all the SMF controlling a particular UPF.

5.8.2.3.2 CN Tunnel Info Allocation / Release in the SMF

If the network is configured to perform allocation/release of CN Tunnel Info in the SMF, the SMF shall manage the CN Tunnel Info space. The SMF shall allocate CN Tunnel Info for the applicable N4 reference points when a PDU Session is established and release the CN Tunnel Info when a PDU Session is released. In case of PDU Session establishment, the SMF shall provide the allocated CN Tunnel Info to UPF. The SMF shall also provide the CN Tunnel Info to RAN in order to complete the PDU Session establishment. In case of PDU Session release, the SMF shall notify the UPF about the release of the CN Tunnel Info.

5.8.2.3.3 CN Tunnel Info Allocation / Release in the UPF

If the network is configured to perform allocation/release of CN Tunnel Info in the UPF, the UPF shall manage the CN Tunnel Info space. In case of PDU Session establishment, the SMF shall request UPF to allocate CN Tunnel Info for the applicable N4 reference points. In response, the UPF provides CN Tunnel Info to the SMF. The SMF shall provide received CN Tunnel Info from the UPF to the RAN in order to complete the PDU Session establishment. In case of PDU Session release, the SMF shall request UPF to release CN Tunnel Info for the PDU Session.

5.8.2.4 Traffic Detection

5.8.2.4.1 General

This clause describes the detection process at the UPF that identifies the packets belonging to a session, or a service data flow.

The SMF is responsible for instructing the UP function about how to detect user data traffic belonging to a Packet Detection Rule (PDR). The other parameters provided within a PDR describe how the UP function shall treat a packet that matches the detection information.

5.8.2.4.2 Traffic Detection Information

The SMF controls the traffic detection at the UP function by providing detection information for every PDR.

For IPv4 or IPv6 PDU Session type, detection information is a combination of:

- PDU Session.
- QFI.
- IP Packet Filter Set as defined in clause 5.7.6.2.
- Application Identifier: The Application ID is an index to a set of application detection rules configured in UPF.

For Ethernet PDU Session type, detection information is a combination of:

- PDU Session,
- QFI,
- Ethernet Packet Filter Set as defined in clause 5.7.6.3.

In this release of the specification for Unstructured PDU Session Type, the UPF does not perform -QoS Flow level traffic detection for QoS enforcement.

Traffic detection information sent by the SMF to the UPF for a PDU Session may be associated with Network instance for detection and routing of traffic over N6.

NOTE: The UPF connected to different DN with possibly overlapping IP addresses is an example of a usage of a Network Instance.

5.8.2.5 Control of User Plane Forwarding

The SMF controls user-plane packet forwarding for traffic detected by a PDR by providing a FAR with instructions to the UPF, including:

- Forwarding operation information;
- Forwarding target information.

The details of the forwarding target and operation will depend on the scenario and is described below. The following forwarding functionality is required by the UPF:

- Apply GTP-U tunnel related handling, i.e. encapsulation.
- Forward the traffic to the SMF, e.g. DHCP signalling).
- Forward the SM PDU DN Request Container from SMF to DN-AAA server
- Forward the traffic according to locally configured policy for traffic steering.

5.8.2.6 Charging and Usage Monitoring Handling

5.8.2.6.1 General

The SMF shall support interfaces towards OCS/OFCS and PCF. The SMF interacts with OCS/PFCS and PCF based on information received from other control plane NFs and user plane related information received from the UPF.

QoS Flow level, PDU Session level and subscriber related information remain at the SMF, and only usage information is requested from the UPF.

5.8.2.6.2 Activation of Usage Reporting in UPF

Triggered by the PCC rules received from the PCF or preconfigured information available at SMF, as well as from the OCS for online charging via Credit-Control session mechanisms, the SMF shall provide Usage Reporting Rules to the UPF for controlling how usage reporting is performed.

The SMF shall request the report of the relevant usage information for Usage Monitoring, based on Monitoring Keys and triggers which are specified in TS 23.503 [45]. Each Usage Reporting Rule requested for usage monitoring control contains a list of "traffic flows" for UPF whose traffic is to be accounted under this rule. The SMF shall use Monitoring-key either preconfigured or received from the PCF within the PCC Rule in order to generate this list and also shall keep the mapping between them. This list may overlap across multiple Usage Reporting Rules, e.g. multiple different Usage Reporting Rules may contain the same "traffic flows".

The SMF shall request the report of the relevant usage information for offline and online charging, based on Rating Groups and triggers which are specified in TS 32.240 [41]. Each Usage Reporting Rule requested for offline or online charging contains a list of "traffic flows" for UPF whose traffic is to be accounted under this rule. The SMF shall use Rating Group or Sponsor Identity either preconfigured or provided by PCF and/or OCS as defined in TS 32.240 [41] and the PCC rule in order to generate this list and also shall keep the mapping between them. This list may overlap across multiple Usage Reporting Rules, e.g. multiple different Usage Reporting Rules may contain the same "traffic flows".

The SMF function shall also provide reporting trigger events to the UPF for when to report usage information. The reporting trigger events (e.g. triggers, threshold information etc.) shall be supported for the PDU Session level reporting as well as on Rule level basis as determined by the SMF. The triggers may be provided as a volume, time or event to cater for the different charging/usage monitoring models supported by the TS 23.503 [45] for usage monitoring and by TS 32.240 [41] for offline and online charging. The SMF shall decide on the thresholds value(s) based on allowance received from PCF, OCS or based on local configuration.

In some cases, the same Usage Reporting Rule can be used for different purposes (for both usage monitoring and charging), e.g. in case the same set of traffic flows, measurement method, trigger event, threshold, etc. apply. Similarly a reported measurement can be used for different purposes by the SMF.

5.8.2.6.3 Reporting of Usage Information towards SMF

The UPF shall support reporting of usage information to the SMF. The UPF shall be capable to support reporting based on different triggers, including:

- Periodic reporting with period defined by the SMF.
- Usage thresholds provided by the SMF.
- Report on demand received from the SMF.

The SMF shall make sure that the multiple granularity levels required by the reporting keys in the Usage Reporting rules satisfy the following aggregation levels without requiring a knowledge of the granularity levels by the UPF:

- PDU Session level reporting;
- Traffic flow (for both charging and usage monitoring) level reporting as defined by the reporting keys in the Usage Reporting Rule (see the description above).

Based on the mapping between Monitoring-key and PCC rule stored at the SMF, the SMF shall combine the reported information with session and subscriber related information which is available at the SMF, for Usage Monitoring reporting over the corresponding Npcf interface (N7 reference point).

Based on the mapping between Rating Group or Sponsor Identity and PCC rule stored at the SMF, the SMF shall combine the reported information with session and subscriber related information which is available at the SMF, for offline and online charging reporting over the corresponding charging interfaces.

This functionality is specified in TS 32.240 [41].

The usage information shall be collected in the UPF and reported to the SMF as defined in 5.8.2.6, based on Monitoring Keys and triggers which are specified in TS 23.503 [45].

5.8.2.7 PDU Session and QoS Flow Policing

ARP is used for admission control (i.e. retention and pre-emption of the new QoS Flow). The value of ARP is not required to be provided to the UPF.

For every QoS Flow, the SMF shall use the 5QI and optionally, the ARP priority level, to determine the transport level packet marking and provide the transport level packet marking to the UPF.

The SMF shall provide the PDU Session AMBR value to the UE and together with a QoS Enforcement Rule correlation ID to the UPF so that the UPF and the UE can enforce the PDU Session AMBR across all nonGBR QoS Flows of the PDU Session.

SMF shall provide the GFBR and MFBR value for each QoS Flow of the PDU Session to the UPF.

5.8.2.8 PCC Related Functions

5.8.2.8.1 Activation/Deactivation of predefined PCC rules

A predefined PCC rule is configured in the SMF.

The traffic detection filters, e.g. IP packet filter, required in the UP function can be configured either in the SMF and provided to the UPF, as service data flow filter(s), or be configured in the UPF, as the application detection filter identified by an application identifier. For the latter case, the application identifier has to be configured in the SMF and the UPF.

The traffic steering policy information can be only configured in the UPF, together with traffic steering policy identifier(s), while the SMF has to be configured with the traffic steering policy identifier(s).

Policies for traffic handling in the UPF, which are referred by some identifiers corresponding to the parameters of a PCC rule, can be configured in the UPF. These traffic handling policies are configured as predefined QER(s), FAR(s) and URR(s).

When a predefined PCC rule is activated/deactivated by the PCF, SMF shall decide what information has to be provided to the UPF to enforce the rule based on where the traffic detection filters (i.e. service data flow filter(s) or application detection filter), traffic steering policy information and the policies used for the traffic handling in the UPF are configured and where they are enforced:

- If the predefined PCC rule contains an application identifier for which corresponding application detection filters are configured in the UPF, the SMF shall provide a corresponding application identifier to the UPF;
- If the predefined PCC rule contains traffic steering policy identifier(s), the SMF shall provide a corresponding traffic steering policy identifier(s) to the UPF;
- If the predefined PCC rule contains service data flow filter(s), the SMF shall provide them to the UPF;
- If the predefined PCC rule contains some parameters for which corresponding policies for traffic handling in the UPF are configured in the UPF, the SMF shall activate those traffic handling policies via their rule ID(s).

The SMF shall maintain the mapping between a PCC rule received over Npcf and the QoS Flow level PDR rule(s) used on N4 interface.

5.8.2.8.2 Enforcement of Dynamic PCC Rules

The application detection filters required in the UPF can be configured either in the SMF and provided to the UPF as the service data flow filter, or be configured in the UP function identified by an application identifier.

When receiving a dynamic PCC rule from the PCF which contains an application identifier and/or parameters for traffic handling in the UPF:

- if the application detection filter is configured in the SMF, the SMF shall provide it in the service data flow filter to the UPF, as well as parameters for traffic handling in the UPF received from the dynamic PCC rule;
- otherwise, the application detection filters is configured in UPF, the SMF shall provide to UPF with the application identifier and the parameters for traffic handling in the UPF as required based on the dynamic PCC rule.

The SMF shall maintain the mapping between a PCC rule received over Npcf and the QoS Flow level PDR(s) used on N4 interface.

5.8.2.8.3 Redirection

The uplink application's traffic redirection may be enforced either in the SMF (as specified in 5.8.2.5 Control of user plane forwarding) or directly in the UPF. The redirect destination may be provided in the dynamic PCC rule or be preconfigured, either in the SMF or in the UPF.

When receiving redirect information (redirection enabled/disabled and redirect destination) within a dynamic PCC rule or being activated/deactivated by the PCF for the predefined redirection policies, SMF shall decide whether to provide and what information to be provided to the UPF based on where the redirection is enforced and where the redirect destination is acquired/preconfigured. When redirection is enforced in the UPF and the redirect destination is acquired from the dynamic PCC rule or is configured in the SMF, SMF shall provide the redirect destination to the UPF. When redirection is enforced in the SMF, SMF shall instruct the UPF to forward applicable user plane traffic to the SMF.

5.8.2.8.4 Support of SDCI

PFDF /or NEF shall provide PFD(s) to the SMF on the request of SMF (pull mode) or on the request of PFD management from NEF (push mode), as described in TS 23.503 [45]. The SMF shall provide the PFD(s) to the UPF, on which the Application ID corresponding to the PFD(s) is active.

The SMF supports the procedures in clause 4.4.3.1 of TS 23.502, for management of PFDs. PFD(s) is cached in the SMF, and the SMF maintains a caching timer associated to the PFD(s). When the caching timer expires and there's no active PCC rule that refers to the corresponding application identifier, the SMF informs the UPF to remove the PFD(s) identified by the application identifier using the PFD management message.

When a PDR is provided for an Application ID corresponding to the PFD(s) that are not already provided to the UPF, the SMF shall provide the PFD(s) to the UPF (if there are no PFD(s) cached, the SMF retrieves them from the PFDF / NEF as specified in TS 23.503 [45]). When any update of the PFD(s) is received from PFDF/NEF by SMF (using "push" or "pull" mode), and there are still active PDRs in UPF for the Application ID, the SMF shall provision the updated PFD set corresponding to the Application ID to the UPF using the PFD management message.

NOTE 1: SMF should assure not to overload N4 signalling while managing PFD(s) to the UPF, e.g. forwarding the PFD(s) to the right UPF where the PFD(s) is enforced.

When the UPF receives the updated PFD(s) from either the same or different SMF for the same application identifier, the latest received PFD(s) shall overwrite any existing PFD(s) stored in the UPF.

NOTE 2: For the case a single UPF is controlled by multiple SMF, the conflict of PFD(s) corresponding to the same application identifier provided by different SMF should be avoided by operator enforcing a well-planned PFDF/NEF and SMF/UPF deployment.

5.8.2.9 Functionality of Sending of "End marker"

5.8.2.9.0 Introduction

Sending of "end marker" is a functionality which involve SMF and UPF in order to assist the reordering function in the Target RAN. As part of the functionality, constructing of end marker packets can either be done in the SMF or in the UPF, as described in clauses 5.8.2.9.1 and 5.8.2.9.2. Whether constructing of end marker packets is performed by SMF or UPF is determined by network configuration.

5.8.2.9.1 UPF Constructing the "End marker" Packets

UPF referred in this clause is the UPF terminates N3 reference point.

It is assumed that the PDU Session for the UE comprises of an UPF that acts as a PDU Session anchor and an intermediate UPF terminating N3 reference point at the time of this Handover procedure.

In case of inter NG-RAN handover procedure without UPF change, SMF shall indicate the UPF to switch the N3 path(s) by sending an N4 Session Modification Request message with the new AN Tunnel Info of NG RAN and in addition, provide an indication to the UPF to send the end marker packet(s) on the old N3 user plane path.

On receiving this indication, the UPF shall construct end marker packet(s) and send it for each N3 GTP-U tunnel towards the source NG RAN after sending the last PDU on the old path.

In case of inter NG-RAN handover procedure with UPF change, SMF shall indicate the PSA UPF to switch the N9 user plane path(s) by sending an N4 Session Modification Request message (N4 session ID, new CN Tunnel Info of UPF) and in addition, provide an indication to the PSA UPF to send the end marker packet(s) on the old path.

On receiving this indication, the PSA UPF shall construct end marker packet(s) and send it for each N9 GTP-U tunnel towards the source UPF after sending the last PDU on the old path.

On receiving the end marker packet(s) on N9 GTP-U tunnel, source UPF shall forward the end marker packet(s) and send it for each N3 GTP-U tunnel towards the source NG RAN.

5.8.2.9.2 SMF Constructing the "End marker" Packets

UPF referred in this clause is the UPF terminates N3 reference point.

It is assumed that the PDU Session for the UE comprises of an UPF that acts as a PDU Session Anchor and an intermediate UPF terminating N3 reference point at the time of this Handover procedure.

In case of inter NG-RAN handover procedure without UPF change, SMF shall indicate the UPF to switch the N3 path(s) by sending an N4 Session Modification Request message (N4 session ID, new AN Tunnel Info of NG RAN). After sending the last PDU on the old path, UPF shall replace the old AN Tunnel Info with the new one and responds with an N4 Session Modification Response message to acknowledge the success of path switch.

When the path switch is finished, SMF constructs the end marker packet(s) and sends it to the UPF. UPF then forwards the packet(s) to the source NG RAN.

In case of inter NG-RAN handover procedure with UPF change, SMF shall indicate the PSA UPF to switch the N9 user plane path(s) by sending an N4 Session Modification Request message (N4 session ID, new CN Tunnel Info of UPF). After sending the last PDU on the old N9 path, PSA UPF shall replace the old CN Tunnel Info with the new one and responds with an N4 Session Modification Response message to acknowledge the success of path switch.

When the path switch is finished, SMF constructs the end marker packet(s) and sends it to PSA UPF. PSA UPF then forwards the packet(s) to the source UPF.

5.8.2.10 UP Tunnel Management

5GC shall support per PDU Session tunnelling on N3 between (R)AN and UPF and N9 between UPFs. If there exist more than one UPF involved for the PDU Session, any tunnel(s) between UPFs (e.g. in case of two UPFs, between the UPF that is an N3 terminating point and the UPF for PDU Session Anchor) remains established when a UE enters CM-IDLE state. In the case of downlink data buffering by UPF, when mobile terminated (MT) traffic arrives at the PDU Session Anchor UPF, it is forwarded to the UPF which buffer the data packet via N9 tunnel. See clause 5.8.3 for more details on UPF buffering. In case of Home Routed roaming, the SMF in HPLMN is not aware of the UP activation state of a PDU Session.

When the UP connection of the PDU Session is deactivated, the SMF may release the UPF of N3 terminating point. In that case the UPF (e.g. the Branching Point/UL CL or PDU Session Anchor) connecting to the released UPF of N3 terminating point will buffer the DL packets. Otherwise, when the UPF with the N3 connection is not released, this UPF will buffer the DL packets.

When the UP connection of the PDU Session is activated due to a down-link data arrived and a new UPF is allocated to terminate the N3 connection, a data forwarding tunnel between the UPF that has buffered packets and the newly allocated UPF is established, so that the buffered data packets are transferred from the old UPF that has buffered packets to the newly allocated UPF via the data forwarding tunnel..

For a PDU Session whose the UP connection is deactivated and the SMF has subscribed the location change notification, when the SMF is notified of UE's new location from the AMF and detects that the UE has moved out of the service area of the existing intermediate UPF, the SMF may decide to maintain the intermediate UPF, remove the established tunnel between UPFs (in case of removal of the intermediate UPF) or reallocate the tunnel between UPFs (in case of reallocation of the intermediate UPF).

5.8.2.11 Parameters for N4 session management

These parameters are used to control the functionality of the UPF as well as to inform about events occurring at the UPF.

The N4 session management procedures defined in clause 4.4.1 of TS 23.502 [3] will use the relevant parameters in the same way for all N4 reference points: the N4 session establishment procedure as well as the N4 session modification procedure provide the control parameters to the UPF, the N4 session release procedure removes all control parameters related to an N4 session and the N4 session level reporting procedure informs the SMF about events related to the PDU Session that are detected by the UPF.

The parameters over N4 provided from SMF to UPF comprises N4 Session ID and four different rules (i.e. one "detection" rule and three different "enforcement" rules):

- N4 Session ID assigned by the SMF uniquely identifies a PDU Session for a UE.
- Packet Detection Rule (PDR) contains information to classify a packet arriving at the UPF.
- Forwarding Action Rule (FAR) contains information on whether forwarding, dropping or buffering is to be applied to a packet.
- Usage Reporting Rule (URR) contains information that defines how a packet shall be accounted as well as how a certain measurement shall be reported.
- QoS Enforcement Rule (QER), contains information related to QoS enforcement of traffic.

Editor's note: The detailed description of the above parameters is FFS.

5.8.3 Explicit Buffer Management

5.8.3.1 General

5GC supports buffering of UE's data packets for deactivated PDU Sessions.

Support for buffering in the UPF is mandatory and optional in the SMF.

5.8.3.2 Buffering at UPF

The SMF provides instructions to the UPF for at least the following behaviours:

- buffer without reporting the arrival of first downlink packet,
- buffer with reporting the arrival of first downlink packet, or
- drop packet.

When the UP connection of the PDU Session is deactivated and the SMF decides to activate buffering in UPF for the session, the SMF shall inform the UPF to start buffering packets for this PDU Session.

Buffering in the UPF may be configured based on timers or the amount of downlink data to be buffered. The SMF decides whether buffering timers or amount of downlink data are handled by the UPF or SMF.

After starting buffering, when the first downlink packet arrives, UPF shall inform the SMF if it is setup to report. UPF sends a downlink data notification message to the SMF via N4 unless specified otherwise and indicates the user plane path on which the downlink packet was received.

When the UP connection of the PDU Session is activated, the SMF updates the UPF of the change in buffering state. The buffered data packets, if any, are then forwarded to the (R)AN by the UPF.

If the UP connection of the PDU Session has been deactivated for a long time, the SMF may indicate the UPF to stop buffering for this PDU Session.

5.8.3.3 Buffering at SMF

When the UP connection of the PDU Session is deactivated and the SMF supports buffering capability, the SMF may decide to activate buffering on SMF, the SMF shall inform the UPF to start forwarding the downlink data packets towards the SMF.

When the UP connection of the PDU Session is activated, if there are buffered packets available and their buffering duration has not expired, the SMF shall forward those packets to the UPF to relay them to the UE. These packets are then forwarded by the UPF to the (R)AN.

5.8.4 SMF Pause of Charging

The SMF Pause of Charging functionality is supported with the purpose that the charging and usage monitoring data in the core network more accurately reflects the downlink traffic actually sent to the (R)AN. When the amount of downlink data incoming at the UPF for a PDU Session that is in deactivated state goes above a pre-configured threshold, the pause of charging functionality ensures that data that dropped in the core network is not included in charging and usage monitoring records.

The procedures for SMF Pause of Charging are described in TS 23.502 [3].

5.9 Identifiers

5.9.1 General

Each subscriber in the 5G System shall be allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system. The 5G System supports identification of subscriptions independently of identification of the user equipment. Each UE accessing the 5G System shall be assigned a Permanent Equipment Identifier (PEI).

The 5G System supports allocation of a temporary identifier (5G-GUTI) in order to support user confidentiality protection.

5.9.2 Subscription Permanent Identifier

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

The following have been identified as valid SUPI types for this Release:

- IMSI as defined in TS 23.003 [19].
- Network Access Identifier (NAI) using the NAI RFC 4282 [20] based user identification as defined in TS 23.003 [19].

NOTE: By using the NAI, it will be possible to also use non-IMSI based SUPIs.

It is possible for a representation of the IMSI to be contained within the NAI for the SUPI e.g. when used over a non-3GPP Access Technology.

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

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

5.9.3 Permanent Equipment Identifier

A Permanent Equipment Identifier (PEI) is defined for the 3GPP UE accessing the 5G System.

The PEI can assume different formats for different UE types and use cases. The UE shall present the PEI to the network together with an indication of the PEI format being used.

If the UE supports at least one 3GPP access technology, the UE must be allocated a PEI in the IMEI format.

In the scope of this release, the only format supported for the PEI parameter is an IMEI, as defined in TS 23.003 [19].

5.9.4 5G Globally Unique Temporary Identifier

The AMF shall allocate a 5G Globally Unique Temporary Identifier (5G-GUTI) to the UE that is common to both 3GPP and non-3GPP access. It shall be possible to use the same 5G-GUTI for accessing 3GPP access and non-3GPP access security context within the AMF for the given UE. An AMF may re-assign a new 5G-GUTI to the UE at any time. The AMF may delay updating the UE with its new 5G-GUTI until the next NAS transaction.

The 5G-GUTI shall be structured as:

<5G-GUTI> := <GUAMI> <5G-TMSI>

where GUAMI identifies the assigned AMF and 5G-TMSI identifies the UE uniquely within the AMF.

The Globally Unique AMF ID (GUAMI) shall be structured as:

<GUAMI> := <MCC> <MNC> <AMF Region ID> <AMF Set ID> <AMF Pointer>

where AMF Region ID identifies the region, AMF Set ID uniquely identifies the AMF Set within the AMF Region and AMF Pointer uniquely identifies the AMF within the AMF Set.

NOTE 1: The AMF Region ID addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer by enabling operators to re-use the same AMF Set IDs and AMF Pointers in different regions.

NOTE 2: See TS 23.003 [19] for details on the structure of the fields of GUAMI.

The 5G-S-TMSI is the shortened form of the GUTI to enable more efficient radio signalling procedures (e.g. during Paging and Service Request) and is defined as:

<5G-S-TMSI> := <AMF Set ID> <AMF Pointer> <5G-TMSI>

5.9.5 AMF Name

An AMF is identified by an AMF Name. It can be configured with one or more GUAMIs. At a given time, GUAMI value is associated to one AMF name only.

5.9.6 Data Network Name (DNN)

A DNN is equivalent to an APN as defined in TS 23.003 [19]. Both identifiers have an equivalent meaning and carry the same information.

The DNN may be used e.g. to:

- Select a SMF and UPF(s) for a PDU Session.
- Select N6 interface(s) for a PDU Session.
- Determine policies to apply to this PDU Session.

5.9.7 Internal-Group Identifier

The subscription data for an UE in UDM may associate the subscriber with groups. A group is identified by an Internal-Group Identifier.

NOTE 1: A UE can belong to a limited number of groups, the exact number is defined in stage 3 specifications

NOTE 2: In this release of the specification, the support of groups is only defined in non-roaming case.

The group identifiers corresponding to an UE are provided by the UDM to the SMF and (when PCC applies to a PDU Session) by the SMF to the PCF. The SMF may use this information to apply local policies and to store this information in CDR. The PCF may use this information to enforce AF requests as described in clause 5.6.7.

5.9.8 Generic Public Subscription Identifier

Generic Public Subscription Identifier (GPSI) is needed for addressing a 3GPP subscription in different data networks outside of the 3GPP system. The 3GPP system stores within the subscription data the association between the GPSI and the corresponding SUPI.

GPSIs are public identifiers used both inside and outside of the 3GPP system.

The GPSI is either an MSISDN or an External Identifier, see TS 23.003 [19]. If MSISDN is included in the subscription data, it shall be possible that the same MSISDN value is supported in both 5GS and EPS.

NOTE: There is no implied 1-to-1 relationship between GPSI and SUPI.

5.10 Security aspects

5.10.1 General

The security functions in the 5G System include:

- Authentication of the UE by the network and vice versa (mutual authentication between UE and network).
- Security context generation and distribution.
- User Plane data confidentiality and integrity protection.

- Control Plane signalling confidentiality and integrity protection.
- User identity confidentiality.
- Support of LI requirements as specified in TS 33.106 [35] subject to regional/national regulatory requirements, including protection of LI data (e.g., target list) that may be stored or transferred by an NF.

Detailed security related network functions for 5G are described in TS 33.501 [29].

5.10.2 Security Model for non-3GPP access

5.10.2.1 Signalling Security

When a UE is connected via a NG-RAN and via a standalone non-3GPP accesses, the multiple N1 instances are secured using independent NAS security contexts, each created based on the security context in the corresponding SEAF (e.g. in the common AMF when the UE is served by the same AMF) derived from the UE authentication.

5.11 Support for Dual Connectivity, Multi-Connectivity

5.11.1 Support for Dual Connectivity

Dual Connectivity involves two radio network nodes in providing radio resources to a given UE (with active radio bearers), while a single N2 termination point exists for the UE between an AMF and the RAN. The RAN architecture and related functions to support Dual Connectivity is further described in RAN specifications (e.g. TS 37.340 [31]).

The RAN node at which the N2 terminates, performs all necessary N2 related functions such as mobility management, relaying of NAS signalling, etc. and manages the handling of user plane connection (e.g. transfer over N3). It is called the Master RAN Node. It may use resources of another RAN node, the Secondary RAN node, to exchange User Plane traffic of an UE

If the UE has Mobility Restriction (either signalled from the UDM, or, locally generated by VPLMN policy in the AMF) the AMF signals these restrictions to the Master RAN Node as Handover Restriction List; This may prevent the Master RAN node from setting up a Dual Connectivity for an UE.

Dual Connectivity provides the possibility for the Master RAN to request SMF:

- For some or all PDU Sessions of an UE: Direct all the DL User Plane traffic of the PDU Session to the either the Master RAN Node or to the Secondary RAN Node. In this case, there is a single N3 tunnel termination at the RAN for such PDU Session.

NOTE: The terminating RAN Node, can decide to keep traffic for specific QFI(s) in a PDU Session for a UE on a single RAT, or split them across the two RATs.

- For some other PDU Sessions of an UE: Direct the DL User Plane traffic of some QoS Flows of the PDU Session to the Secondary (respectively Master) RAN Node while the remaining QoS Flows of the PDU Session are directed to the Master (respectively Secondary) RAN Node. In this case there are, irrespective of the number of QoS Flows, two N3 tunnel terminations at the RAN for such PDU Session.

The Master RAN may create and change this assignment for the user plane of a PDU Session at any time during the life time of the PDU Session;

In both cases, a single PDU Session Id is used to identify the PDU Session.

Additional functional characteristics are:

- User location information reporting is based on the identity of the cell that is serving the UE in the Master RAN node.
- Path update signalling related with Dual Connectivity and UPF re-allocation cannot occur at the same time.

5.12 Charging

The 5GC charging supports collection and reporting of charging information for network resource usage, as defined in TS 32.240 [41].

The SMF supports the interactions towards the charging system, as defined in TS 32.240 [41]. The UPF supports functionality to collect and report usage data to SMF. The N4 reference point supports the SMF control of the UPF collection and reporting of usage data.

5.13 Support for Edge Computing

Edge computing enables operator and 3rd party services to be hosted close to the UE's access point of attachment, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

NOTE: Edge Computing typically applies to non-roaming and LBO roaming scenarios.

The 5G Core Network selects a UPF close to the UE and executes the traffic steering from the UPF to the local Data Network via a N6 interface. This may be based on the UE's subscription data, UE location, the information from Application Function (AF) as defined in clause 5.6.7, policy or other related traffic rules.

Due to user or Application Function mobility, the service or session continuity may be required based on the requirements of the service or the 5G network.

The 5G Core Network may expose network information and capabilities to an Edge Computing Application Function.

NOTE: Depending on the operator deployment, certain Application Functions can be allowed to interact directly with the Control Plane Network Functions with which they need to interact, while the other Application Functions need to use the external exposure framework via the NEF (see clause 6.2.10 for details).

The functionality supporting for edge computing includes:

- User plane (re)selection: the 5G Core Network (re)selects UPF to route the user traffic to the local Data Network as described in clause 6.3.3;
- Local Routing and Traffic Steering: the 5G Core Network selects the traffic to be routed to the applications in the local Data Network;
  - this includes the use of a single PDU Session with multiple PDU Session Anchor(s) (UL CL / IP v6 multi-homing) as described in clause 5.6.4.
- Session and service continuity to enable UE and application mobility as described in clause 5.6.9;
- An Application Function may influence UPF (re)selection and traffic routing via PCF or NEF as described in clause 5.6.7;
- Network capability exposure: 5G Core Network and Application Function to provide information to each other via NEF as described in clauses 5.20 and 7.4 or directly as described in clause 7.3;
- QoS and Charging: PCF provides rules for QoS Control and Charging for the traffic routed to the local Data Network;
- Support of Local Area Data Network: 5G Core Network provides support to connect to the LADN in a certain area where the applications are deployed as described in clause 5.6.5.

5.14 Policy Control

The policy and charging control framework for the 5G System is defined in TS 23.503 [45].

5.15 Network slicing

5.15.1 General

A Network Slice is defined within a PLMN and shall include:

- the Core Network Control Plane and User Plane Network Functions, as described in clause 4.2,

and, in the serving PLMN, at least one of the following:

- the NG Radio Access Network described in 3GPP TS 38.300 [27],
- the N3IWF functions to the non-3GPP Access Network described in clause 4.2.7.2.

Network slicing support for roaming is described in clause 5.15.6.

Network slices may differ for supported features and network functions optimisations, in which case such Network Slices may have e.g. different S-NSSAIs with different Slice/Service Types (see sub-clause 5.15.2.1). The operator can deploy multiple Network Slice instances delivering exactly the same features but for different groups of UEs, e.g. as they deliver a different committed service and/or because they are dedicated to a customer, in which case such Network Slices may have e.g. different S-NSSAIs with the same Slice/Service Type but different Slice Differentiators (see sub-clause 5.15.2.1).

The network may serve a single UE with one or more Network Slice instances simultaneously via a 5G-AN and associated with at most eight different S-NSSAIs in total. The AMF instance serving the UE logically belongs to each of the Network Slice instances serving the UE, i.e. this AMF instance is common to the Network Slice instances serving a UE.

NOTE: In this release of the specification it is assumed that in any (home or visited) PLMN it is always possible to select an AMF that can serve any combination of S-NSSAIs that will be provided as an Allowed NSSAI.

The selection of the set of Network Slice instances for a UE is triggered by the first contacted AMF in a registration procedure normally by interacting with the NSSF, and can lead to a change of AMF. This is further described in clause 5.15.5.

A PDU Session belongs to one and only one specific Network Slice instance per PLMN. Different Network Slice instances do not share a PDU Session, though different slices may have slice-specific PDU Sessions using the same DNN.

During the Handover procedure the source AMF selects a target AMF by interacting with the NRF as specified in clause 6.3.5.

5.15.2 Identification and selection of a Network Slice: the S-NSSAI and the NSSAI

5.15.2.1 General

An S-NSSAI identifies a Network Slice.

An S-NSSAI is comprised of:

- A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services;
- A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

An S-NSSAI can have standard values (i.e. such S-NSSAI is only comprised of an SST with a standardised SST value, see clause 5.15.2.2, and no SD) or non-standard values (i.e. such S-NSSAI is comprised of either both an SST and an SD or only an SST without a standardised SST value and no SD). An S-NSSAI with a non-standard value identifies a single Network Slice within the PLMN with which it is associated. An S-NSSAI with a non-standard value shall not be used by the UE in access stratum procedures in any PLMN other than the one to which the S-NSSAI is associated.

HPLMN values are used for the S-NSSAIs in the NSSP of the URSP rules (see clause 6.6.2, TS 23.503 [45]) and Subscribed S-NSSAIs (see clause 5.15.3). They are also used as part of the optional mapping of the Configured NSSAI, the Allowed NSSAI (see clause 5.15.4.1) and the Requested NSSAI (see clause 5.15.5.2.1) to the Configured NSSAI for the HPLMN.

Serving PLMN values are used for the S-NSSAIs in the Configured NSSAI for that PLMN, in the Allowed NSSAI (see clause 5.15.4.1) and in the Requested NSSAI (see clause 5.15.5.2.1).

The NSSAI is a collection of S-NSSAIs. An NSSAI may be a Configured NSSAI, a Requested NSSAI or an Allowed NSSAI. There can be at most eight S-NSSAIs in Allowed and Requested NSSAIs sent in signalling messages between the UE and the Network. The Requested NSSAI signalled by the UE to the network allows the network to select the Serving AMF, Network Slice(s) and Network Slice instance(s) for this UE, as specified in sub-clause 5.15.5.

Based on the operator's operational or deployment needs, a Network Slice instance be associated with one or more S-NSSAIs, and an S-NSSAI can be associated with one or more Network Slice instances. Multiple Network Slice instances associated with the same S-NSSAI may be deployed in the same or in different Tracking Areas. When multiple Network Slice instances associated with the same S-NSSAI are deployed in the same Tracking Areas, the AMF instance serving the UE may logically belong to (i.e. be common to) more than one Network Slice instance associated with this S-NSSAI.

In a PLMN, when an S-NSSAI is associated with more than one Network Slice instance one of these Network Slice instances, as a result of the Network Slice instance selection procedure defined in clause 5.15.5, serves a UE that is allowed to use this S-NSSAI. For any S-NSSAI, the network may at any one time serve the UE with only one Network Slice instance associated with this S-NSSAI until cases occur where e.g. this Network Slice instance is no longer valid in a given registration area, or a change in UE's Allowed NSSAI occurs etc. In such cases, procedures mentioned in clause 5.15.5.2.2 or clause 5.15.5.2.3 apply.

Based on the Requested NSSAI (if any) and the Subscription Information, the 5GC is responsible for selection of a Network Slice instance(s) to serve a UE including the 5GC Control Plane and User Plane Network Functions corresponding to this Network Slice instance(s).

The (R)AN may use Requested NSSAI in access stratum signalling to handle the UE Control Plane connection before the 5GC informs the (R)AN of the Allowed NSSAI. The Requested NSSAI is not used by the RAN for routing when the UE provides a 5G-GUTI.

When a UE is successfully registered, the CN informs the (R)AN by providing the Allowed NSSAI.

NOTE: The details of how the RAN uses NSSAI information are described in TS 38.300 [27].

5.15.2.2 Standardised SST values

Standardized SST values provide a way for establishing global interoperability for slicing so that PLMNs can support the roaming use case more efficiently for the most commonly used Slice/Service Types.

The SSTs which are standardised are in the following Table 5.15.2.2-1.

Table 5.15.2.2-1 - Standardised SST values

Slice/Service type	SST value	Characteristics.
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.

NOTE: The support of all standardised SST values is not required in a PLMN.

5.15.3 Subscription aspects

The Subscription Information may contain one or more S-NSSAIs i.e. Subscribed S-NSSAIs. At most eight Subscribed S-NSSAIs can be marked as a default S-NSSAI. If an S-NSSAI is marked as default, then the network is expected to serve the UE with the related applicable Network Slice instance when the UE does not send any valid S-NSSAI to the network in a Registration Request message as part of the Requested NSSAI.

The Subscription Information for each S-NSSAI may contain multiple DNNs and one default DNN.

The network verifies the Requested NSSAI the UE provides in the Registration Request against the Subscription Information.

In roaming case, the UDM may provide to the VPLMN a subset of the Subscribed S-NSSAIs in the Subscription Information, reflecting the set of S-NSSAIs the HPLMN enables for the UE in the VPLMN.

5.15.4 UE NSSAI configuration and NSSAI storage aspects

5.15.4.1 General

A UE can be configured by the HPLMN with slice configuration information.

The slice configuration information contains one or more Configured NSSAI(s). A Configured NSSAI may apply either to one PLMN or to all PLMNs that do not have a specific Configured NSSAI (e.g. this could be possible for NSSAIs containing only S-NSSAIs with standard values, see clause 5.15.2.1). There is at most one Configured NSSAI per PLMN.

The Configured NSSAI of a PLMN may include S-NSSAIs that have standard values or PLMN-specific values.

The Configured NSSAI for the Serving PLMN includes the S-NSSAI values which can be used in the Serving PLMN and may be associated with mapping of each S-NSSAI of the Configured NSSAI to the corresponding S-NSSAI values in the Configured NSSAI for the HPLMN.

The S-NSSAIs in the Configured NSSAI for the HPLMN, at the time when they are provided to the UE, match the Subscribed S-NSSAIs for the UE.

When providing a Requested NSSAI to the network upon registration, the UE in a given PLMN only includes and uses S-NSSAIs applying to this PLMN, possibly associated with mapping of each S-NSSAI of the Requested NSSAI to the S-NSSAIs of the Configured NSSAI for the HPLMN i.e. part of the Configured and/or Allowed NSSAIs applicable for this PLMN. Upon successful completion of a UE's Registration procedure, the UE obtains an Allowed NSSAI, which includes one or more S-NSSAIs, from the AMF, possibly associated with mapping of Allowed NSSAI to Configured NSSAI for the HPLMN. These S-NSSAIs are valid for the current Registration Area provided by the serving AMF the UE has registered with and can be used simultaneously by the UE (up to the maximum number of simultaneous Network Slices or PDU Sessions).

The UE might also obtain one or more rejected S-NSSAIs with cause and validity of rejection from the AMF. An S-NSSAI may be rejected:

- for the PLMN; or
- for the current Registration area.

While it remains RM-REGISTERED in the PLMN, the UE shall not re-attempt to register to an S-NSSAI rejected in the PLMN.

While it remains RM-REGISTERED in the PLMN, the UE shall not re-attempt to register to an S-NSSAI rejected in the current Registration Area until it moves out of the current Registration Area.

NOTE 1: The details and more cases of S-NSSAI rejection are described in TS 24.501 [47].

The UE shall use only the S-NSSAI(s) in the Allowed NSSAI corresponding to a Network Slice for the subsequent procedures in the serving PLMN, as described in clause 5.15.5.

The UE stores (S)NSSAIs as follows:

- When the UE is provisioned with a Configured NSSAI for a PLMN and optionally associated mapping of the Configured NSSAI to Configured NSSAI for the HPLMN, the Configured NSSAI and the mapping shall be stored in the UE until a new Configured NSSAI for this PLMN is provisioned in the UE by the HPLMN:
  - When provisioned with a new Configured NSSAI for a PLMN and optionally associated mapping of the Configured NSSAI to Configured NSSAI for the HPLMN, the UE shall both replace any stored Configured NSSAI for this PLMN and the associated mapping with the new Configured NSSAI and the associated mapping, and delete any stored Allowed NSSAI and rejected S-NSSAI for this PLMN;

NOTE 2: It is expected that the UE keeps storing a received Configured NSSAI for a PLMN even when registering in another PLMN. However, the number of Configured NSSAI to be kept stored in the UE for PLMNs other than the HPLMN is up to UE implementation.

- If received, the Allowed NSSAI for a PLMN and any associated mapping of the Allowed NSSAI to the Configured NSSAI for the HPLMN shall be stored in the UE. The UE should store the Allowed NSSAI also when the UE is turned off;

NOTE 3: Whether the UE stores the Allowed NSSAI also when the UE is turned off is left to UE implementation.

  - When a new Allowed NSSAI for a PLMN is received, the UE shall replace any stored Allowed NSSAI for this PLMN with this new Allowed NSSAI and any associated mapping;

- If received, a S-NSSAI permanently rejected in the PLMN shall be stored in the UE while RM-REGISTERED.
- If received, a S-NSSAI rejected in the current Registration Area shall be stored in the UE while RM-REGISTERED until the UE moves out of the current Registration Area.

NOTE 4: The storage aspects of rejected S-NSSAIs are described in TS 24.501 [47].

One or more S-NSSAIs in the Allowed NSSAI provided to the UE can have values, which are not part of the UE's slice configuration information for the Serving PLMN. In this case, the Allowed NSSAI is associated with mapping information regarding how of each S-NSSAI of the Allowed NSSAI to the S-NSSAI(s) of the Configured NSSAI for the HPLMN. This mapping allows the UE to associate for a given application the S-NSSAI as per NSSP of the URSP rules as defined in clause 6.6.2, TS 23.503 [45], with the corresponding S-NSSAI from the Allowed NSSAI.

5.15.4.2 Update of UE Network slicing configuration

At any time, the AMF may provide the UE with a new Configured NSSAI for the Serving PLMN, associated with mapping of the Configured NSSAI to the Configured NSSAI for the HPLMN. The AMF provides the new Configured NSSAI as specified in TS 23.502 [3], clause 4.2.4 UE Configuration Update procedure.

If the HPLMN is performing the configuration update, this will result in updates to Configured NSSAI for the HPLMN. AMF provides mapping information as specified in clause 5.15.4.1.

A UE for which the Configured NSSAI for the Serving PLMN has been updated and has deleted the stored Allowed NSSAI as described in clause 5.15.4.1 shall initiate a Registration procedure to receive a new valid Allowed NSSAI (see clause 5.15.5.2.1).

The update of URSP rules (which include the NSSP), if necessary, is described in TS 23.503 [45].

5.15.5 Detailed Operation Overview

5.15.5.1 General

The establishment of User Plane connectivity to a Data Network via a Network Slice instance(s) comprises two steps:

- performing a RM procedure to select an AMF that supports the required Network Slices.
- establishing one or more PDU Session to the required Data network via the Network Slice Instance(s).

5.15.5.2 Selection of a Serving AMF supporting the Network Slices

5.15.5.2.1 Registration to a set of Network Slices

When a UE registers with a PLMN, if the UE for this PLMN has a Configured NSSAI or an Allowed NSSAI, the UE shall provide to the network in RRC and NAS layer a Requested NSSAI containing the S-NSSAI(s) corresponding to the slice(s) to which the UE wishes to register, in addition to the 5G-S-TMSI if one was assigned to the UE.

The Requested NSSAI shall be one of:

- the Configured-NSSAI, or a subset thereof as described below, if the UE has no Allowed NSSAI for the serving PLMN; or
- the Allowed-NSSAI, or a subset thereof as described below, if the UE has an Allowed NSSAI for the serving PLMN; or
- the Allowed-NSSAI, or a subset thereof as described below, plus one or more S-NSSAIs from the Configured-NSSAI for which no corresponding S-NSSAI is present in the Allowed NSSAI and that were not previously rejected in the PLMN by the network.

The subset of Configured-NSSAI provided in the Requested NSSAI consists of one or more S-NSSAI(s) in the Configured NSSAI applicable to this PLMN, if the S-NSSAI was not previously rejected in the PLMN by the network.

The UE shall include the Requested NSSAI at RRC Connection Establishment and in NAS messages. However, the UE shall not indicate any NSSAI in RRC Connection Establishment or Initial NAS message unless it has a Configured NSSAI or Allowed NSSAI for the corresponding PLMN. The RAN shall route the NAS signalling between this UE and an AMF selected using the Requested NSSAI obtained during RRC Connection Establishment. If the RAN is unable to select an AMF based on the Requested NSSAI, it routes the NAS signalling to an AMF from a set of default AMFs. In the NAS signalling the UE provides the mapping of each S-NSSAI of the Requested NSSAI to the S-NSSAIs of the Configured NSSAI for the HPLMN.

When a UE registers with a PLMN, if for this PLMN the UE has not included a Requested NSSAI, the RAN shall route all NAS signalling from/to this UE to/from a default AMF. When receiving from the UE a Requested NSSAI and a 5G-S-TMSI in RRC, if the RAN can reach an AMF corresponding to the 5G-S-TMSI, then RAN forwards the request to this AMF. Otherwise, the RAN selects a suitable AMF based on the Requested NSSAI provided by the UE and forwards the request to the selected AMF. If the RAN is not able to select an AMF based on the Requested NSSAI, then the request is sent to a default AMF.

When the AMF selected by the AN receives the UE Initial Registration request:

- As part of the registration procedure described in TS 23.502 [3], clause 4.2.2.2.2, the AMF may query the UDM to retrieve UE subscription information including the Subscribed S-NSSAIs.
- The AMF verifies whether the S-NSSAI(s) in the Requested NSSAI are permitted based on the Subscribed S-NSSAIs (to identify the Subscribed S-NSSAIs the AMF may use the mapping to the S-NSSAI(s) of the Configured NSSAI for the HPLMN provided by the UE, in the NAS message, for each S-NSSAI of the Requested NSSAI).
- When the UE context in the AMF does not yet include an Allowed NSSAI, the AMF queries the NSSF (see (B) below for subsequent handling), except in the case when, based on configuration in this AMF, the AMF is allowed to determine whether it can serve the UE (see (A) below for subsequent handling).

NOTE 1: The configuration in the AMF depends on operator's policy.

- When the UE context in the AMF already includes an Allowed NSSAI, based on the configuration for this AMF, the AMF may be allowed to determine whether it can serve the UE (see (A) below for subsequent handling).

NOTE 2: The configuration in the AMF depends on the operator's policy.

(A) Depending on fulfilling the configuration as described above, the AMF may be allowed to determine whether it can serve the UE, and the following is performed:

- AMF checks whether it can serve all the S-NSSAI(s) from the Requested NSSAI present in the Subscribed S-NSSAIs (potentially using configuration for mapping S-NSSAI values between HPLMN and Serving PLMN), or all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in case no Requested NSSAI was provided (see clause 5.15.3).

  - If this is the case, the AMF remains the serving AMF for the UE. The Allowed NSSAI is then composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if no Requested NSSAI was provided, all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs (see (C) below for subsequent handling). It also determines the mapping if the S-NSSAI(s) included in the Allowed NSSAI needs to be mapped to Subscribed S-NSSAI(s) values.

  - If this is not the case, the AMF queries the NSSF (see (B) below).

(B) When required as described above, the AMF needs to query the NSSF, and the following is performed:

- The AMF queries the NSSF, with Requested NSSAI, mapping of Requested NSSAI to Configured NSSAI for the HPLMN, the Subscribed S-NSSAIs (with an indication if marked as default S-NSSAI), PLMN ID of the SUPI and UE's current Tracking Area(s).

NOTE: When more than one UE's Tracking Area is indicated, the UE is using more than one Access Type.

- Based on this information, local configuration, and other locally available information including RAN capabilities in the current Tracking Area for the UE, the NSSF does the following:

  - It verifies whether the S-NSSAI(s) in the Requested NSSAI are permitted based on the Subscribed S-NSSAIs and the mapping of Requested NSSAI to Configured NSSAI for the HPLMN.

  - It selects the Network Slice instance(s) to serve the UE. When multiple Network Slice instances in the UE's Tracking Areas are able to serve a given S-NSSAI, based on operator's configuration, the NSSF may select one of them to serve the UE, or the NSSF may defer the selection of the Network Slice instance until a NF/service within the Network Slice instance needs to be selected.

  - It determines the target AMF Set to be used to serve the UE, or, based on configuration, the list of candidate AMF(s), possibly after querying the NRF.

  - It determines the Allowed NSSAI, taking also into account the availability of the Network Slice instances as described in clause 5.15.8 that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas.

  - It also determines the mapping of each S-NSSAI of the Allowed NSSAI to the Subscribed S-SNSSAIs if necessary.

  - Based on operator configuration, the NSSF may determine the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s).

  - Additional processing to determine the Allowed NSSAI in roaming scenarios and the mapping to the Subscribed S-NSSAIs, as described in clause 5.15.6.

- The NSSF returns to the current AMF the Allowed NSSAI, the mapping if determined and the target AMF Set, or, based on configuration, the list of candidate AMF(s). The NSSF may return the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s), and the NRF to be used to determine the list of candidate AMF(s) from the AMF Set. The NSSF may return NSI ID(s) to be associated to the Network Slice instance(s) corresponding to certain S-NSSAIs. NSSF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1.

- Depending on the available information and based on configuration, the AMF may query the appropriate NRF (e.g. locally pre-configured or provided by the NSSF) with the target AMF Set. The NRF returns a list of candidate AMFs.

- If rerouting to a target serving AMF is necessary, the current AMF reroutes the Registration Request to a target serving AMF as described in clause 5.15.5.2.3.

(C) The serving AMF shall determine a Registration Area such that all S-NSSAIs of the Allowed NSSAI are available in all Tracking Areas of the Registration Area (and also considering other aspects as described in clause 5.3.2.3) and then return to the UE the Allowed NSSAI and the mapping of the Allowed NSSAI to the Subscribed S-NSSAIs if provided. The AMF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1.

Upon successful Registration, the UE is provided with a 5G-S-TMSI by the serving AMF. The UE shall include this 5G-S-TMSI in any RRC Connection Establishment during subsequent initial accesses to enable the RAN to route the NAS signalling between the UE and the appropriate AMF.

If the UE receives an Allowed NSSAI from the serving AMF, it shall store this new Allowed NSSAI and the associated mapping of the Allowed NSSAI to the Configured NSSAI for the HPLMN, if any, and override any previously stored Allowed NSSAI for this PLMN, as described in clause 5.15.4.1.

When no Requested NSSAI was included or when an S-NSSAI was rejected in the PLMN, the AMF may update the UE slice configuration information for the PLMN as described in clause 5.15.4.2.

5.15.5.2.2 Modification of the Set of Network Slice(s) for a UE

The set of Network Slices for a UE can be changed at any time while the UE is registered with a network, and may be initiated by the network, or by the UE, under certain conditions as described below.

The network, based on local policies, subscription changes and/or UE mobility, operational reasons (e.g. a Network Slice instance is no longer available), may change the set of Network Slice(s) to which the UE is registered and provide the UE new Allowed NSSAI. The network may perform such a change during a Registration procedure or trigger a notification towards the UE of the change of the Network Slices using a Generic UE Configuration Update procedure as specified in TS 23.502 [3], clause 4.2.4. The new Allowed NSSAI is determined as described in clause 5.15.5.2.1 (an AMF Re-allocation may be needed). The AMF provides the UE with the new Allowed NSSAI and TAI list, and:

- If the changes to the Allowed NSSAI do not require the UE to perform a registration procedure:
  - The AMF indicates that acknowledgement is required, but does not indicate the need to perform a registration procedure;
  - The UE responds with a UE configuration update complete message for the acknowledgement.
- If the changes to the Allowed NSSAI require the UE to perform a registration procedure (e.g. the new S-NSSAIs require a separate AMF that cannot be determined by the current serving AMF):
  - The serving AMF indicates to the UE that current 5G-GUTI is invalid and the need for the UE to perform a registration procedure after entering CM-IDLE state. The AMF shall release the NAS signalling connection to the UE to allow to enter CM-IDLE based on local policies (e.g. immediately or delayed release). The UE initiates a Registration procedure after the UE enters CM-IDLE state. The UE shall include the SUPI and a Requested NSSAI matching the Allowed NSSAI in the Registration Request message.

In addition to sending the new Allowed NSSAI to the UE, when a Network Slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies:

- If the Network Slice becomes no longer available under the same AMF (e.g. due to UE subscription change), the AMF indicates to the SMF(s) which PDU Session ID(s) corresponding to the relevant S-NSSAI shall be released. SMF releases the PDU Session according to clause 4.3.4.2 in TS 23.502 [3].
- If the Network Slice becomes no longer available upon a change of AMF (e.g. due to Registration Area change), the new AMF indicates to the old AMF that the PDU Session(s) corresponding to the relevant S-NSSAI shall be released. The old AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the new AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status in the Registration Accept message.

The UE uses UE Configuration (e.g. NSSP in the URSP rules) to determine whether ongoing traffic can be routed over existing PDU Sessions belonging to other Network Slices or establish new PDU Session(s) associated with same/other Network Slice.

In order to change the set of S-NSSAIs being used, the UE shall initiate a Registration procedure as specified in clause 5.15.5.2.1.

A change of the set of S-NSSAIs (whether UE or Network initiated) to which the UE is registered may, subject to operator policy, lead to AMF change, as described in clause 5.15.5.2.1.

5.15.5.2.3 AMF Re-allocation due to Network Slice(s) Support

During a Registration procedure in a PLMN, if the network decides that the UE should be served by a different AMF based on Network Slice(s) aspects, then the AMF that first received the Registration Request shall redirect the Registration request to another AMF via the RAN or via direct signalling between the initial AMF and the target AMF. The redirection message sent by the AMF via the RAN shall include information for selection of a new AMF to serve the UE.

For a UE that is already registered, the system shall support a redirection initiated by the network of a UE from its serving AMF to a target AMF due to Network Slice(s) considerations (e.g. the operator has changed the mapping between the Network Slice instances and their respective serving AMF(s)). Operator policy determines whether redirection between AMFs is allowed.

5.15.5.3 Establishing a PDU Session in a Network Slice

The establishment of a PDU Session in a Network Slice to a DN allows data transmission in a Network Slice. A PDU Session is associated to an S-NSSAI and a DNN. A UE that is registered in a PLMN and has obtained an Allowed NSSAI, shall indicate in the PDU Session Establishment procedure the S-NSSAI according to the NSSP in the URSP and, if available, the DNN the PDU Session is related to. The UE includes the appropriate S-NSSAI from the Allowed NSSAI and, if mapping of the Allowed NSSAI to the Configured NSSAI for the HPLMN was provided, an S-NSSAI with the corresponding value from the Configured NSSAI for the HPLMN.

If the URSP (which includes the NSSP) is not available in the UE, the UE shall not indicate any S-NSSAI in the PDU Session Establishment procedure.

The network operator (HPLMN) may provision the UE with Network Slice selection policy (NSSP) as part of the URSP rules, see clause 6.6.2, TS 23.503 [45]. The NSSP rules associate an application with one or more Subscribed S-NSSAI corresponding to the Subscribed S-NSSAIs of the UE. A default rule which matches all applications to a Subscribed S-NSSAI may also be included. When a UE application associated with a specific S-NSSAI requests data transmission,

- if the UE has one or more PDU Sessions established corresponding to the specific S-NSSAI, the UE routes the user data of this application in one of these PDU Sessions, unless other conditions in the UE prohibit the use of these PDU Sessions. If the application provides a DNN, then the UE considers also this DNN to determine which PDU Session to use. This is further described in clause 6.6.2, TS 23.503 [45].

The UE shall store the URSP rules, including the NSSP, as described in TS 23.503 [45]..

If the UE does not have a PDU Session established with this specific S-NSSAI, the UE requests a new PDU Session corresponding to this S-NSSAI and with the DNN that may be provided by the application. In order for the RAN to select a proper resource for supporting network slicing in the RAN, RAN needs to be aware of the Network Slices used by the UE. This is further described in clause 6.6.2, TS 23.503 [45].

If the AMF is not able to determine the appropriate NRF to query for the S-NSSAI provided by the UE, the AMF may query the NSSF with this specific S-NSSAI, location information, PLMN ID of the SUPI. The NSSF determines and returns the appropriate NRF to be used to select NFs/services within the selected Network Slice instance. The NSSF may also return an NSI ID identifying the Network Slice instance to use for this S-NSSAI.

SMF discovery and selection within the selected Network Slice instance is initiated by the AMF when a SM message to establish a PDU Session is received from the UE. The appropriate NRF is used to assist the discovery and selection tasks of the required network functions for the selected Network Slice instance.

The AMF queries the appropriate NRF to select an SMF in a Network Slice instance based on S-NSSAI, DNN, NSI-ID (if available) and other information e.g. UE subscription and local operator policies, when the UE triggers the establishment of a PDU Session. The selected SMF establishes a PDU Session based on S-NSSAI and DNN.

When the AMF belongs to multiple Network Slices, based on configuration, the AMF may use an NRF at the appropriate level for the SMF selection.

For further details on the SMF selection, refer to clause 4.3.2.2.3 in TS 23.502 [3].

When a PDU Session for a given S-NSSAI is established using a specific Network Slice instance, the CN provides to the (R)AN the S-NSSAI corresponding to this Network Slice instance to enable the RAN to perform access specific functions.

5.15.6 Network Slicing Support for Roaming

For roaming scenarios:

- If the UE only uses standard S-NSSAI values, then the same S-NSSAI values can be used in VPLMN as in the HPLMN.
- If the VPLMN and HPLMN have an SLA to support non-standard S-NSSAI values in the VPLMN, the NSSF of the VPLMN maps the Subscribed S-NSSAIs values to the respective S-NSSAI values to be used in the VPLMN. The S-NSSAI values to be used in the VPLMN are determined by the NSSF of the VPLMN based on the SLA. The NSSF of the VPLMN need not inform the HPLMN of which values are used in the VPLMN.

  Depending on operator's policy and the configuration in the AMF, the AMF may decide the S-NSSAI values to be used in the VPLMN and the mapping to the Subscribed S-NSSAIs.
- The UE constructs Requested NSSAI as described in clause 5.15.5.2.1. The mapping of each S-NSSAI of the Requested NSSAI to the S-NSSAIs of the Configured NSSAI for the HPLMN.
- The NSSF in the VPLMN determines the Allowed NSSAI without interacting with the HPLMN.
- The Allowed NSSAI in the Registration Accept includes S-NSSAI values used in the VPLMN. The mapping information described above is also provided to the UE with the Allowed NSSAI as described in clause 5.15.4.
- In PDU Session Establishment procedures, the UE includes a Subscribed S-NSSAI based on the NSSP in the URSP rules (an S-NSSAI with a value defined by the HPLMN), and the related (mapped) S-NSSAI from the Allowed NSSAI (an S-NSSAI with a value defined by the VPLMN) based on the mapping of the Allowed NSSAI to the Configured NSSAI for the HPLMN. For the home routed case, the V-SMF send the PDU Session Establishment Request message to the H-SMF along with the S-NSSAI with the value from the HPLMN.
- When a PDU Session is established, the CN provides to the AN the S-NSSAI with the value from the VPLMN corresponding to this PDU Session, as described in clause 5.15.5.3.
- The Network Slice instance specific network functions in the VPLMN are selected by the VPLMN by using the S-NSSAI with the value from the VPLMN and querying an NRF that has either been pre-configured, or provided by the NSSF in the VPLMN. The Network Slice specific functions of the HPLMN (if applicable) are selected by the VPLMN by using the related S-NSSAI with the value from the HPLMN via the support from an appropriate NRF in the HPLMN, identified as specified in clause 4.17.5 of TS 23.502 [3] and, for SMF in clause 4.3.2.2.3.3 of TS 23.502 [3].

5.15.7 Network slicing and Interworking with EPS

5.15.7.1 General

A 5GC which supports Network Slicing might need to interwork with the EPS in its PLMN or in other PLMNs.The EPC may support the Dedicated Core Networks (DCN). In some deployments, the MME selection may be assisted by a DCN-ID provided by the UE to the RAN (see TS 23.401 [26]).

Mobility between 5GC to EPC does not guarantee all active PDU Session(s) can be transferred to the EPC.

During PDN connection establishment in the EPC, the UE allocates the PDU Session ID and sends it to the PGW-C+SMF via PCO. An S-NSSAI associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF, e.g. based on a combination of PGW-C+SMF address and APN, and is sent to the UE in PCO. The UE stores this S-NSSAI associated with the PDN connection.

5.15.7.2 IDLE Mode aspects

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking with N26:

- When UE moves from 5GS to EPS, the MM context information sent by AMF to MME includes the UE Usage type, which is retrieved from UDM by AMF as part of subscription data.
- When UE moves from EPS to 5GS, then the UE includes the S-NSSAIs associated with the established PDN connections in the Requested NSSAI in RRC and NAS. The UE also includes the list of PDU session IDs and

related S-NSSAIs in the Registration request. In the home-routed roaming case, the AMF selects V-SMFs based on the S-NSSAIs received from the UE.

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking without N26:

- The UE includes the S-NSSAI received from PGW-C/SMF when moving PDN connections to 5GC using PDU Session Establishment Request.

5.15.7.3 CONNECTED Mode aspects

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking with N26:

- When a UE is CM-CONNECTED in 5GC and a handover to EPS occur, the AMF selects the target MME based on the source AMF Region ID, AMF Set ID and target location information. The AMF forwards the UE context to the selected MME over the N26 Interface. The handover procedure is executed as documented in TS 23.502 [3]. When the Handover completes the UE performs a Tracking Area Update. This completes the UE registration in the target EPS. As part of this the UE obtains a DCN-ID if the target EPS uses it.
- When a UE is ECM-CONNECTED in EPC, and performs a handover to 5GS, the MME selects the target AMF based on target location information, e.g. TAI and any other available local information (including the UE Usage Type if one is available for the UE in the subscription data) and forwards the UE context to the selected AMF over the N26 interface. In the home-routed roaming case, the AMF selects default V-SMFs. The handover procedure is executed as documented in TS 23.502 [3]. When the Handover completes the UE performs a Registration procedure including the list of PDU session IDs and related S-NSSAIs. The AMF may select a different AMF as specified in clause 4.2.2.2.3 in TS 23.502 [3]. This completes the UE registration in the target 5GS and as part of this the UE obtains an Allowed NSSAI.

5.15.8 Configuration of Network Slice availability in a PLMN

A Network Slice may be available in the whole PLMN or in one or more Tracking Areas of the PLMN.

The availability of a Network Slice refers to the support of the NSSAI in the involved NFs. In addition, policies in the NSSF may further restrict from using certain Network Slices in a particular TA, e.g. depending on the HPLMN of the UE.

The availability of a Network Slice in a TA is established end-to-end using a combination of OAM and signalling among network functions. It is derived by using the S-NSSAIs supported per TA in NG-RAN, the S-NSSAIs supported in the AMF and operator policies per TA in the NSSF.

The AMF learns the S-NSSAIs supported per TA by the NG-RAN when the NG-RAN nodes establish or update the N2 connection with the AMF (see TS 38.413 [34]) and TS 38.300 [27]). One or all AMF per AMF Set provides and updates the NSSF the with the S-NSSAIs support per TA. The NG-RAN learns the S-NSSAIs the AMFs it connects to support when the NG-RAN nodes establishes the NG2 connection with the AMF or when the AMF updates the N2 connection with the NG-RAN (see TS 38.413 [34] and TS 38.300 [27]).

The NSSF may be configured with operator policies specifying under what conditions the S-NSSAIs can be restricted per TA and per HPLMN of the UE.

The per TA restricted S-NSSAIs may be provided to the AMFs of the AMF Sets at setup of the network and whenever changed.

The AMF may be configured for the S-NSSAIs it supports with operator policies specifying any restriction per TA and per HPLMN of the UE.

5.16 Support for specific services

5.16.1 Public Warning System

The functional description for supporting Public Warning System for 5G System can be found in TS 23.041 [46].

5.16.2 SMS over NAS

5.16.2.1 General

This clause includes feature description for supporting SMS over NAS in 5G System. Support for SMS incurs the following functionality:

- Support for SMS over NAS transport between UE and AMF. This applies to both 3GPP and Non 3GPP accesses.
- Support for AMF determining the SMSF for a given UE.
- Support for subscription checking and actual transmission of MO/MT-SMS transfer by the SMSF.
- Support for MO/MT-SMS transmission for both roaming and non-roaming scenarios.
- Support for selecting proper domains for MT SMS message delivery including initial delivery and re-attempting in other domains.

5.16.2.2 SMS over NAS transport

During registration procedure, a UE that wants to use SMS provides an "SMS supported" indication over NAS signalling indicating the UE's capability for SMS over NAS transport. "SMS supported" indication indicates whether UE can support SMS delivery over NAS via 3GPP access or via both 3GPP and non-3GPP access. If the core network supports SMS functionality, the AMF includes "SMS supported" indication to the UE, and whether SMS delivery over NAS via 3GPP access or via both the 3GPP and non-3GPP access is accepted by the network.

SMS is transported over NAS without the need to establish data radio bearers, via NAS transport message, which can carry SMS messages as payload.

5.16.3 IMS support

5.16.3.1 General

IP-Connectivity Access Network specific concepts when using 5GS to access IMS can be found in TS 23.228 [15].

5GS supports IMS with the following functionality:

- Indication toward the UE if IMS voice over PS session is supported.
- Capability to transport the P-CSCF address(es) to UE.
- Paging Policy Differentiation for IMS as defined in TS 23.228 [15].
- IMS emergency service as defined in TS 23.167 [18].
- Domain selection for UE originating sessions.
- Terminating domain selection for IMS voice.

5.16.3.2 IMS voice over PS Session Supported Indication over 3GPP access

The serving PLMN AMF shall send an indication toward the UE during the Registration procedure over 3GPP access to indicate if an IMS voice over PS session is supported or not supported. A UE with "IMS voice over PS" voice capability over 3GPP access should take this indication into account when performing voice domain selection, as described in clause 5.16.3.5.

The serving PLMN AMF may only indicate IMS voice over PS session supported over 3GPP access in one of the following cases:

- If the network is able to provide a successful IMS voice over PS session in the current Registration Area with a 5G QoS Flow that supports voice as specified in clause 5.7.

- If the network is not able to provide a successful IMS voice over PS session over NR connected to 5GC, but is able for one of the following:
    - If E-UTRA connected to 5GC supports voice, and the NG-RAN supports a handover to E-UTRA connected to 5GC for this UE at QoS Flow establishment for voice; or
    - If the UE supports HO to EPS, the EPS supports voice, and the NG-RAN supports a handover to EPS for this UE at QoS Flow establishment for voice.

The serving PLMN provides this indication based e.g. on local policy, HPLMN and how extended NG-RAN coverage is. The AMF in serving PLMN shall indicate that IMS voice over PS is not supported if serving PLMN does not have an IMS roaming agreement with HPLMN. This indication is per Registration Area.

Editor's note: If interactions between the AMF and RAN to determine functionality equivalent to Voice Support Match Indicator of EPC are needed, they are FFS.

5.16.3.2a IMS voice over PS Session Supported Indication over non-3GPP access

The serving PLMN AMF shall send an indication toward the UE during the Registration procedure over non-3GPP access to indicate whether an IMS voice over PS session is supported or not supported via non-3GPP access. A UE with "IMS voice over PS" voice capability over non-3GPP access should take this indication into account when performing the selection between N3IWF and ePDG described in clause 6.3.6.

The serving PLMN AMF may only indicate IMS voice over PS session supported over non-3GPP access if the network is able to provide a successful IMS voice over PS session over N3IWF connected to 5GC with a 5G QoS Flow that supports voice as specified in clause 5.7.

5.16.3.3 Homogeneous support for IMS voice over PS Session supported indication

5GC shall support the usage of "Homogeneous Support of IMS Voice over PS Sessions" indication between AMF and UDM.

When the AMF initiates Update Location procedure to the UDM, it shall:

- if "IMS Voice over PS Sessions" is supported homogeneously in all TAs in the serving AMF for the UE, include the "Homogeneous Support of IMS Voice over PS Sessions" indication set to "Supported";
- if none of the TAs of the serving AMF supports "IMS Voice over PS Sessions" for the UE, include the "Homogeneous Support of IMS Voice over PS Sessions" indication set to "Not supported";
- if "IMS Voice over PS Sessions" support is either non-homogeneous or unknown, not include the "Homogeneous Support of IMS Voice over PS Sessions" indication.

The UDM shall take this indication into account when doing T-ADS procedure for IMS voice.

5.16.3.4 P-CSCF address delivery

At PDU Session Establishment procedure related to IMS, SMF shall support the capability to send the P-CSCF address(es) to UE. The SMF is located in VPLMN if LBO is used. This is sent by visited SMF if LBO is used. For Home routed, this information is sent by the SMF in HPLMN. P-CSCF address(es) shall be sent transparently through AMF, and in case of Home Routed also through the SMF in VPLMN.

NOTE 1: Other options to provide P-CSCF to the UE as defined in TS 23.228 [15] is not excluded.

NOTE 2: PDU Session for IMS is identified by "APN" or "DNN".

5.16.3.5 Domain selection for UE originating sessions / calls

For UE originating calls, the 5GC capable UE performs access domain selection. The UE shall be able to take following factors into account for access domain selection decision:

- The state of the UE in the IMS. The state information shall include: Registered, Unregistered.
- The "IMS voice over PS session supported indication" as defined in clause 5.16.3.2.

- Whether the UE is expected to behave in a "voice centric" or "data centric" way for 5GS.
- UE capability of supporting IMS PS voice.
- UE capability for operating in dual-registration mode with selective PDU Session transfer as defined in clause 5.17.2.3.3.

To allow for appropriate domain selection for originating voice calls, the UE shall attempt initial registration in 5GC. If the UE fails to use IMS for voice, e.g. due to "IMS voice over PS session supported indication" indicates voice is not supported in 5G System, the UE behaves as described below for "voice centric" for 5GS or "data centric" for 5GS:

- A UE set to "voice centric" for 5GS shall always try to ensure that Voice service is possible. A voice centric 5GC capable and EPC capable UE unable to obtain voice service in 5GS shall not select a cell connected only to 5GC. By disabling capabilities to access 5GS, the UE re-selects to E-UTRAN connected to EPC first (if available). When the UE selects E-UTRAN connected to EPC, the UE performs Voice Domain Selection procedures as defined in TS 23.221 [23].
- A UE set to "data centric" for 5GS does not need to perform any reselection if voice services cannot be obtained.

NOTE: The related radio capabilities in order for the voice centric UE to not reselect to NR or E-UTRA cell connected to 5GC (i.e. avoid ping pong) will be defined by RAN WGs.

5.16.3.6 Terminating domain selection for IMS voice

When requested by IMS, the UDM/HSS shall be able to query the serving AMF for T-ADS related information.

The AMF shall respond to the query with the following information unless the UE is detached:

- whether or not IMS voice over PS Session is supported in the registration area (s) where the UE is currently registered;
- the time of the last radio contact with the UE; and
- the current Access Type and RAT type.

5.16.3.7 UE's usage setting

If the UE is configured to support IMS voice, the UE shall include the information element "UE's usage setting" in Registration Update Request messages. The UE's usage setting indicates whether the UE behaves in a "voice centric" or "data centric" way (as defined in clause 5.16.3.5).

NOTE: Depending on operator's configuration, the UE's usage setting can be used by the network to choose the RFSP Index in use (see clause 5.3.4.3). As an example, this enables the enforcement of selective idle mode camping over E-UTRA for voice centric UEs.

5.16.3.8 Domain Selection for UE originating SMS

To allow for appropriate domain selection for SMS delivery, the following applies for an IMS capable UE which supports SMS over IP networks:

- It should be possible to provision UEs with the following HPLMN operator preferences on how an IMS enabled UE is supposed to handle SMS services:
  - SMS is not to be invoked over IP networks: the UE does not attempt to deliver SMS over IP networks. The UE attempts to deliver SMS over NAS signalling.
  - SMS is preferred to be invoked over IP networks: the UE attempts to deliver SMS over IP networks. If delivery of SMS over IP networks is not available, the UE attempts to deliver SMS over NAS signalling.
- It should be possible to provision UEs with the following HPLMN operator preferences on access selection for delivering SMS over NAS signalling:
  - SMS is preferred to be invoked over 3GPP access for NAS transport: the UE attempts to deliver SMS over NAS via 3GPP access if UE both registered in 3GPP access and non-3GPP access.

- SMS is preferred to be invoked over non-3GPP access for NAS transport: the UE attempts to deliver SMS over NAS via non-3GPP access if UE both registered in 3GPP access and non-3GPP access. If delivery of SMS over NAS via non-3GPP access is not available, the UE attempts to deliver SMS over NAS via 3GPP access.

5.16.4 Emergency services

5.16.4.1 Introduction

Emergency services are provided to support IMS emergency sessions. Emergency services refers to functionalities provided by the serving network when the network is configured to support emergency services. Emergency services are provided to normal registered UEs and depending on local regulation, to emergency registered UEs i.e. that are in limited service state. Receiving emergency services in limited service state does not require a valid subscription. Depending on local regulation and an operator's policy, the network may allow or reject an emergency registration request for UEs that have been identified to be in limited service state. Four different behaviours of emergency services as identified in TS 23.401 [26] clause 4.3.12.1 is supported.

To provide emergency services, the AMF is configured with Emergency Configuration Data that are applied to emergency services that are established by an AMF based on request from the UE. The AMF Emergency Configuration Data contains the Emergency DNN which is used to derive an SMF. In addition, the AMF Emergency Configuration Data may contain the statically configured SMF for the Emergency DNN. The SMF may also store Emergency Configuration Data that contains statically configured UPF information for the Emergency DNN.

The UE shall not issue an emergency session over untrusted Non-3GPP access to 5GC if the emergency session can be established via 3GPP access. To get 5GC access for emergency services in case of untrusted Non-3GPP access, the UE may select any N3IWF as specified in clause 6.3.6.

When the UE is camped normally in the cell, during Registration procedure described in TS 23.502 [3] clause 4.2.2.2, the serving AMF includes an indication for Emergency Services Support within the Registration Accept to the UE. The Emergency Services Support indication is valid within the current Registration Area per RAT (i.e. this is to cover cases when the same registration area supports multiple RATs and they have different capability).

The Emergency Services Support is configured in the AMF according to local regulations and network capabilities. AMF includes Emergency Services Support indicator in the Registration Area Accept message to indicate whether the UE can setup emergency PDU session or UE should perform Service Request as defined in clause 5.16.4.11.

Editor's note: need for per RAT indicated will need to be confirmed.

The 5GS includes Emergency Services Support indicator if any of the following conditions are true:

- the Network is able to support Emergency Services natively over 5GS;
- E-UTRA connected to 5GC supports IMS Emergency (e.g. voice) Services, and the NG-RAN is able to trigger handover to E-UTRA connected to 5GC at QoS Flow establishment for IMS Emergency Services (e.g. voice);
- NG-RAN is able to trigger handover to EPS at QoS Flow establishment for IMS Emergency Services (e.g. voice); or
- NG-RAN triggers redirection to EPS at QoS Flow establishment for IMS Emergency Services (e.g. voice).

The 5GS includes an indication that it can support Emergency Services Support using fallback when it can trigger fallback for emergency services (as defined in clause 5.16.4.11) to a RAT or System where Emergency Services are supported natively.

If a certain RAT is restricted for Emergency, AMF signals that the corresponding RAT is restricted for Emergency Services Support to the Master RAN Node. This helps assist the Master RAN node determine whether to set up Dual Connectivity for Emergency Services.

UEs that are in limited service state, as specified in TS 23.122 [17], initiate the Registration procedure by indicating that the registration is to receive emergency services, referred to as emergency registration, and a Follow-on request is included in the Registration Request to initiate PDU Session Establishment procedure with a Request Type indicating "Emergency Request". UEs that had registered for normal services and do not have emergency PDU Sessions established and the UE is subject to Mobility Restriction in the present area or RAT (e.g. because of restricted tracking area) shall initiate the UE Requested PDU Session Establishment procedure to receive emergency services. Based on local regulation, the network supporting emergency services for UEs in limited service state provides emergency services to these UE, regardless whether the UE can be authenticated, has roaming or Mobility Restrictions or a valid subscription. For emergency services over 3GPP access, other than eCall over IMS, the UEs in limited service state determine that the cell supports emergency services over NG-RAN from a broadcast indicator in AS. For emergency services over untrusted non-3GPP access, other than eCall over IMS, the UE in limited service selects a any N3IWF as specified in clause 6.3.6. Emergency calls for eCall Over IMS are only performed if the UE has a USIM.

UE is considered to be emergency registered if it has only PDU Sessions for emergency services.

A serving network shall provide the RAN with an Access Stratum broadcast indication to UEs as to whether eCall Over IMS is supported. A UE that is not in limited service state determines that the cell supports eCall Over IMS using the broadcast indicator for eCall over IMS. Emergency calls for eCall Over IMS are not supported over non-3GPP access.

NOTE 1: The Access Stratum broadcast indicator is determined according to operator policies and minimally indicates that the PLMN, or all of the PLMNs in the case of network sharing, and at least one emergency center or PSAP to which an eCall Over IMS can be routed, support eCall Over IMS.

A UE in limited service state determines that the cell supports eCall Over IMS using both the broadcast indicator for support of emergency services over NG-RAN and the broadcast indicator for eCall over IMS. Emergency calls for eCall Over IMS are not supported over Non-3GPP access.

NOTE 2: The broadcast indicator for eCall Over IMS does not indicate whether UEs in limited service state are supported. So, the broadcast indicator for support of emergency services over NG-RAN that indicates limited service state support needs to be applied in addition.

For a UE that is Emergency Registered, if it is unauthenticated the security context is not set up on UE.

UEs that camp normally on a cell and in RM-DEREGISTERED state, (i.e. without any conditions that result in limited service state) or that decide to access 5GC via untrusted non-3GPP access, initiate the normal initial Registration procedure. Upon successful normal registration (i.e. not emergency registration), such UEs shall initiate the UE Requested PDU Session Establishment procedure to receive emergency services if the AMF indicated support for Emergency Services in 5GC by setting Emergency Services Support indicator to YES for the RAT the UE is currently camped. The UEs that camp normally on a cell or that are connected via untrusted Non-3GPP access are informed that the PLMN supports emergency services over 5G-AN from the Emergency Service Support indicator in the Registration procedure. This applies to both 3GPP and non-3GPP accesses.

NOTE 3: The Emergency Service Support indicator in the Registration procedures does not indicate support for eCall Over IMS.

For a UE that is Emergency Registered, normal PLMN selection principles apply after the end of the IMS emergency session.

For emergency services, there is no support for inter PLMN mobility thus there is a risk of service disruption due to failed inter PLMN mobility attempts.

The UE shall set the RRC establishment cause to emergency as defined in TS 38.331 [28] when it requests an RRC connection in relation to an emergency session.

When a PLMN supports IMS and emergency services:

- all AMFs in that PLMN shall have the capability to support emergency services.
- at least one SMF shall have this capability.

For other emergency scenarios (e.g. UE autonomous selection for initiating emergency services), refer to TS 23.167 [18] for domain selection principles.

5.16.4.2 Architecture Reference Model for Emergency Services

According to clause 4.2, the non-roaming architectures (Figure 4.2.3-1 and Figure 4.2.3-2) and roaming architecture with the visited operator's application function (Figure 4.2.4-1 and Figure 4.2.4-4) apply for emergency services. The other non-roaming and roaming architectures with services provided by the home network do not apply for emergency services.

5.16.4.3 Mobility Restrictions and Access Restrictions for Emergency Services

When Emergency Services are supported and local regulation requires IMS Emergency Sessions to be provided regardless of the Mobility Restrictions (see clause 5.3.4.1), or access should not be applied to UEs receiving emergency services. When the (R)AN resources for emergency services are established, the ARP value for emergency services indicates the usage for emergency services to the 5G-AN.

During handovers, the source NG-RAN and source AMF ignore any UE related restrictions during handover evaluation when there is an active PDU Session associated with emergency service.

During Mobility Registration Update procedures, including a registration update as part of a handover, the target AMF ignores any Mobility or Restrictions or access restrictions for UE with emergency services where required by local regulation. Any non-emergency services are not allowed, by the target network when not allowed by the subscription for the target location. Such UEs with only emergency PDU Sessions behave as emergency registered. To allow the emergency registered UE to get access to normal services after the emergency session has ended and when it has moved to a new area that is not stored by the UE as a forbidden area, after allowing a period of time for subsequent emergency services, the UE may explicitly deregister and register to normal services without waiting for the emergency PDU Session release by the SMF.

This functionality applies to all mobility procedures.

5.16.4.4 Reachability Management

An emergency registered UE over 3GPP access when its periodic registration update timer expires shall not initiate a periodic registration update procedure but enter RM-DEREGISTERED state. For emergency registered UEs over 3GPP access, the AMF runs a mobile reachable timer with a similar value to the UE's periodic registration update timer. After expiry of this timer the AMF may change the UE RM state in the AMF, for 3GPP case of an emergency registered UE to RM-DEREGISTERED. The AMF assigns the periodic registration update timer value to emergency registered UE. This timer keeps the UE emergency registered after change to CM-IDLE state to allow for a subsequent emergency service without a need for emergency registration again.

For emergency registered UEs on untrusted Non-3GPP access, the UE is only reachable in CM-CONNECTED state: since the UE has initiated an emergency registration over untrusted Non-3GPP access only when it is not possible over 3GPP access, 3GPP access is assumed to be unavailable for paging the UE.

5.16.4.5 SMF and UPF selection function for Emergency Services

When a SMF is selected for emergency services, the SMF selection function described in clause 6.3.2 for normal services is applied to the Emergency DNN or the AMF selects the SMF directly from the AMF Emergency Configuration Data. If the SMF selection function described in clause 6.3.2 is used it shall always derive a SMF in the visited PLMN, which guarantees that the IP address is also allocated by the visited PLMN. When a UPF is selected for emergency services, the UPF selection function described in clause 6.3.3 for normal services is applied to the Emergency DNN or the SMF selects the UPF directly from the SMF Emergency Configuration Data. The information in the AMF Emergency Configuration Data and the SMF Emergency Configuration Data is specified in clause 5.16.4.1.

5.16.4.6 QoS for Emergency Services

Local regulation may require supporting emergency calls from an unauthorised UE. In such a case, the SMF may not have subscription data. Additionally, the local network may want to provide emergency services support differently than what is allowed by a UE subscription. Therefore, the initial QoS parameters used for establishing emergency services are configured in the V-SMF (local network) in the SMF Emergency Configuration Data.

This functionality is used by the UE Requested PDU Session Establishment procedure when establishing emergency services.

5.16.4.7 PCC for Emergency Services

Dynamic PCC is used for UEs establishing emergency service and shall be used to manage IMS emergency sessions when an operator allows IMS emergency sessions. When establishing emergency services with a SMF, the PCF provides the SMF with the QoS parameters, including an ARP value reserved for the emergency services to prioritize the QoS Flows when performing admission control, as defined in TS 23.503 [45].

The PCF rejects an IMS session established via the emergency PDU Session if the AF (i.e. P-CSCF) does not provide an emergency indication to the PCF.

5.16.4.8 IP Address Allocation

Emergency service is provided by the serving PLMN. The UE and serving PLMN must have compatible IP address versions in order for the UE to obtain a local emergency PDU Session.

5.16.4.9 Handling of PDU Sessions for Emergency Services

The QoS Flows of a PDU Session associated with the emergency DNN shall be dedicated for IMS emergency sessions and shall not allow any other type of traffic. The emergency contexts shall not be changed to non-emergency contexts and vice versa. The UPF shall block any traffic that is not from or to addresses of network functions (e.g. P-CSCF) providing emergency services. If there is already an emergency PDU Session, the UE shall not request another emergency PDU Session. The network shall reject any additional emergency PDU Session requests. The UE shall not request any PDU Session modification for the emergency PDU Session. The network shall reject any UE requested PDU Session modification that is for the emergency PDU Session. The ARP reserved for emergency service shall only be assigned to QoS Flows associated with an emergency PDU Session.

Editor's note: How the 5GC reacts to existing services via normal registration, and how new services via normal registration operate when an Emergency Registration has occurred is FFS.

5.16.4.10 Support of eCall Only Mode

For service requirements for eCall only mode, refer to TS 22.101 [33].

A UE configured for eCall Only Mode shall remain in RM-DEREGISTERED state, shall camp on a network cell when available but shall refrain from any Registration Management, Connection Management or other signalling with the network. The UE may instigate Registration Management and Connection Management procedures in order to establish, maintain and release an eCall Over IMS session or a session to any non-emergency MSISDN(s) or URI(s) configured in the USIM for test and/or terminal reconfiguration services. Following the release of either session, the UE starts a timer whose value depends on the type of session (i.e. whether eCall or a session to a non-emergency MSISDN or URI for test/reconfiguration). While the timer is running, the UE shall perform normal RM/CM procedures and is permitted to respond to paging to accept and establish an incoming session (e.g. from an emergency centre, PSAP or HPLMN operator). When the timer expires, the UE shall perform a UE-initiated deregistration procedure if still registered and enter RM-DEREGISTERED state.

NOTE 1: An HPLMN operator can change the eCall Only Mode configuration state of a UE in the USIM. An HPLMN operator can also instead add, modify or remove a non-emergency MSISDN or URI in the USIM for test and/or terminal reconfiguration services. This can occur following a UE call to a non-emergency MSISDN or URI configured for reconfiguration. When the eCall Only Mode configuration is removed, the UE operates as a normal UE that can support eCall over IMS.

NOTE 2: A test call and a reconfiguration call can be seen as normal (non-emergency) call by a serving PLMN and normal charging rules can apply depending on operator policy.

NOTE 3: An MSISDN configured in the USIM for test and/or terminal reconfiguration services for eCall Over IMS can differ from an MSISDN configured in the USIM for test services for eCall over the CS domain.

5.16.4.11 Emergency services fallback

In order to support various deployment scenarios for obtaining Emergency Services, the UE and 5GC may support the mechanism to direct or redirect the UE either towards E-UTRA connected to 5GC (RAT fallback) when only NR does not support Emergency Services or towards EPS (E-UTRAN connected to EPC System fallback) when the 5GC does not support Emergency Services.

Following principles apply for Emergency Services Fallback:

- If the AMF indicates support for Emergency services using fallback in the Registration Accept message, then in order to initiate Emergency Service, normally registered UE supporting Emergency Services fallback shall initiate a Service Request with Service Type set to Emergency as defined in TS 23.502 [3] clause 4.13.4.1.

- AMF uses the Service Type Indication within the Service Request to redirect the UE towards the appropriate RAT/System. The 5GS may, for emergency services, trigger one of the following procedures:
  - Redirection to EPS.
  - Redirection to E-UTRA connected to 5GC.
- After receiving the Service Request for Emergency Fallback, the AMF triggers N2 procedure resulting in either CONNECTED state mobility (Handover procedure) or IDLE state mobility (redirection) to either E-UTRA/5GC or to E-UTRAN/EPC depending on factors such as N26 availability, network configuration and radio conditions.

5.16.5 Multimedia Priority Services

TS 22.153 [24] specifies the service requirements for Multimedia Priority Service (MPS). MPS allows certain subscribers (i.e. Service Users as per TS 22.153 [24]) priority access to system resources in situations such as during congestion, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials and/or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis.

MPS is based on the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions. MPS is supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

NOTE 1: If a session terminates on a server in the Internet (e.g. web-based service), then the remote end and the Internet transport are out of scope for this specification.

A Service User may use an MPS-subscribed UE or any other UE to obtain MPS. An MPS-subscribed UE obtains priority access to the Radio Access Network by using the Access Class Barring mechanism according to TS 22.011 [25]. This mechanism provides preferential access to UEs based on its assigned Access Class. If an MPS-subscribed UE belongs to one of the special access classes as defined in TS 22.011 [25], the UE has preferential access to the network compared to ordinary UEs in periods of congestion.

MPS subscription allows users to receive priority services, if the network supports MPS. MPS subscription entitles a USIM with special Access Class(es). MPS subscription includes indication for support of priority PDU connectivity service and IMS priority service support for the end user. Priority level regarding QoS Flows and IMS are also part of the MPS subscription information. The usage of priority level is defined in TS 22.153 [24], TS 23.203 [4] and TS 23.228 [15].

NOTE 2: The term "Priority PDU connectivity services" is used to refer to 5G System functionality that corresponds to the functionality as provided by LTE/EPC Priority EPS bearer services in clause 4.3.18.3 of TS 23.401 [26].

MPS includes signalling priority and media priority. All MPS-subscribed UEs get priority for QoS Flows (e.g., used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by setting MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers or not, based on regional/national regulatory requirements. On Demand service is based on Service User invocation/revocation explicitly and applied to the media QoS Flows being established. When not On Demand MPS service does not require invocation, and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

NOTE 3: According to regional/national regulatory requirements and operator policy, On-Demand MPS Service Users can be assigned the highest priority.

Priority treatment is applicable to IMS based multimedia services and priority PDU connectivity service.

Priority treatment for MPS includes priority message handling, including priority treatment during authentication, security, and Mobility Management procedures.

Priority treatment for MPS session requires appropriate ARP and 5QI (plus 5G QoS characteristics) setting for QoS Flows according to the operator's policy.

NOTE 4: Use of QoS Flows for MPS with QoS characteristics signalled as part of QoS profile enables the flexible assignment of 5G QoS characteristics (e.g. priority level) for MPS.

When an MPS session is requested by a Service User, the following principles apply in the network:

- QoS Flows employed in an MPS session shall be assigned ARP value settings appropriate for the priority level of the Service User.

- Setting ARP pre-emption capability and vulnerability for MPS QoS Flows, subject to operator policies and depending on national/regional regulatory requirements.

- Pre-emption of non-Service Users over Service Users during network congestion situation, subject to operator policy and national/regional regulations.

The terminating network identifies the priority of the MPS session and applies priority treatment, including paging with priority, to ensure that the MPS session can be established with priority to the terminating user (either a Service User or normal user).

MPS priority mechanisms can be classified as subscription-related, invocation-related, and those applied to existing QoS Flows. Subscription related mechanisms, as described in clause 5.22.1, are further divided into two groups: those which are always applied and those which are conditionally applied. Invocation-related mechanisms, as described in clause 5.22.2, are further divided into three groups: those that apply for mobile originated SIP call/sessions, those that apply for mobile terminated SIP call/sessions, and those that apply for the Priority PDU connectivity services. Methods applied to existing QoS Flows focus on handover and congestion control and are described in clause 5.22.3.

5.16.6 Mission Critical Services

According to TS 23.280 [37], a Mission Critical Service (MCX) is a communication service reflecting enabling capabilities Mission Critical Applications and provided to end users from Mission Critical Organizations and mission critical applications for other businesses and organizations (e.g. utilities, railways). An MCX Service is either Mission Critical Push To Talk (MCPTT) as defined in TS 23.379 [38], Mission Critical Video (MCVideo) as defined in TS 23.281 [39], or Mission Critical Data (MCData) as defined in TS 23.282 [40] and represents a shared underlying set of requirements between two or more MCX service types.

MCX Services are based on the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions. As specified in TS 22.261 [2] clause 6.8, MCX Users require 5GS functionality that allows for real-time, dynamic, secure and limited interaction with the QoS and policy framework for modification of the QoS and policy framework by authorized users. The limited interaction is based on operator policy, and provides specific limitations on what aspects of the QoS and policy framework an authorized MCX User can modify. MCX service is supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

Mission Critical Services leverage the foundation of the 5G QoS Model as defined in clause 5.7, and 5G Policy Control as defined in clause 5.14. It requires that the necessary subscriptions are in place for both the 5G QoS Profile and the necessary Policies. In addition, Mission Critical Services leverage priority mechanism as defined in subclause 5.22.

The terminating network identifies the priority of the MCX session and applies priority treatment, including paging with priority, to ensure that the MCS session can be established with priority to the terminating user (either an MCX User or normal user).

Priority treatment for MCX service includes priority message handling, including priority treatment during authentication, security, and Mobility Management procedures.

Priority treatment for MCX sessions requires appropriate ARP and 5QI (plus 5G QoS characteristics) setting for QoS Flows according to the operator's policy.

NOTE: Use of QoS Flows for MCX session with non-standardized 5QI values enables the flexible assignment of 5G QoS characteristics (e.g. priority level).

When a MCX session is requested by an MCX User, the following principles apply in the network:

- QoS Flows employed in a Mission Critical Service session shall be assigned ARP value settings appropriate for the priority level of the MCX User.

- Setting ARP pre-emption capability and vulnerability of QoS Flows related to MCX session, subject to operator policies and depending on national/regional regulatory requirements.

- Pre-emption of non-MCX Users over MCX Users during network congestion situation, subject to operator policy and national/regional regulations.

Priority treatment is applicable to IMS based multimedia services and priority PDU connectivity service.

Relative PDU priority decisions for MCX sessions are based on real-time data of the state of the network and/or based on modification of the QoS and policy framework by authorized users as described in clause 6.8 of TS 22.261 [2].

5.17 Interworking and Migration

5.17.1 Support for Migration from EPC to 5GC

5.17.1.1 General

Clause 5.17.1 describes the UE and network behaviour for the migration from EPC to 5GC.

Deployments based on different 3GPP architecture options (i.e. EPC based or 5GC based) and UEs with different capabilities (EPC NAS and 5GC NAS) may coexist at the same time within one PLMN.

It is assumed that a UE that is capable of supporting 5GC NAS procedures may also be capable of supporting EPC NAS (i.e. the NAS procedures defined in TS 24.301 [13]) to operate in legacy networks e.g. in case of roaming.

The UE will use EPC NAS or 5GC NAS procedures depending on the core network by which it is served.

In order to support smooth migration, it is assumed that the EPC and the 5GC have access to a common subscriber database, that is HSS in case of EPC and the UDM in case of 5GC, acting as the master data base for a given user as defined in TS 23.002 [21].

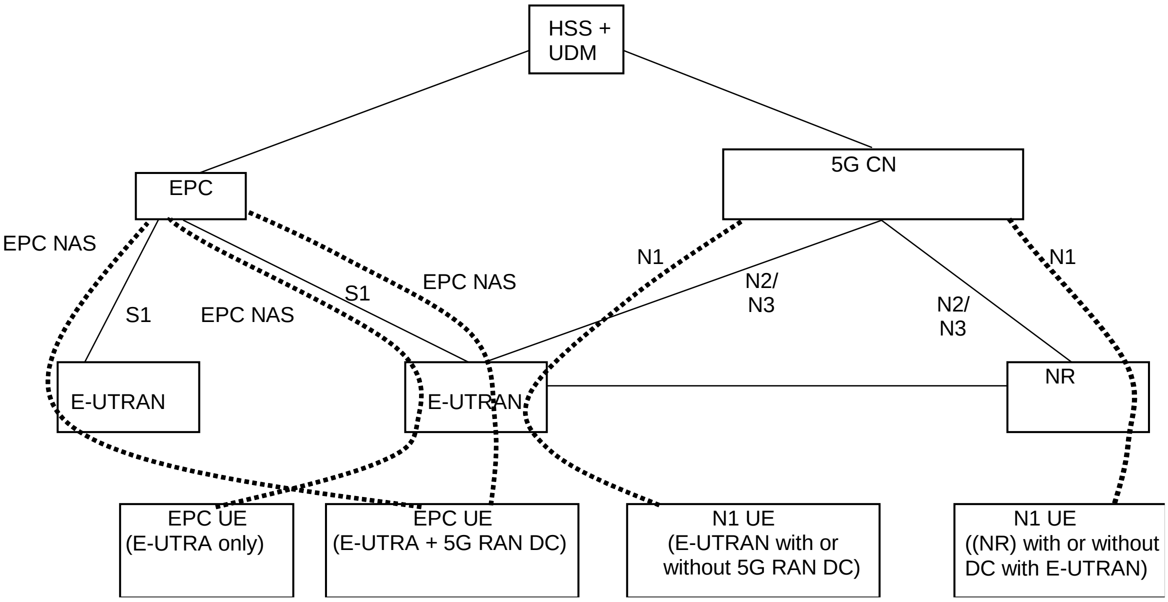

HSS + UDM
EPC
5G CN
EPC NAS
S1
EPC NAS
S1
EPC NAS
N1
N2/ N3
N2/ N3
N1
E-UTRAN
E-UTRAN
NR
EPC UE (E-UTRA only)
EPC UE (E-UTRA + 5G RAN DC)
N1 UE (E-UTRAN with or without 5G RAN DC)
N1 UE ((NR) with or without DC with E-UTRAN)

Figure 5.17.1.1-1: Architecture for migration scenario for EPC and 5G CN

A UE that supports only EPC based Dual Connectivity with secondary RAT NR:

- always performs initial access through E-UTRA (LTE-Uu) but never through NR;
- performs EPC NAS procedures over E-UTRA (i.e. Mobility Management, Session Management etc) as defined in TS 24.301 [13].

A UE that supports camping on 5G Systems with 5GC NAS:

- performs initial access either through E-UTRAN that connects to 5GC or NR towards 5GC;
- performs initial access through E-UTRAN towards EPC, if supported and needed;

- performs EPC NAS or 5GC NAS procedures over E-UTRAN or NR respectively (i.e. Mobility Management, Session Management etc) depending on capability indicated in AS, if the UE also supports EPC NAS.

NOTE 1: When camping on E-UTRA that connects to 5GC, a UE supporting EPC NAS and 5GC NAS initiates 5GC NAS procedures when 5GC is supported by the serving PLMN.

In order to support different UEs with different capabilities in the same network, i.e. both UEs that are capable of only EPC NAS (possibly including EPC based Dual Connectivity with secondary NR) and UEs that support 5GC NAS procedures in the same network:

- eNB that supports access to 5GC shall broadcast that it can connect to 5GC.

- The UE that supports 5GC NAS procedures shall provide a capability indication at Access Stratum as defined in TS 38.300 [27] when it performs initial access (the capability indication can be used to indicate ability to support N1 procedures).

Editor's note: The exact Access Stratum protocol for the indicator to be used by RAN to perform CN selection (EPC or 5GC) is going to be defined in RAN specifications.

NOTE 2: The UE that supports EPC based Dual Connectivity with secondary RAT only does not provide this indication at Access Stratum when it performs initial access and therefore eNB uses the "default" CN selection mechanism to direct this UE to an MME

Based on the Core Network type restriction described in clause 5.3.4.1.1 the 5GC network may steer the UE towards EPC.

In this release of the specification there is no support in 5G System for some functionalities supported in EPS such as ProSe, MBMS, CIOT optimisations, V2X etc. The UE that wants to use one or more of these functionalities not supported by 5G System, when in CM-IDLE may disable all the related radio capabilities and the capability indication that allow the UE to access 5G System. The triggers to disable and re-enable the capabilities to access 5G System in this case are left up to UE implementation.

5.17.2 Interworking with EPC

5.17.2.1 General

Interworking with EPC in this clause refers to mobility procedures between 5GC and EPC/E-UTRAN, except for subclause 5.17.2.4.

In order to interwork with EPC, the UE that supports both 5GC and EPC NAS can operate in single-registration mode or dual-registration mode:

- In single-registration mode, UE has only one active MM state (either RM state in 5GC or EMM state in EPC) and it is either in 5GC NAS mode or in EPC NAS mode (when connected to 5GC or EPC, respectively). UE maintains a single coordinated registration for 5GC and EPC. Accordingly, the UE maps the EPS-GUTI to 5G GUTI during mobility between EPC and 5GC and vice versa following the mapping rules in Annex B. To enable re-use of a previously established 5G security context when returning to 5GC, the UE also keeps the native 5G-GUTI and the native 5G security context when moving from 5GC to EPC.

- In dual-registration mode, UE can handle independent registrations for 5GC and EPC. In this mode, UE maintains 5G-GUTI and EPS-GUTI independently. In this mode, UE provides native 5G-GUTI, if previously allocated by 5GC, for registrations towards 5GC and it provides native EPS-GUTI, if previously allocated by EPC, for Attach/TAU towards EPC. In this mode, the UE may be registered to 5GC only, EPC only, or to both 5GC and EPC.

The support of single registration mode is mandatory for UEs that support both 5GC and EPC NAS.

During E-UTRAN Initial Attach, UE supporting both 5GC and EPC NAS shall indicate its support of 5G NAS in UE Network Capability described in clause 5.11.3 of TS 23.401 [26].

During registration to 5GC, UE supporting both 5GC and EPC NAS shall indicate its support of EPC NAS.

NOTE: This indication may be used to give the priority towards selection of PGW-C + SMF for UEs that support both EPC and 5GC NAS.

PDU Session types "Ethernet" and "Unstructured" are transferred to EPC as "non-IP" PDN type (when supported by UE and network). UE sets the PDN type to non-IP when it moves from 5GS to EPS and after the transfer to EPS, the UE and the SMF shall maintain information about the PDU Session type used in 5GS, i.e. information indicating that the PDN Connection with "non-IP" PDN type corresponds to PDU Session type Ethernet or Unstructured respectively. This is done to ensure that the appropriate PDU Session type will be used if the UE transfers to 5GS.

It is assumed that if a UE supports Ethernet PDU Session type and/or Unstructured PDU Session type in 5GS it will also support non-IP PDN type in EPS. If this is not the case, the UE shall locally delete any EBI(s) corresponding to the Ethernet/Unstructured PDU Session(s) to avoid that the Ethernet/Unstructured PDU Session(s) are transferred to EPS.

Networks that support interworking with EPC, may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface. Interworking procedures with N26 support providing IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPC NAS. Networks that support interworking procedures without N26 shall support procedures to provide IP address continuity on inter-system mobility to UEs operating in both single-registration mode and dual-registration mode.

In entire clause 5.17.2 the terms "initial attach", "handover attach" and "TAU" for the UE procedures in EPC can alternatively be combined EPS/IMSI Attach and combined TA/LA depending on the UE configuration defined in TS 23.221 [23].

5.17.2.2 Interworking Procedures with N26 interface

5.17.2.2.1 General

Interworking procedures using the N26 interface, enables the exchange of MM and SM states between the source and target network. When interworking procedures with N26 is used, the UE operates in single-registration mode. For the 3GPP access, the network keeps only one valid MM state for the UE, either in the AMF or MME. For the 3GPP access, either the AMF or the MME is registered in the HSS+UDM.

The support for N26 interface between AMF in 5GC and MME in EPC is required to enable seamless session continuity (e.g. for voice services) for inter-system change. When the UE moves from 5GS to EPS, the SMF determines which PDU sessions can be relocated to the target EPS, e.g. based on capability of the deployed EPS, operator policies for which PDU session, seamless session continuity should be supported etc. The SMF can release the PDU sessions that cannot be transferred as part of the handover. However, whether the PDU Session is successfully moved to the target network is determined by target EPS.

NOTE: When applying the AMF planned removal procedure or the procedure to handle AMF failures (see clause 5.21.2) implementations are expected to update the DNS configuration to enable MMEs to discover alternative AMFs if the MME tries to retrieve a UE context from an AMF that has been taken out of service or has failed. This addresses the scenario of UEs performing 5GS to EPS Idle mode mobility and presenting a mapped GUTI pointing to an AMF that has been taken out of service or has failed.

5.17.2.2.2 Mobility for UEs in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure with the N26 interface:

- For idle-mode mobility from 5GS to EPS, the UE performs either TAU or Attach procedure with EPS GUTI mapped from 5G-GUTI sent as old Native GUTI, as described in clause 4.11.1.3.2.1 of TS 23.502 [3] and indicates that it is moving from 5GC. The MME retrieves the UE's MM and SM context from 5GC. For connected-mode mobility from 5GS to EPS, either inter-system handover or RRC connection release with redirection to E-UTRAN is performed. During the TAU or Attach procedure the HSS+UDM cancels any AMF registration associated with the 3GPP access (but not AMF registration associated with the non-3GPP access): an AMF that was serving the UE over both 3GPP and non-3GPP accesses does not consider the UE as deregistered over non 3GPP access.

NOTE 1: MMEs supporting interworking with N26 interface are not required to process the indication from the UE that it is moving from 5GC and will assume that the UE is moving from another MME.

- For idle-mode mobility from EPC to 5GC, the UE performs mobility registration procedure with the 5G GUTI mapped from EPS GUTI and indicates that it is moving from EPC. The UE also includes the native 5G-GUTI as an additional GUTI in the Registration request. The AMF and SMF retrieve the UE's MM and SM context from EPC. For connected-mode mobility from EPC to 5GC, either inter-system handover or RRC connection release with redirection to NG-RAN is performed. During the Registration procedure, the HSS+UDM cancels any MME registration. For both idle mode and connected mode mobility from EPC to 5GC, if the UE supports Reflective QoS functionality, the UE shall trigger the PDU session modification procedure to indicate the support of reflective QoS to the network (i.e. SMF).

5.17.2.3 Interworking Procedures without N26 interface

5.17.2.3.1 General

For interworking without the N26 interface, IP address continuity is provided to the UEs on inter-system mobility by storing and fetching PGW-C+SMF and corresponding APN/DDN information via the HSS+UDM. In such networks AMF also provide an indication that interworking without N26 is supported to UEs during initial Registration in 5GC or MME may optionally provide an indication that interworking without N26 is supported in the Attach procedure in EPC as defined in TS 23.401 [26].

NOTE 1: The indication from MME that interworking without N26 is useful for UE supporting dual registration mode.

This indication is valid for the entire Registered PLMN and for PLMNs equivalent to the Registered PLMN. The same indication is provided to all UEs served by the same PLMN. UEs that operate in interworking without N26 may use this indication to decide whether to register early in the target system. UEs that operate in single-registration mode may use this indication as described in clause 5.17.2.3.2.

Interworking procedures without N26 interface use the following two features:

1. When PDU Session are created in 5GC, the PGW-C+SMF updates its information along with DNN in the HSS+UDM.

2. The HSS+UDM provides the information about dynamically allocated PGW-C+SMF and APN/DNN information to the target CN network.

To support mobility both for single and dual registration mode UEs, the following also are supported by the network:

3. When UE performs Initial Attach in EPC (with or without "Handover" indication in PDN CONNECTIVITY Request message) and indicates that it is moving from 5GC, the MME does not include "initial attach" indicator to the HSS+UDM. This results in HSS+UDM not cancelling the registration of AMF, if any.

4. When UE performs Initial Registration in 5GC and indicates that it is moving from EPC, the AMF does not include "initial attach" indicator to the HSS+UDM. This results in HSS+UDM not cancelling the registration of MME, if any.

5. When PDN connections are created in EPC, the MME stores the PGW-C+SMF and APN information in the HSS+UDM.

NOTE 3: Items 4 and 5 are also supported in networks that support interworking with N26 procedures. This enables a VPLMN that does not deploy N26 interface to provide IP address continuity to roamed-in single-registration mode UEs from a HPLMN that only supports interworking with N26 procedures.

Networks that support 5GS-EPS interworking procedures without N26 interface do not need to provide the UEs with mapped target system parameters (e.g. QoS parameters, bearer IDs/QFI, PDU Session ID, etc.) of the target system when UE is in the source network.

When an AMF in such a network receives a request to allocate an EBI(s) for a QoS Flow(s) from a PGW-C+SMF, it may not provide the EBI(s).

NOTE 4: A UE in a VPLMN that supports interworking without N26 may be provided with mapped QoS parameters from PGW-C+SMF in HPLMN for home-routed PDN connection, if the HPLMN supports interworking procedures with N26 interface.

A UE that operates in dual registration mode ignores any received mapped target system parameters (e.g. QoS parameters, bearer IDs/QFI, PDU Session ID, etc.).

5.17.2.3.2 Mobility for UEs in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure without N26 interface:

- For mobility from 5GC to EPC, the UE with at least one PDU Session established in 5GC may either:
  - if supported and if it has received the network indication that interworking without N26 is supported, perform Attach in EPC with EPS GUTI mapped from 5G-GUTI sent as old Native GUTI with Request type "Handover" in PDN CONNECTIVITY Request message (TS 23.401 [26], clause 5.3.2.1) and indicating that the UE is moving from 5GC and subsequently moves all its other PDU Session using the UE requested PDN connectivity establishment procedure with Request Type "handover" flag (TS 23.401 [26] clause 5.10.2), or.
  - perform TAU with 4G-GUTI mapped from 5G-GUTI sent as old Native GUTI (TS 23.401 [26], clause 5.3.3) indicating that it is moving from 5GC, in which case the MME instructs the UE to re-attach. IP address preservation is not provided in this case.

NOTE 1: The first PDN connection may be established during the E-UTRAN Initial Attach procedure (see TS 23.401 [26]).

NOTE 2: At inter-PLMN mobility the UE always uses the TAU procedure.

- For mobility from 5GC to EPC, the UE with no PDU Session established in 5GC
  - performs Attach in EPC (TS 23.501 clause 5.3.2.1) indicating that the UE is moving from 5GC.
- For mobility from EPC to 5GC, the UE performs Registration of type "mobility registration update" in 5GC with 5G-GUTI mapped from EPS GUTI and indicating that the UE is moving from EPC. In this case, the AMF determines that old node is an MME, but proceeds as if the Registration is of type "initial registration". The UE may either:
  - if supported and if it has received the network indication that dual registration mode is supported, move all its PDN connections from EPC using the UE initiated PDU Session establishment procedure with "Existing PDU Sessions" flag (TS 23.502 [3], clause 4.3.2.2.1), or
  - re-establish PDU Sessions corresponding to the PDN connections that it had in EPS. IP address preservation is not provided in this case.

NOTE 3: When single-registration mode UE uses interworking procedures without N26, the registration states during the transition period (e.g. while UE is transferring all PDU Sessions / PDN Connections on the target side) are defined in Stage 3 specifications.

5.17.2.3.3 Mobility for UEs in dual-registration mode

To support mobility in dual-registration mode, the support of N26 interface between AMF in 5GC and MME in EPC is not required.

For UE operating in dual-registration mode the following principles apply for PDU Session transfer from 5GC to EPC:

- UE operating in Dual Registration mode may register in EPC ahead of any PDU Session transfer using the Attach procedure indicating that the UE is moving from 5GC without establishing a PDN Connection in EPC if the EPC supports EPS Attach without PDN Connectivity as defined in TS 23.401 [26]. Support for EPS Attach without PDN Connectivity is mandatory for UE supporting dual-registration procedures.

NOTE 1: Before attempting early registration in EPC the UE needs to check whether EPC supports EPS Attach without PDN Connectivity by reading the related SIB in the target cell.

- UE performs PDU Session transfer from 5GC to EPC using the UE initiated PDN connection establishment procedure with "handover" indication in the PDN Connection Request message (TS 23.401 [26], clause 5.10.2).
- If the UE has not registered with EPC ahead of the PDU Session transfer, the UE can perform Attach in EPC with "handover" indication in the PDN Connection Request message (TS 23.401 [26], clause 5.3.2.1).
- UE may selectively transfer certain PDU Sessions to EPC, while keeping other PDU Sessions in 5GC.

- UE may maintain the registration up to date in both 5GC and EPC by re-registering periodically in both systems. If the registration in either 5GC or EPC times out (e.g. upon mobile reachable timer expiry), the corresponding network starts an implicit detach timer.

NOTE 2: Whether UE transfers some or all PDU Sessions on the EPC side and whether it maintains the registration up to date in both EPC and 5GC can depend on UE capabilities that are implementation dependent. The information for determining which PDU Sessions are transferred on EPC side and the triggers can be pre-configured in the UE and are not specified in this release of the specification.

For UE operating in dual-registration mode the following principles apply for PDN connection transfer from EPC to 5GC:

- UE operating in Dual Registration mode may register in 5GC ahead of any PDN connection transfer using the Registration procedure indicating that the UE is moving from EPC (TS 23.502 [3], clause 4.2.2.2.2).
- UE performs PDN connection transfer from EPC to 5GC using the UE initiated PDU Session Establishment procedure with "Existing PDU Session" indication (TS 23.502 [3], clause 4.3.2.2.1).
- UE may selectively transfer certain PDN connections to 5GC, while keeping other PDN Connections in EPC.
- UE may maintain the registration up to date in both EPC and 5GC by re-registering periodically in both systems. If the registration in either EPC or 5GC times out (e.g. upon mobile reachable timer expiry), the corresponding network starts an implicit detach timer.

NOTE 3: Whether UE transfers some or all PDN connections on the 5GC side and whether it maintains the registration up to date in both 5GC and EPC can depend on UE capabilities that are implementation dependent. The information for determining which PDN connections are transferred on 5GC side and the triggers can be pre-configured in the UE and are not specified in this release of the specification.

NOTE 4: If EPC does not support EPS Attach without PDN Connectivity the MME detaches the UE when the last PDN connection is released by the PGW as described in TS 23.401 [26] clause 5.4.4.1 (in relation to transfer of the last PDN connection to non-3GPP access).

When sending a control plane request for MT services (e.g. MT SMS) the network routes it via either the EPC or the 5GC. In absence of UE response, the network should attempt routing the control plane request via the other system.

NOTE 5: The choice of the system through which the network attempts to deliver the control plane request first is left to network configuration.

5.17.2.3.4 Redirection for UEs in connected mode

When the UE supports single-registration mode or dual-registration mode without N26 interface:

- If the UE is in CM-CONNECTED status in 5GC, the NG-RAN may perform RRC connection release with redirection to E-UTRAN based on certain criteria (e.g. based on local configuration in NG-RAN, or triggered by the AMF upon receiving handover request from NG-RAN).
- If the UE is in ECM-CONNECTED status in EPC, the E-UTRAN may perform RRC connection release with redirection to NG-RAN based on certain criteria (e.g. based on local configuration in E-UTRAN, or triggered by the MME upon receiving handover request from E-UTRAN).

5.17.2.4 Mobility between 5GS and GERAN/UTRAN

IP address preservation upon mobility between 5GS and GERAN/UTRAN is not supported.

Upon mobility from 5GS to GERAN/UTRAN (e.g. upon leaving NG-RAN coverage) the UE shall perform the A/Gb mode GPRS Attach procedure or Iu mode GPRS Attach procedure (see TS 23.060 [56]).

Upon mobility from GERAN/UTRAN to 5GS (e.g. upon selecting an NG-RAN cell) the UE shall perform the Registration procedure of "initial registration" type as described in TS 23.502 [3].

5.17.3 Interworking with EPC in presence of Non-3GPP PDU sessions

When a UE is simultaneously connected to the 5GC over a 3GPP access and a non-3GPP access, it may have PDU sessions associated with 3GPP access and PDU Sessions associated with non-3GPP access. When inter-system handover is performed for PDU sessions associated with 3GPP access, the PDU sessions associated with non-3GPP access remain anchored in 5GC.

5.18 Network Sharing

5.18.1 General concepts

A network sharing architecture shall allow multiple participating operators to share resources of a single shared network according to agreed allocation schemes. The shared network includes a radio access network. The shared resources include radio resources.

The shared network operator allocates shared resources to the participating operators based on their planned and current needs and according to service level agreements.

In this release of the specification, only the 5G Multi-Operator Core Network (5G MOCN) network sharing architecture, in which only the RAN is shared in 5G System, is supported. 5G MOCN for 5G System, including UE, RAN and AMF, shall support operators' ability to use more than one PLMN ID (i.e. with same or different country code (MCC) which is specified in TS 23.122 [17] and different network codes (MNC)).

NOTE: Different PLMN IDs can also point to the same 5GC.

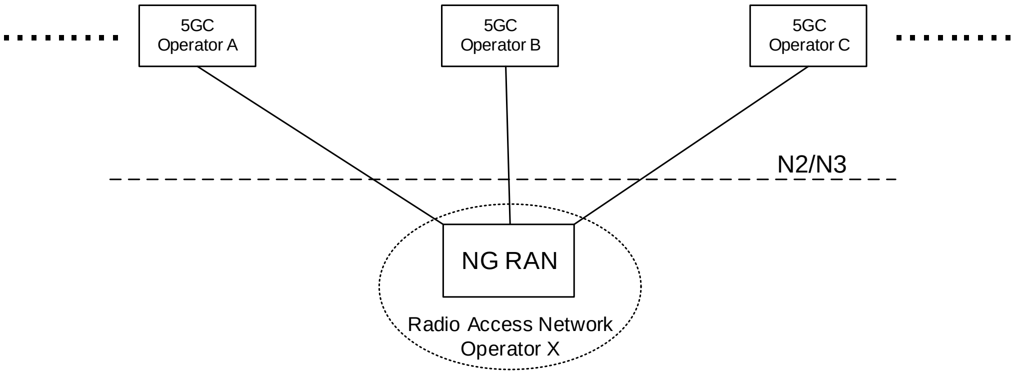


Figure 5.18.1-1: A 5G Multi-Operator Core Network (5G MOCN) in which multiple CNs are connected to the same NG-RAN

5.18.2 Broadcast system information for network sharing

If a shared NG-RAN is configured to indicate available PLMNs for selection by UEs, each cell in the shared radio access network shall in the broadcast system information include PLMNs concerning available core network operators in the shared network.

The Broadcast System Information broadcasts a set of PLMN IDs and one or more additional set of parameters per PLMN e.g. cell-ID, Tracking Areas. All 5G System capable UEs that connect to NG-RAN support reception of multiple PLMN IDs and per PLMN specific parameters.

The available core network operator PLMNs shall be the same for all cells of a Tracking Area in a shared NG-RAN network.

UE decodes the broadcast system information and takes the information concerning available PLMN IDs into account in PLMN and cell (re-)selection procedures. Broadcast system information is specified in TS 38.331 [28] for NR, TS 36.331 [51] for E-UTRA and related UE access stratum idle mode procedures in TS 38.304 [50] for NR and TS 36.304 [52] for E-UTRA.

5.18.3 Network selection

A UE that has a subscription to one of the sharing core network operators shall be able to select this core network operator while within the coverage area of the shared network and to receive subscribed services from that core network operator.

Each cell in shared NG-RAN shall in the broadcast system information include the PLMN-IDs concerning available core network operators in the shared network.

When a UE performs an initial registration to a network, one of available PLMNs shall be selected to serve the UE. UE uses all the received broadcast PLMN-IDs in its PLMN (re)selection processes which is specified in TS 23.122 [17]. UE shall inform the NG-RAN of the selected PLMN so that the NG-RAN can route correctly. The NG-RAN shall inform the core network of the selected PLMN.

As per any network, after initial registration to the shared network and while remaining served by the shared network, the UE should not change to another available PLMN as long as the selected PLMN is available to serve the UE's location. The network selection procedures specified in TS 23.122 [17] may cause the UE to perform a reselection of another available PLMN. Also the network should not move the UE to another available PLMN, e.g. by handover, as long as the selected PLMN is available to serve the UE's location.

UE uses all of the received broadcast PLMN-IDs in its PLMN (re)selection processes.

5.18.4 Network selection in Handover procedure

The NG-RAN uses the selected PLMN (provided by the UE at RRC establishment, or, provided by the AMF/source NG-RAN at N2/Xn handover) to select target cells for future handovers (and radio resources in general) appropriately.

In the case of handover to a shared network:

- The NG-RAN selects a target PLMN based on either (1) PLMN in use (2), pre-configuration, or (3) the EPLMN list in the Handover Restriction List provided by the AMF. When multiple PLMN IDs are broadcast in a cell selected by NG-RAN for handover, NG-RAN shall select a target PLMN, taking into account the prioritized list of PLMN IDs provided via Handover Restriction list from AMF.
- For Xn based HO procedure, Source NG-RAN indicates a selected PLMN ID to the target NG-RAN by using target cell ID.
- For N2 based HO procedure, the NG-RAN indicates a selected PLMN ID to the AMF as part of the TAI sent in the HO required message. Source AMF uses the TAI information supplied by the source NG-RAN to select the target AMF/MME. The source AMF should forward the selected PLMN ID to the target AMF/MME. The target AMF/MME indicates the selected PLMN ID to the target NG-RAN/eNB so that the target NG-RAN/eNB can select target cells for future handover appropriately.

A change in serving PLMN is indicated to the UE as part of the UE registration with the selected network.

5.18.5 Network Sharing and Network Slicing

As defined in clause 5.15.1, a Network Slice is defined within a PLMN. Network sharing is performed among different PLMNs. In case of network sharing, each PLMN sharing the NG-RAN defines and supports its PLMN-specific set of slices that are supported by the common NG-RAN.

5.19 Control Plane Load Control, Congestion and Overload Control

5.19.1 General

In order to ensure that the network functions within 5G System are operating under nominal capacity for providing connectivity and necessary services to the UE. Thus, it supports various measures to guard itself under various operating conditions (e.g. peak operating hour, extreme situations). It includes support for load (re-)balancing, overload control and NAS level congestion control. A 5GC NF is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic).

5.19.2 TNLA Load Balancing and TNLA Load Re-Balancing

AMF can support load balancing and re-balancing of TNL associations between AN and AMF by using mechanisms specified in clause 5.21.1.

5.19.3 AMF Load Balancing

The AMF Load Balancing functionality permits UEs that are entering into an AMF Region/AMF Set to be directed to an appropriate AMF in a manner that achieves load balancing between AMFs. This is achieved by setting a Weight Factor for each AMF, such that the probability of the AN selecting an AMF is proportional to Weight Factor of the AMF. The Weight Factor is typically set according to the capacity of an AMF node relative to other AMF nodes. The Weight Factor is sent from the AMF to the NG-AN via NGAP messages (see TS 38.413 [34]).

NOTE 1: An operator may decide to change the Weight Factor after the establishment of NGAP connectivity as a result of changes in the AMF capacities. E.g., a newly installed AMF may be given a very much higher Weight Factor for an initial period of time making it faster to increase its load.

NOTE 2: It is intended that the Weight Factor is NOT changed frequently. e.g. in a mature network, changes on a monthly basis could be anticipated, e.g. due to the addition of RAN or CN nodes.

When Network slicing is deployed, load balancing by NG-AN node is only performed between AMFs that belong to the same AMF set, i.e. AMFs with the same PLMN and AMF Set ID value.

The NG AN node may have their Load Balancing parameters adjusted (e.g. the Weight Factor is set to zero if all subscribers are to be removed from the AMF, which will route new entrants to other AMFs within an AMF Set).

5.19.4 AMF Load Re-Balancing

The AMF load re-balancing functionality permits cross-section of its subscribers that are registered on an AMF (within an AMF Set) to be moved to another AMF within the same AMF set with minimal impacts on the network and end users. AMF may request some or all of the AN node(s) to redirect a cross-section of UE(s) returning from IDLE mode to be redirected to another AMF within the same AMF set, if the AN is configured to support this. If AMF is configured with more than one GUAMI, the AMF may request some or all of the AN node(s) to redirect UE(s) served by one of its GUAMI(s) to a specific target AMF or to a different AMF within the same AMF set.

For UE(s) in IDLE mode, when UE subsequently returns from IDLE mode and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI pointing to an AMF that requested for redirection, the 5G-AN should select the specific target AMF (provided by the original AMF) or a different AMF from the same AMF set and forward the initial NAS message. The newly selected/target AMF (which is now the serving AMF) will re-assign the GUTI (using its own GUAMI(s)) to the UE(s). It is not expected that the 5G-AN node rejects any request or enables access control restriction when it receives a request for redirection for load control from the connected AMF(s).

When the AMF wants to stop redirection, the AMF can indicate that it can serve all UE(s) in IDLE mode to stop the redirection.

NOTE 1: An example use for the AMF load re-balancing functionality is for the AMF to pro-actively re-balance its load prior to reaching overload i.e. to prevent overload situation.

NOTE 2: Typically, AMF Load Re-Balancing is not needed when the AMF becomes overloaded because the Load Balancing function should have ensured that the other AMFs within the AMF Set are similarly overloaded.

5.19.5 AMF Control Of Overload

5.19.5.1 General

The AMF shall contain mechanisms for avoiding and handling overload situations. This includes the following measures:

- N2 overload control that could result in RRC reject and unified access barring.

- NAS congestion control.

5.19.5.2 AMF Overload Control

Under unusual circumstances, if AMF has reached overload situation, the AMF activates NAS level congestion control as specified in Clause 5.19.7 and AMF restricts the load that the AN node(s) are generating, if the AN is configured to support overload control. N2 overload control can be achieved by the AMF invoking the N2 overload procedure (see TS 38.300 [27] and TS 38.413 [34]) to all or to a proportion of the AN nodes with which the AMF has N2 connections. The AMF may include the S-NSSAI(s) in N2 overload control message sent to AN node(s) to indicate the congestion of the Network Slice(s) at the CN part. To reflect the amount of load that the AMF wishes to reduce, the AMF can adjust the proportion of AN nodes which are sent NGAP OVERLOAD START message, and the content of the overload start procedure.

The AMF should select the 5G-AN node(s) to which it triggers overload start procedure at random to avoid that multiple AMFs in an AMF Set request reduction of load from the same subset of 5G-AN node(s).

An AN node supports rejecting of AN signalling connection establishments for certain UEs as specified in TS 38.331 [28]. Additionally, an AN node provides support for the barring of UEs as described in TS 22.261 [2]. These mechanisms are further specified in TS 38.331 [28].

Using the overload start procedure, the AMF can request the AN node to:

- reject AN signaling connection (RRC connection over 3GPP access or UE-N3IWF connection over N3GPP access) requests that are for non-emergency and non-high priority mobile originated services; or

- reject new AN signaling connection requests for uplink NAS signalling transmission to that AMF;

- release AN signalling connection for uplink NAS signalling transmission where the Requested NSSAI at AS layer only includes the indicated S-NSSAI(s).

- only permit AN signaling connection requests for emergency sessions and mobile terminated services for that AMF; or

- only permit AN signaling connection requests for high priority sessions and mobile terminated services for that AMF;

NOTE 2: The AN signaling connection requests listed in this clause also include the request from UE in RRC-Inactive state..

The AMF can provide percentage value that indicates how much amount of signalling traffic to be rejected in the overload start message, and the AN node may consider this value for congestion control.

When rejecting an AN signaling connection request for overload reasons the AN indicates to the UE an appropriate wait timer value that limits further AN signaling connection requests for a while.

During an overload situation, the AMF should attempt to maintain support for emergency services and for MPS.

When the AMF is recovering, the AMF can either:

- trigger overload start procedure with new percentage value that permit more signalling traffic to be carried, or

- the AMF trigger overload stop procedure.

to some or all of the 5G-AN node(s).

5.19.6 SMF Overload Control

The SMF shall contain mechanisms for avoiding and handling overload situations. This can include the following measures:

- SMF overload control that could result in rejections of NAS requests.

The SMF overload control may be activated by SMF due to congestion situation at SMF e.g. configuration, by a restart or recovery condition of a UPF, or by a partial failure or recovery of a UPF for a particular UPF(s).

Under unusual circumstances, if the SMF has reached overload situation, the SMF activates NAS level congestion control as specified in the clause 5.19.7. The SMF may restrict the load that the AMF(s) are generating, if the AMF is configured to enable the overload restriction.

5.19.7 NAS level congestion control

5.19.7.1 General

NAS level congestion control may be applied in general i.e. for all NAS messages, per DNN, per DNN and S-NSSAI or for a specific group of UEs.

NAS level congestion control applied on all NAS messages is achieved by the AMF rejecting NAS messages, from the UE, with a back-off timer. To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the AMF should select the back-off timer value so that the deferred requests are not synchronized. When the UE receives a rejection of a NAS message with a back-off timer, the UE shall not initiate any NAS signalling with regards to the applied congestion control until the back-off timer expires or the UE receives a paging request from the network, or the UE initiates signalling with a higher priority than was used when the UE received the back-off timer.

AMFs and SMFs may apply NAS level congestion control, but should not apply NAS level congestion control for high priority access and emergency services.

5.19.7.2 General NAS level congestion control

Under general overload conditions the AMF may reject Registration and Mobility Management signalling requests from UEs. When a NAS request is rejected, a Mobility Management back-off timer may be sent by the AMF and AMF may store the back-off time per UE if AMF maintains the UE context. The AMF may immediately reject any subsequent request from the UE before the stored back-off time is expired. While the Mobility Management back-off timer is running, the UE shall not initiate any NAS request for Registration or Mobility Management procedures except for Deregistration procedure and except for high priority access, emergency services and mobile terminated services. After any such Deregistration procedure, the back-off timer continues to run. While the Mobility Management back-off timer is running, the UE is allowed to perform Registration for mobility registration update if the UE is already in CM-CONNECTED state. If the UE receives a paging request or a NAS notification message via Non-3GPP access from the AMF while the Mobility Management back off timer is running, the UE shall stop the Mobility Management back-off timer and initiate the Service Request procedure or the Registration procedure for mobility registration update.

The Mobility Management back-off timer shall not impact Cell/RAT and PLMN change. Cell/RAT and TA change do not stop the Mobility Management back-off timer. The Mobility Management back-off timer shall not be a trigger for PLMN reselection. The back-off timer is stopped as defined in TS 24.501 [47] when a new PLMN that is not an equivalent PLMN is accessed.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the AMF should select the Mobility Management back-off timer value so that the deferred requests are not synchronized.

The AMF should not reject Registration Request message for mobility registration update that are performed when the UE is already in connected mode.

For CM-IDLE state mobility, the AMF may reject Registration Request messages for mobility registration update and include a Mobility Management back off timer value in the Registration Reject message.

If the AMF rejects Registration Request messages or Service Request with a Mobility Management back-off timer which is larger than the sum of the UE's periodic registration update timer plus the Implicit Deregistration timer, the AMF should adjust the mobile reachable timer and/or Implicit Deregistration timer such that the AMF does not implicitly deregister the UE while the Mobility Management back-off timer is running.

NOTE: This is to minimize unneeded signalling after the Mobility Management back-off timer expires.

5.19.7.3 DNN based congestion control

The use of the DNN based congestion control is for avoiding and handling of NAS signalling congestion associated with UEs with a particular DNN regardless of S-NSSAI. Both UEs and 5GC shall support the functions to provide DNN based congestion control.

SMFs may apply DNN based congestion control towards the UE by rejecting PDU Session Establishment/Modification Request messages towards a specific DNN, from the UE, with a back-off timer and the associated DNN. The SMF may release PDU Sessions belonging to a congested DNN by sending a PDU Session Release Request message towards the UE with a back-off timer. If back-off timer is set in the PDU Session Release Request message then the cause "reactivation requested" should not be set.

The AMF may provide a NAS Transport Error message for the NAS Transport message carrying an SM message and in the NAS Transport Error message include a back-off timer and the associated DNN. While the back-off timer for the specific DNN is running, then the UE will not send any NAS messages for the specific DNN.

Upon reception of the back-off timer for a DNN, the UE shall take the following actions until the timer expires:

- If DNN is provided in association with the back-off timer, the UE shall not initiate any Session Management procedures for the congested DNN. The UE may initiate Session Management procedures for other DNNs;
- If DNN is not provided in association with the back-off timer, the UE shall not initiate any Session Management requests of any PDU Session Type without DNN. The UE may initiate Session Management procedures for specific DNN;
- Cell/TA/PLMN/RAT change do not stop the back-off timer;
- The UE is allowed to initiate the Session Management procedures for high priority access and emergency services even when the back-off timer is running; and
- If the UE receives a network initiated Session Management Request message for the congested DNN while the back-off timer is running, the UE shall stop the Session Management back-off timer associated with this DNN and respond to the 5GC.

The UE is allowed to initiate PDU Session Release procedure (e.g. sending PDU Session Release Request message) when the back-off timer is running.

NOTE 3: The UE does not delete the related back-off timer when disconnecting a PDU Session.

The UE shall support a separate back-off timer for every DNN that the UE may use.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the 5GC should select the back-off timer value so that deferred requests are not synchronized.

The DNN based Session Management congestion control is applicable to the NAS SM signalling initiated from the UE in the Control Plane. The Session Management congestion control does not prevent the UE to send and receive data or initiate Service Request procedures for activating User Plane connection towards the DNN(s) that are under Session Management congestion control.

5.19.7.4 S-NSSAI based congestion control

The use of the S-NSSAI based congestion control is for avoiding and handling of NAS signalling congestion associated with UEs for a particular S-NSSAI.

S-NSSAI based congestion control is applied as follows:

- If an S-NSSAI is determined as congested, then the SMF may apply S-NSSAI based congestion control towards the UE for SM requests which includes an S-NSSAI, and provides a back-off timer, and an associated S-NSSAI and optionally a DNN;
- The SMF may release PDU Sessions belonging to a congested S-NSSAI by sending a PDU Session Release Request message towards the UE with a back-off timer associated to the S-NSSAI and optionally a DNN;
- If an S-NSSAI is determined as congested, then the AMF may apply S-NSSAI based congestion control towards the UE, by providing an NAS Transport Error message for the NAS Transport message carrying the SM message

and in the NAS Transport Error message include a back-off timer and an associated S-NSSAI and optionally in addition a DNN;

- Upon reception of a back-off timer with an associated S-NSSAI and optionally a DNN, the UE shall take the following actions until the timer expires:
  - The UE shall not initiate any Session Management procedures for the congested S-NSSAI;
  - If the back-off timer was associated with an S-NSSAI and a DNN, then the UE shall not initiate any Session Management procedures for that combination of S-NSSAI and DNN;
  - If the UE receives a network initiated Session Management Request message for the congested S-NSSAI and DNN while the back-off timer associated to the S-NSSAI and DNN is running, the UE shall stop the back-off timer associated with this S-NSSAI and DNN and respond to the 5GC.
  - Cell/TA/PLMN/RAT change doos not stop the back-off timer for the S-NSSAI;
  - The UE is allowed to initiate the Session Management procedures for high priority access and emergency services for the S-NSSAI even when the back-off timer associated to the S-NSSAI is running;

The UE shall support a separate back-off timer for every S-NSSAI that the UE may use.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the 5GC should select the value of the back-off timer for the S-NSSAI based congestion control so that deferred requests are not synchronized.

The S-NSSAI based congestion control does not prevent the UE to send and receive data or initiate Service Request procedure for activating User Plane connection belongs to the S-NSSAI that is under the congestion control.

5.19.7.5 Group specific NAS level congestion control

The group specific NAS level congestion control applies to a specific group of UEs. Group specific NAS level congestion control is performed at the 5GC. The AMF and SMF may apply NAS level congestion control for a UE associated to an Internal-Group Identifier (see clause 5.9.7). There is no impact on the UE, and hence, UE's behaviour as described in clauses 5.19.2.2 and 5.19.2.3 does not change.

NOTE: 5GC logic for Group specific NAS level congestion control is not described in this release.

5.20 External Exposure of Network Capability

The Network Exposure Function (NEF) supports external exposure of capabilities of network functions. External exposure can be categorized as Monitoring capability, Provisioning capability, and Policy/Charging capability. The Monitoring capability is for monitoring of specific event for UE in 5G System and making such monitoring events information available for external exposure via the NEF. The Provisioning capability is for allowing external party to provision of information which can be used for the UE in 5G System. The Policy/Charging capability is for handling QoS and charging policy for the UE based on the request from external party.

Monitoring capability is comprised of means that allow the identification of the 5G network function suitable for configuring the specific monitoring events, detect the monitoring event, and report the monitoring event to the authorised external party. Monitoring capability can be used for exposing UE's mobility management context such as UE location, reachability, roaming status, and loss of connectivity.

Provisioning capability allows an external party to provision the foreseen UE behavioural information to 5G NF via the NEF. The provisioning comprises of; the authorisation of the provisioning external third party, receiving the provisioned external information via the NEF, storing the information as part of the subscription data, and distributing that information among those NFs that use it. The externally provisioned data can be consumed by different NF, depending on the data. The externally provisioned information is defined as the Expected UE Behaviour in TS 23.502 [3] clause 4.15.6.3, and it consists of information on expected UE movement and expected UE communication intervals. The provisioned Expected UE Behaviour parameter may be used for the setting of mobility management or session management parameters of the UE. The affected NFs are informed of the subscriber data update.

Policy/Charging capability is comprised of means that allow the request for session and charging policy, enforce QoS policy, and apply accounting functionality. It can be used for specific QoS/priority handling for the session of the UE, and for setting applicable charging party or charging rate.

5.21 Architectural support for virtualized deployments

5.21.0 General

5GC supports different deployment scenarios, including but not limited to the options below:

- A Network Function instance can be deployed as fully distributed, fully redundant, stateless, and fully scalable NF instance that provides the services from several locations and several execution instances in each location.
  - This type of deployments would typically not require support for addition or removal of NF instances for redundancy and scalability. In case of an AMF this deployment option may use enablers like, addition of TNLA, removal of TNLA, TNLA release and rebinding of NGAP UE association to a new TNLA to the same AMF.
- A Network Function instance can also be deployed such that several network function instances are present within a NF set provide fully distributed, fully redundant and scalability together as a set of NF instances.
  - This type of deployments may support for addition or removal of NF instances for redundancy and scalability. In case of an AMF this deployment option may use enablers like, addition of AMFs and TNLAs, removal of AMFs and TNLAs, TNLA release and rebinding of NGAP UE association to a new TNLA to different AMFs in the same AMF set.

Also, deployments taking advantage of only some or any combination of concepts from each of the above options is possible.

5.21.1 Architectural support for N2

5.21.1.1 TNL associations

5G-AN node shall have the capability to support multiple TNL associations per AMF, i.e. AMF name.

An AMF shall provide the 5G-AN node with the weight factors for each TNL association of the AMF.

The AMF shall be able to request the 5G-AN node to add or remove TNL associations to the AMF.

The AMF shall be able to indicate to the 5G-AN node the set of TNL associations used for UE-associated signalling and the set of TNL associations used for non-UE associated signalling.

NOTE: The TNL association(s) indicated for UE-associated and non-UE associated signalling can either be overlap or be different.

5.21.1.2 NGAP UE-TNLA-binding

While a UE is in CM-Connected state the 5G-AN node shall maintain the same NGAP UE-TNLA-binding (i.e. use the same TNL association and same NGAP association for the UE) unless explicitly changed or released by the AMF.

An AMF shall be able to update the NGAP UE-TNLA-binding (i.e. change the TNL association for the UE) in CM-Connected mode at any time.

An AMF shall be able to update the NGAP UE-TNLA-binding (i.e. change the TNL association for the UE) in response to an N2 message received from the 5G-AN by triangular redirection (e.g. by responding to the 5G-AN node using a different TNL association).

An AMF shall be able to command the 5G-AN node to release the NGAP UE-TNLA-binding for a UE in CM-Connected mode while maintaining N3 (user-plane connectivity) for the UE at any time.

5.21.1.3 N2 TNL association selection

The 5G-AN node shall consider the following factors for selecting a TNL association for the AMF for the initial N2 message e.g. N2 INITIAL UE MESSAGE:

- Availability of candidate TNL associations.
- Weight factors of candidate TNL associations.

The AMF may use any TNL association intended for non-UE associated signalling for initiation of the N2 Paging procedure.

5.21.2 AMF Management

5.21.2.1 AMF Addition/Update

The 5G System should support establishment of association between AMF and 5G-AN node.

A new AMF can be added to an AMF set and association between AMF and GUAMI can be created and/or updated as follows:

- AMF shall be able to dynamically update the NRF with the new or updated GUAMI(s) to provide mapping between GUAMI(s) and AMF information. Association between GUAMI(s) and AMF is published to NRF. In addition, to deal with planned maintenance and failure, an AMF may optionally provide backup AMF information, i.e. it act as a backup AMF if the indicated GUAMI associated AMF is unavailable. Based on that information one GUAMI is associated with an AMF, optionally with a backup AMF used for planned removal and/or another (same or different) backup AMF used for failure.
- Upon successful update, the NRF considers the new and/or updated GUAMI(s) for providing AMF discovery results to the requester. Requester can be other CP network functions.

Information about new AMF should be published and available in the DNS system. It should allow 5G-AN to discover AMF and setup associations with the AMF required.

To support the legacy EPC core network entity to discover and communicate with the AMF, the information about the AMF should be published and available in the DNS system.

5.21.2.2 AMF planned removal procedure

5.21.2.2.1 AMF planned removal procedure with UDSF deployed

An AMF can be taken graciously out of service as follows:

- If an UDSF is deployed in the network, then the AMF stores the context for registered UE(s) in the UDSF. The UE context includes the NGAP-UE-AMF-ID that is unique per AMF set. If there are ongoing transactions (e.g. N1 procedure) for certain UE(s), AMF stores the UE context(s) in the UDSF upon completion of an ongoing transaction.
- The AMF deregister itself from NRF indicating due to AMF planned removal.

NOTE 1: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

NOTE 2: Before removal of AMF the overload control mechanism can be used to reduce the amount of ongoing transaction.

An AMF identified by GUAMI(s) shall be able to notify the 5G-AN that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF. Upon receipt of the indication that an AMF(identified by GUAMI(s)) is unavailable, 5G-AN shall take the following action:

- 5G-AN should mark this AMF as unavailable and not consider the AMF for selection for subsequent N2 transactions until 5G-AN learns that it is available (e.g. as part of discovery results or by configuration).
- If 5G-AN indicated support of timer capability during NGAP Setup procedure, the AMF may include an additional indicator that the AMF will rebind or release the NGAP UE-TNLA binding on per UE-basis for UE(s) in CONNECTED mode. If that indicator is included and the 5G-AN supports timer mechanism, the 5G-AN starts a timer to control the release of NGAP UE TNLA binding. For the duration of the timer or until the AMF releases or re-binds the NGAP UE TNLA binding the AN does not select a new AMF for subsequent UE transactions. Upon timer expiry, the 5G-AN releases the NGAP UE UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s), for subsequent N2 message, the 5G-AN should select a different AMF from the same AMF set when the subsequent N2 message needs to be sent.

NOTE 3: For UE(s) in CONNECTED mode, after indicating that the AMF is unavailable for processing UE transactions and including an indicator that the AMF releases the NGAP UE -TNLA bindings on a per UE-basis, the AMF can either trigger a re-binding of the NGAP UE associations to an available TNLA on a different AMF in the same AMF set or use the NGAP UE TNLA binding per UE release procedure defined in TS 23.502 [3] to release the NGAP UE-TNLA binding on a per UE-basis while requesting the AN to maintain N3 (user plane connectivity) and UE context information.

- If the instruction does not include the indicator, for UE(s) in CONNECTED mode, 5G-AN considers this as a request to release the NGAP-UE-TNLA-binding with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and UE context information. For subsequent N2 message, the 5G-AN should select a different AMF from the same AMF set when the subsequent N2 message needs to be sent.

- For UE(s) in IDLE mode, when it subsequently returns from IDLE mode and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI pointing to an AMF that is marked unavailable, the 5G-AN should select a different AMF from the same AMF set and forward the initial NAS message. If the 5G-AN can't select an AMF from the same AMF set, the 5G-AN selects another new AMF as described in clause 6.3.5.

An AMF identified by GUAMI(s) shall be able to instruct other peer CP NFs, subscribed to receive such a notification, that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF. If the CP NFs register with NRF for AMF unavailable notification, then the NRF shall be able to notify the subscribed NFs to receive such a notification that AMF identified by GUAMI(s) will be unavailable for processing transactions. Upon receipt of the notification that an AMF (GUAMI(s)) is unavailable, the other CP NFs shall take the following actions:

- CP NF should mark this AMF (identified by GUAMI(s)) as unavailable and not consider the AMF for selection for subsequent MT transactions until the CP NF learns that it is available (e.g. as part of NF discovery results or via NF status notification from NRF).

- Mark this AMF as unavailable while not changing the status of UE(s) associated to this AMF (UE(s) previously served by the corresponding AMF still remain registered in the network), and AMF Set information.

- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF that is marked unavailable, CP NF should select another AMF from the same AMF set (as in clause 6.3.5) and forward the transaction together with the old GUAMI. The new AMF retrieves UE context from the UDSF.

NOTE 4: If the CP NF does not subscribe to receive AMF unavailable notification (either directly from the AMF or via NRF), the CP NF may attempt forwarding the transaction towards the old AMF and detect that the AMF is unavailable after certain number of attempts. When it detects unavailable, it marks the AMF and its associated GUAMI(s) as unavailable. CP NF should select another AMF from the same AMF set (as in clause 6.3.5) and forward the transaction together with the old GUAMI. The new AMF retrieves UE context from the UDSF and process the transaction.

Following actions should be performed by the newly selected AMF:

- When there is a transaction with the UE the newly selected AMF retrieves the UE context from the UDSF based on SUPI, 5G-GUTI or AMF UE NGAP ID and processes the UE message accordingly and updates the 5G-GUTI towards the UE. For UE(s) in CONNECTED mode, it may also update the NGAP UE association with a new NGAP-UE-AMF-ID towards the 5G-AN.

- The new selected AMF updates the peer NFs (that subscribed to receive AMF unavailability notification from old AMF), with the new selected AMF information.

- If the new AMF is aware of a different AMF serving the UE (by implementation specific means) it redirects the uplink N2 signalling of the UE to that AMF if necessary, or reject the transaction from the peer CP NFs with a cause to indicate that new AMF has been selected. The peer CP NFs resend the transaction to the new AMF.

NOTE 4: This bullet above addresses situations where 5G-AN node selects an AMF and CP NFs select another AMF for the UE concurrently. It also addresses the situation where CP NFs select an AMF for the UE concurrently

- If the UE is in CM-IDLE state and the new AMF does not have access to the UE context, the new AMF selects one available AMF from the old AMF set as described in clause 6.3.5. The selected AMF retrieves the UE context from the UDSF and provides the UE context to the new AMF. If the new AMF doesn't receive the UE context then the AMF may force the UE to perform initial registration.

5.21.2.2.2 AMF planned removal procedure without UDSF

An AMF can be taken graciously out of service as follows:

- The AMF can forward registered UE contexts, UE contexts grouped by the same GUAMI value, to target AMF(s) within the same AMF set, including the source AMF name used for redirecting UE's MT transaction. The UE context includes the per AMF Set unique AMF NGAP UE ID. If there are ongoing transactions (e.g. N1 procedure) for certain UE(s), AMF forwards the UE context(s) to the target AMF upon completion of an ongoing transaction.
- The AMF deregister itself from NRF indicating due to AMF planned removal.

NOTE 1: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

NOTE 2: Before removal of AMF the overload control mechanism can be used to reduce the amount of ongoing transaction.

An AMF shall be able to instruct the 5G-AN that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF and its corresponding target AMF(s). The target AMF shall be able to update the 5G-AN that the UE(s) served by the old GUAMI(s) are now served by target AMF. The target AMF provides the old GUAMI value that the 5G-AN can use to locate UE contexts served by the old AMF. Upon receipt of the indication that an old AMF is unavailable, 5G-AN shall take the following action:

- 5G-AN should mark this AMF as unavailable and not consider the AMF for selection for subsequent N2 transactions until 5G-AN learns that it is available (e.g. as part of discovery results or by configuration). The associated GUAMIs are marked as unavailable.
- If 5G-AN indicated support of timer capability during NGAP Setup, the AMF may include an additional indicator that the AMF will rebind or release the NGAP UE-TNLA binding on per UE-basis. If that indicator is included and the 5G-AN supports timer mechanism, the 5G-AN starts a timer to control the release of NGAP UE TNLA bindings. For the duration of the timer or until the AMF releases or re-binds the NGAP UE TNLA binding, the AN does not select a new AMF for subsequent transactions. Upon timer expiry, the 5G-AN releases the NGAP UE TNLA-binding(s) with the corresponding AMF for the respective UE(s), for subsequent N2 message, the 5G-AN uses GUAMI which points to the target AMF that replaced the old unavailable AMF, to forward the N2 message to the corresponding target AMF(s).

NOTE 3: For UE(s) in CONNECTED mode, after indicating that the AMF is unavailable for processing UE transactions and including an indicator that the AMF releases the NGAP UE -TNLA binding on a per UE-basis, the AMF can either trigger a re-binding of the NGAP UE associations to an available TNLA on a different AMF within the same AMF set or use the NGAP UE TNLA binding per UE release procedure defined in TS 23.502 [3] to release the NGAP UE-TNLA binding on a per UE-basis while requesting the AN to maintain N3 (user plane connectivity) and UE context information.

If the instruction does not include the indicator, for UE(s) in CONNECTED mode, 5G-AN considers this as a request to release the NGAP UE UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and UE context information. For subsequent N2 message, the 5G-AN uses GUAMI based resolution which points to the target AMF that replaced the old unavailable AMF, to forward the N2 message to the corresponding target AMF(s).

- For UE(s) in IDLE mode, when it subsequently returns from IDLE mode and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI, based resolution the 5G-AN uses 5G S-TMSI or GUAMI which points to the target AMF that has replaced the old unavailable AMF and, the 5G-AN forwards N2 message.

An AMF shall be able to instruct other peer CP NFs, subscribed to receive such a notification, that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF and its corresponding target AMF(s). The target AMF shall update the CP NF that the old GUAMI(s) is now served by target AMF. The old AMF provides the old GUAMI value to target AMF and the target AMF can use to locate UE contexts served by the old AMF. If the CP NFs register with NRF for AMF unavailable notification, then the NRF shall be able to notify the subscribed NFs to receive such a notification (along with the corresponding target AMF(s)) that AMF identified by GUAMI(s) will be unavailable for processing transactions. Upon receipt of the notification that an AMF is unavailable, the other CP NFs shall take the following action:

- Mark this AMF and its associated GUAMI(s) as unavailable while not changing the status of UE(s) associated to this AMF (UE(s) previously served by the corresponding AMF still remain registered in the network), and AMF Set information.
- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF that is marked unavailable and the old unavailable AMF was replaced by the target AMF, CP NF should forward the transaction together with the old GUAMI to the target AMF(s).

NOTE 4: If the CP NF does not subscribe to receive AMF unavailable notification (either directly with the AMF or via NRF), the CP NF may attempt forwarding the transaction towards the old AMF and detect that the AMF is unavailable after certain number of attempts. When it detects unavailable, it marks the AMF and its associated GUAMI(s) as unavailable.

Following actions should be performed by the target AMF:

- To allow AMF process ongoing transactions for some UE(s) even after it notifies unavailable status to the target AMF, the target AMF keeps the association of the old GUAMI(s) and the old AMF for a configured time. During that configured period, if target AMF receives the transaction from the peer CP NFs and cannot locate UE context, it rejects the transaction with old AMF name based on that association, and the indicated AMF is only used for the ongoing transaction. The peer CP NFs resend the transaction to the indicated AMF only for the ongoing transaction. For subsequent transactions, peer CP NFs should use the target AMF. When the timer is expired, the target AMF deletes that association information.
- When there is a transaction with the UE the target AMF uses SUPI, 5G-GUTI or AMF UE NGAP ID to locate UE contexts and processes the UE transactions accordingly and updates the 5G-GUTI towards the UE, if necessary. For UE(s) in CONNECTED mode, it may also update the NGAP UE association with a new NGAP-UE-AMF-ID towards the 5G-AN.
- Target AMF shall not use old GUAMI to allocate 5G-GUTI for UE(s) that are being served by Target AMF.

5.21.2.3 Procedure for AMF Auto-recovery

In order to try and handle AMF failure in a graceful manner (i.e. without impacting the UE), AMF can either back up the UE contexts in UDSF, or per GUAMI granularity in other AMFs (serving as backup AMF for the indicated GUAMI).

NOTE 1: Frequency of backup is left to implementation.

For deployments without UDSF, for each GUAMI the backup AMF information (in association to the GUAMI) is configured in the AMF. The AMF sends this information to 5G-AN and other CP NFs during the N2 setup procedure or the first (per NF) interaction with other CP NFs.

In case an AMF fails and the 5G-AN/peer CP NFs detect that the AMF has failed, or the 5G-AN/peer CP NFs receives notification from another AMF in the same AMF set that this AMF has failed, following actions are taken:

- The OAM deregister the AMF from NRF indicating due to AMF failure.
- 5G-AN marks this AMF as failed and not consider the AMF for selection until explicitly notified.
- For UE(s) in CONNECTED mode, 5G-AN considers failure detection or failure notification as a trigger to release the NGAP UE TNLA binding(s) with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and other UE context information. For subsequent N2 message, if the backup AMF information of the corresponding failed AMF is not available the 5G-AN should select a different AMF (as in clause 6.3.5) from the same AMF set when the subsequent N2 message needs to be sent for the UE(s). If no other AMF from the AMF set is available, then it can select an AMF from the same AMF Region as in clause 6.3.5. If backup AMF information of the corresponding failed AMF is available, the 5G-AN forwards the N2 message to the backup AMF.

NOTE 2: One AMF in the AMF set may be configured to send this failure notification message.

- For UE(s) in IDLE mode, when it subsequently returns from IDLE mode and the 5G-AN receives an initial NAS message with a S-TMSI or GUAMI pointing to an AMF that is marked failed, if the backup AMF information of the corresponding failed AMF is not available the 5G-AN should select a different AMF from the same AMF set and forward the initial NAS message. If no other AMF from the AMF set is available, then it can select an AMF from the same AMF Region as in clause 6.3.5. If backup AMF information of the corresponding failed AMF is available, the 5G-AN forwards the N2 message to the backup AMF.

- Peer CP NFs consider this AMF as unavailable while retaining the UE context.
- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF, if backup AMF information of the corresponding failed AMF is not available, CP NF should select another AMF from the same AMF set and forward the transaction together with the old GUAMI. If backup AMF information of the corresponding failed AMF is available, the CP NF forwards transaction to the backup AMF.
- When the 5G-AN or CP NFs need to select a different AMF from the same AMF set,
  - For deployments with UDSF, any AMF from the same AMF set can be selected.
  - For deployments without UDSF, the backup AMF is determined based on the GUAMI of the failed AMF.

Following actions should be taken by the newly selected AMF:

- For deployments with UDSF, when there is a transaction with the UE the newly selected AMF retrieves the UE context from the UDSF and it processes the UE message accordingly and updates the 5G-GUTI towards the UE, if necessary.
- For deployments without UDSF, backup AMF (the newly selected AMF), based on the failure detection of the old AMF, instructs peer CP NFs and 5G-AN that the UE contexts corresponding to the GUAMI of the failed AMF is now served by this newly selected AMF. The backup AMF shall not use old GUAMI to allocate 5G-GUTI for UE(s) that are being served by Target AMF. The backup AMF uses the GUAMI to locate the respective UE Context(s).
- The new AMF updates the peer NFs (that subscribed to receive AMF unavailability notification from old AMF) with the new AMF information.
- If the new AMF is aware of a different AMF serving the UE (by implementation specific means) it redirects the uplink N2 signalling to that AMF, or reject the transaction from the peer CP NFs with a cause to indicate that new AMF has been selected. The peer CP NFs may wait for the update from the new AMF and resend the transaction to the new AMF.

NOTE 3: This bullet above addresses situations where 5G-AN node selects an AMF and other CP NFs select an AMF for the UE concurrently. It also addresses the situation where CP NFs select an AMF for the UE concurrently.

NOTE 4: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

- If the UE is in CM-IDLE state and the new AMF does not have access to the UE context, the new AMF selects one available AMF from the old AMF set as described in clause 6.3.5. The selected AMF retrieves the UE context from the UDSF and provides the UE context to the new AMF. If the new AMF doesn't receive the UE context then the AMF may force the UE to perform initial registration.

NOTE 5: The above N2 TNL association selection and AMF management is applied to the selected PLMN.

5.22 System Enablers for priority mechanism

5.22.1 General

The 5GS and the 5G QoS model allow classification and differentiation of specific services such as listed in clause 5.16, based on subscription-related and invocation-related priority mechanisms. These mechanisms provide abilities such as invoking, modifying, maintaining, and releasing QoS Flows with priority, and delivering QoS Flow packets according to the QoS characteristics under network congestion conditions.

Subscription-related Priority Mechanisms include the ability of prioritize flows based on subscription information, including the prioritization of RRC connection establishment based on access class barring mechanisms and the establishment of prioritized QoS Flows.

Invocation-related Priority Mechanisms include the ability for the service layer to request/invoke the activation of prioritized QoS Flows through an interaction over Rx/N5 and packet detection in the UPF.

QoS Mechanisms applied to established QoS Flows include the ability to fulfil the QoS characteristics of QoS Flows through preservation of differentiated treatment for prioritized QoS Flow and resource distribution prioritization.

In addition, the separation of concerns between the service classification provided by the core network through the association of Service Data Flows to QoS, and the enforcing of QoS differentiation in (R)AN through the association of QoS Flows to Data Radio bearers, supports the prioritization of QoS Flows when a limitation of the available data radio bearers occurs.

5.22.2 Subscription-related Priority Mechanisms

Subscription-related mechanisms which are always applied:

- (R)AN: During initial RRC Connection Establishment, the Establishment Cause is set to indicate that special treatment is to be applied by the (R)AN in the radio resource allocation as specified in clause 5.2.
- **AMF:** Following RRC Connection Establishment, the receipt of the designated Establishment Cause by the AMF will result in priority handling of the "Initial UE Message" received as part of the Registration procedures of clause 4.2.2 of TS 23.502 [3] and the Service Request procedures of clause 4.2.3 of TS 23.502 [3]. In addition, certain exemptions to Control Plane Congestion and Overload Control are provided as specified in clause 5.19.

Subscription-related mechanisms which are conditionally applied:

- **UE:** When Access Class Barring parameters are broadcast, Access Class Barring based on USIM or other permitted identities is applied prior to an initial upstream transmission for the UE and provides a mechanism to limit transmissions from UEs categorized as non-prioritized, while allowing transmissions from UEs categorized as prioritized (such as MPS subscribed UEs), during the RRC Connection Establishment procedure as specified in clause 5.2.
- **UDM:** One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is set to an appropriate Priority Level. The 5QI for prioritized QoS Flows is set in accordance with the prioritized service requirements, including QoS characteristics used in combination with any non-standard 5QI values.
- **PCF:** The "IMS Signalling Priority" information is set for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling, for each DN which supports prioritized services leveraging on IMS signalling, to an appropriate Priority Level assigned for that service.

5.22.3 Invocation-related Priority Mechanisms

The generic mechanisms used based on invocation-related Priority Mechanisms for prioritised services are based an interaction with an Application Server and between the Application Server and the PCF over Rx/N5 interface, as described in TS 23.228 [15] clause 5.21 in case of MPS using IMS.

NOTE: Clause 5.21 in TS 23.228 [15] is applicable to 5GS, with the understanding that the term PCRF corresponds to PCF in the 5GS.

Invocation-related mechanisms for Mobile Originations e.g. via SIP/IMS:

- PCF: When an indication for a session arrives over the Rx/N5 Interface and the UE does not have priority for the signalling QoS Flow, the PCF derives the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, of the QoS Flow for Signalling as per Service Provider policy as specified in clause 6.1.11.4 of TS 23.203 [4].
- PCF: For sessions such as MPS, when establishing or modifying a QoS Flow for media as part of the session origination procedure, the PCF selects the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to provide priority treatment to the QoS Flow(s).
- PCF: When all active sessions to a particular DN are released, and the UE is not configured for priority treatment to that particular PDU Session for a DN, the PCF will downgrade the IMS Signalling QoS Flows from appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations e.g. via SIP/IMS:

- PCF: When an indication for a session arrives over the Rx/N5 Interface, mechanisms as described above for Mobile Originations are applied.

- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE over a QoS Flow which has an ARP priority level value that is entitled for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N4 interface "Downlink Data Notification" message, as specified in clause 4.2.3.4 of TS 23.502 [3].

- SMF:If a "Downlink Data Notification" message arrives at the SMF containing an ARP priority level value that is entitled for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "Downlink Data Notification" message, as specified in clause 4.2.3.4 of TS 23.502 [3].

- AMF:If a "Downlink Data Notification" message arrives at the AMF containing an ARP priority level value that is entitled for priority use, the AMF handles the request with priority and includes the "Paging Priority" IE in the N2 "Paging" message set to a value assigned to indicate that there is an IP packet at the UPF entitled to priority treatment, as specified in clause 4.2.3.4 of TS 23.502 [3].

- SMF: For a UE that is not configured for priority treatment, upon receiving the "N7 PDU-CAN Session Modification" message from the PCF with an ARP priority level that is entitled for priority use, the SMF sends an "N4 Session Modification Request" to update the ARP for the Signalling QoS Flows, and sends an "N11 SM Request with PDU Session Modification Command" message to the AMF, as specified in clause 4.3.3.2 of TS 23.502 [3].

- AMF: Upon receiving the "N11 SM Request with PDU Session Modification Command" message from the SMF with an ARP priority level that is entitled for priority use, the AMF updates the ARP for the Signalling QoS Flows, as specified in clause 4.3.3.2 of TS 23.502 [3].

- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging in times of congestion at the (R)AN as specified in clause 4.2.3.4 of TS 23.502 [3]. the service receives appropriate priority treatment based on the "Paging Priority" IE.

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF: If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flow(s) controlled by the Priority PDU connectivity services are established/modified to have the service appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, using the PDU Session Modification procedures as specified in clause 4.3.3 of TS 23.502 [3].

- PCF: If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flow(s) controlled by the Priority PDU connectivity services are modified from service appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to those entitled by the UE as per subscription, using the PDU Session Modification procedures as specified in clause 4.3.3 of TS 23.502 [3].

5.22.4 QoS Mechanisms applied to established QoS Flows

Mechanisms applied to established QoS Flows:

- (R)AN: QoS Flows requested in the Xn "Handover Request" or N2 "Handover Request" which are marked as entitled to priority by virtue of inclusion of an ARP value from the set allocated by the Service Provider for prioritised services are given priority over requests for QoS Flows which do not include an ARP from the set as specified in clause 4.9 of TS 23.502 [3].

- SMF: Congestion management procedures in the SMF will provide priority to QoS Flows established for sessions during periods of extreme overload. Prioritised services are exempt from any session management congestion controls. See clause 5.19.

  AMF: Congestion management procedures in the AMF will provide priority to Mobility Management procedures required for the prioritised services during periods of extreme overload. Prioritised services are exempt from mobility restrictions and any Mobility Management congestion controls. See clauses 5.3.4.1.1 and 5.19.4..

QoS Flows whose ARP parameter is from the set allocated by the Service Provider for prioritised services' use shall be exempt from release during QoS Flow load rebalancing.

(R)AN, UPF: IMS Signalling Packets associated with prioritised services' use are handled with priority. Specifically, during times of severe congestion when it is necessary to drop packets on the IMS Signalling QoS Flow to ensure network stability, these FEs shall drop packets not associated with priority signalling such as MPS or Mission Critical services before packets associated with priority signalling. See clause TBD.

- (R)AN, UPF: During times of severe congestion when it is necessary to drop packets on a media QoS Flow to ensure network stability, these FEs shall drop packets not associated with priority sessions such as MPS or Mission Critical services before packets associated with sessions. See clause TBD.

5.23 Supporting for Asynchronous Type Communication

Asynchronous type communication (ATC) enables 5GC to delay synchronizing UE context with the UE, so as to achieve an efficient signalling overhead and increase system capacity.

5GC supports asynchronous type communication with the following functionality:

- Capability to store the UE context based on the received message, and synchronize the UE context with the involved network functions or UE later;

For network function (e.g. PCF, UDM, etc.) triggered signalling procedure (e.g. network triggered Service Request procedure, network triggered PDU Session Modification procedure, etc.), if the UE CM state in the AMF is CM-IDLE state, the AMF updates and stores the UE context based on the received message without paging UE immediately. When the UE CM state in the AMF enters CM-CONNECTED state, the AMF forwards N1 and N2 message to synchronize the UE context with the (R)AN and/or the UE.

6 Network Functions

6.1 General

Clause 6 provides the functional description of the Network Functions in the 5GC, and the principles for Network Function and Network Function Service discovery and selection.

6.2 Network Function Functional description

6.2.1 AMF

The Access and Mobility Management function (AMF) includes the following functionality. Some or all of the AMF functionalities may be supported in a single instance of an AMF:

- Termination of RAN CP interface (N2).
- Termination of NAS (N1), NAS ciphering and integrity protection.
- Registration management.
- Connection management.
- Reachability management.
- Mobility Management.
- Lawful intercept (for AMF events and interface to LI System).
- Provide transport for SM messages between UE and SMF.
- Transparent proxy for routing SM messages.

- Access Authentication.

- Access Authorization.

- Provide transport for SMS messages between UE and SMSF.

- Security Anchor Functionality (SEAF). It interacts with the AUSF and the UE, receives the intermediate key that was established as a result of the UE authentication process. In case of USIM based authentication, the AMF retrieves the security material from the AUSF.

- Security Context Management (SCM). The SCM receives a key from the SEAF that it uses to derive access-network specific keys.

- Location Services management for regulatory services.

- Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF.

- EPS Bearer ID allocation for interworking with EPS.

NOTE 1: Regardless of the number of Network functions, there is only one NAS interface instance per access network between the UE and the CN, terminated at one of the Network functions that implements at least NAS security and Mobility Management.

In addition to the functionalities of the AMF described above, the AMF may include the following functionality to support non-3GPP access networks:

- Support of N2 interface with N3IWF. Over this interface, some information (e.g. 3GPP cell Identification) and procedures (e.g. Hand-Over related) defined over 3GPP access may not apply, and non-3GPP access specific information may be applied that do not apply to 3GPP accesses.

- Support of NAS signalling with a UE over N3IWF. Some procedures supported by NAS signalling over 3GPP access may be not applicable to untrusted non-3GPP (e.g. Paging) access.

- Support of authentication of UEs connected over N3IWF.

- Management of mobility, authentication, and separate security context state(s) of a UE connected via non-3GPP access or connected via 3GPP and non-3GPP accesses simultaneously.

- Support as described in clause 5.3.2.3 a co-ordinated RM management context valid over 3GPP and Non 3GPP accesses.

- Support as described in clause 5.3.3.4 dedicated CM management contexts for the UE for connectivity over non-3GPP access.

NOTE 2: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the AMF described above, the AMF may include policy related functionalities as described in clause 6.2.8 in TS 23.503 [45].

6.2.2 SMF

The Session Management function (SMF) includes the following functionality. Some or all of the SMF functionalities may be supported in a single instance of a SMF:

- Session Management e.g. Session establishment, modify and release, including tunnel maintain between UPF and AN node.

- UE IP address allocation & management (including optional Authorization).

- DHCPv4 (server and client) and DHCPv6 (server and client) functions.

- ARP proxying as specified in IETF RFC 1027 [53] and / or IPv6 Neighbour Solicitation Proxying as specified in IETF RFC 4861 [54] functionality for the Ethernet PDUs. The SMF 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.

- Selection and control of UP function, including controlling the UPF to proxy ARP or IPv6 Neighbour Discovery, or to forward all ARP/IPv6 Neighbour Solicitation traffic to the SMF, for Ethernet PDU Sessions.
- Configures traffic steering at UPF to route traffic to proper destination.
- Termination of interfaces towards Policy control functions.
- Lawful intercept (for SM events and interface to LI System).
- Charging data collection and support of charging interfaces.
- Control and coordination of charging data collection at UPF.
- Termination of SM parts of NAS messages.
- Downlink Data Notification.
- Initiator of AN specific SM information, sent via AMF over N2 to AN.
- Determine SSC mode of a session.
- Roaming functionality:
  - Handle local enforcement to apply QoS SLAs (VPLMN).
  - Charging data collection and charging interface (VPLMN).
  - Lawful intercept (in VPLMN for SM events and interface to LI System).
  - Support for interaction with external DN for transport of signalling for PDU Session authorization/authentication by external DN.

NOTE: Not all of the functionalities are required to be supported in a instance of a Network Slice.

In addition to the functionalities of the SMF described above, the SMF may include policy related functionalities as described in clause 6.2.2 in TS 23.503 [45].

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).
- 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).
- Packet inspection (e.g. Application detection based on service data flow template and the optional PFDs received from the SMF in addition).
- 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.

- ARP proxying as specified in IETF RFC 1027 [53] and / or IPv6 Neighbour Solicitation Proxying as specified in IETF RFC 4861 [54] functionality 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.

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

6.2.4 PCF

The Policy Control Function (PCF) includes the following functionality:

- Supports unified policy framework to govern network behaviour.
- Provides policy rules to Control Plane function(s) to enforce them.
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR).

NOTE: The PCF accesses the UDR located in the same PLMN as the PCF.

The details of the PCF functionality are defined in clause 6.2.1 of TS 23.503 [45].

6.2.5 NEF

The Network Exposure Function (NEF) supports the following independent functionality:

- Exposure of capabilities and events:

  3GPP NFs expose capabilities and events to other NFs via NEF. NF exposed capabilities and events may be securely exposed for e.g. 3rd party, Application Functions, Edge Computing as described in clause 5.13.

  NEF stores/retrieves information as structured data using a standardized interface (Nudr) to the Unified Data Repository (UDR).

NOTE: The NEF can access the UDR located in the same PLMN as the NEF.

- Secure provision of information from external application to 3GPP network:

  It provides a means for the Application Functions to securely provide information to 3GPP network, e.g. Expected UE Behaviour. In that case the NEF may authenticate and authorize and assist in throttling the Application Functions.

- Translation of internal-external information:

  It translates between information exchanged with the AF and information exchanged with the internal network function. For example, it translates between an AF-Service-Identifier and internal 5G Core information such as DNN, S-NSSAI, as described in clause 5.6.7.

  In particular, NEF handles masking of network and user sensitive information to external AF's according to the network policy.

- The Network Exposure Function receives information from other network functions (based on exposed capabilities of other network functions). NEF stores the received information as structured data using a standardized interface to a Unified Data Repository (UDR) (interface to be defined by 3GPP). The stored information can be accessed and "re-exposed" by the NEF to other network functions and Application Functions, and used for other purposes such as analytics.

- A NEF may also support a PFD Function: The PFD Function in the NEF may store and retrieve PFD(s) in the UDR and shall provide PFD(s) to the SMF on the request of SMF (pull mode) or on the request of PFD management from NEF (push mode), as described in TS 23.503 [45].

A specific NEF instance may support one or more of the functionalities described above and consequently an individual NEF may support a subset of the APIs specified for capability exposure.

NOTE: The NEF can access the UDR located in the same PLMN as the NEF.

The services provided by the NEF are specified in clause 7.2.8.

6.2.6 NRF

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

- Supports service discovery function. Receive NF Discovery Request from NF instance, and provides the information of the discovered NF instances (be discovered) to the NF instance.
- Maintains the NF profile of available NF instances and their supported services.

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

- NF instance ID
- NF type
- PLMN ID
- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID
- FQDN or IP address of NF
- NF capacity information
- NF Specific Service authorization information
- Names of supported services
- Endpoint information of instance(s) of each supported service
- Identification of stored data/information

NOTE 1: This is only applicable for a UDR profile. See applicable input parameters for Nnrf_NFManagement_NFRegister service operation in TS 23.502 [3] clause 5.2.7.2.2. This information applicability to other NF profiles is implementation specific.

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

NOTE 2: It is expected service authorization information is usually provided by OA&M system, and it can also be included in the NF profile in case that e.g. an NF instance has an exceptional service authorization information.

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

- PLMN level (the NRF is configured with information for the whole PLMN),
- shared-slice level (the NRF is configured with information belonging to a set of Network Slices),
- slice-specific level (the NRF is configured with information belonging to an S-NSSAI).

NOTE 3: Whether NRF is an enhancement of DNS server is to be determined during Stage 3.

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

- the NRF(s) in the Visited PLMN (known as the vNRF) configured with information for the visited PLMN.
- the NRF(s) in the Home PLMN (known as the hNRF) configured with information for the home PLMN, referenced by the vNRF via the N27 interface,

6.2.7 UDM

The Unified Data Management (UDM) includes support for the following functionality:

- Generation of 3GPP AKA Authentication Credentials.
- User Identification Handling (e.g. storage and management of SUPI for each subscriber in the 5G system).
- Access authorization based on subscription data (e.g. roaming restrictions).
- UE's Serving NF Registration Management (e.g. storing serving AMF for UE, storing serving SMF for UE's PDU Session).
- Support to service/session continuity e.g. by keeping SMF/DNN assignment of ongoing sessions.
- MT-SMS delivery support.
- Lawful Intercept Functionality (especially in outbound roaming case where UDM is the only point of contact for LI).
- Subscription management.
- SMS management.

To provide this functionality, the UDM uses subscription data (including authentication data) that may be stored in UDR, in which case a UDM implements the application logic and does not require an internal user data storage and then several different UDMs may serve the same user in different transactions.

NOTE 1: The interaction between UDM and HSS is implementation specific.

NOTE 2: The UDM is located in the HPLMN of the subscribers it serves, and access the information of the UDR located in the same PLMN.

6.2.8 AUSF

The AUSF supports the following functionality:

- Supports Authentication Server Function (AUSF) as specified by SA WG3.

6.2.9 N3IWF

The functionality of N3IWF in case of untrusted non-3GPP access includes the following:

- Support of IPsec tunnel establishment with the UE: The N3IWF terminates the IKEv2/IPsec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network.
- Termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively.
- Relaying uplink and downlink control-plane NAS (N1) signalling between the UE and AMF.
- Handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS.
- Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.
- Relaying uplink and downlink user-plane packets between the UE and UPF. This involves:
  - De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling
- Enforcing QoS corresponding to N3 packet marking, taking into account QoS requirements associated to such marking received over N2
- N3 user-plane packet marking in the uplink.
- Local mobility anchor within untrusted non-3GPP access networks using MOBIKE per IETF RFC 4555 [57].
- Supporting AMF selection.

6.2.10 AF

The Application Function (AF) interacts with the 3GPP Core Network in order to provide services, for example to support the following:

- Application influence on traffic routing (see clause 5.6.7),
- Accessing Network Exposure Function (see clause 5.20),
- Interacting with the Policy framework for policy control (see clause 5.14),

Based on operator deployment, Application Functions considered to be trusted by the operator can be allowed to interact directly with relevant Network Functions.

Application Functions not allowed by the operator to access directly the Network Functions shall use the external exposure framework (see clause 7.4) via the NEF to interact with relevant Network Functions.

The functionality and purpose of Application Functions are only defined in this specification with respect to their interaction with the 3GPP Core Network.

6.2.11 UDR

The Unified Data Repository (UDR) supports the following functionality:

- Storage and retrieval of subscription data by the UDM.
- Storage and retrieval of policy data by the PCF.
- Storage and retrieval of structured data for exposure, and application data (including Packet Flow Descriptions (PFDs) for application detection, application request information for multiple UEs), by the NEF.

The Unified Data Repository is located in the same PLMN as the NF service consumers storing in and retrieving data from it using Nudr. Nudr is an intra-PLMN interface.

NOTE 1: Deployments can choose to collocate UDR with UDSF.

6.2.12 UDSF

The UDSF is an optional function that supports the following functionality:

- Storage and retrieval of information as unstructured data by any NF.

NOTE: Deployments can choose to collocate UDSF with UDR.

6.2.13 SMSF

The SMSF supports the following functionality to support SMS over NAS:

- SMS subscription checking.
- SM-RP/SM-CP with the UE (see TS 24.011 [6]).
- Relay the SM from UE toward SMS-GMSC/IWMSC/SMS-Router.
- Relay the SM from SMS-GMSC/IWMSC/SMS-Router toward the UE.
- SMS related CDR.
- Lawful Interception.
- Interaction with AMF and SMS-GMSC for notification procedure that the UE is unavailable for SMS transfer (i.e, notifies SMS-GMSC to inform UDM when UE is unavailable for SMS).
- SMS domain selection via UDM by selecting another possible entity for re-attempting MT SM message delivery when the delivery via SMSF fails.

6.2.14 NSSF

The Network Slice Selection Function (NSSF) supports the following functionality:

- Selecting the set of Network Slice instances serving the UE,
- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs,
- Determining the AMF Set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF.

6.2.15 5G-EIR

The 5G-EIR is an optional network function that supports the following functionality:

- Check the status of PEI (e.g. to check that it has not been blacklisted).

6.2.16 LMF

The LMF includes the following functionality:

- Supports location determination for a UE.
- Obtains downlink location measurements or a location estimate from the UE.
- Obtains uplink location measurements from the NG RAN.
- Obtains non-UE associated assistance data from the NG RAN.

6.2.17 SEPP

The Security Edge Protection Proxy (SEPP) is a non-transparent proxy and supports the following functionality:

Message filtering and policing on inter-PLMN control plane interfaces

Topology hiding

Detailed functionality of SEPP, related flows and the N32 reference point, are specified in TS 33.501 [29].

NOTE 1: Since the SEPP is a proxy no service-based interface is needed.

6.3 Principles for Network function and Network Function Service discovery and selection

6.3.1 General

The NF discovery and NF service discovery enables one NF to discover a set of NF instance with specific NF service or a target NF type. NF service discovery is enabled via the NF discovery, as specified in TS 23.502 [3], clause 5.1.1.

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

In order to enable access to a requested NF type or NF service, the requester NF initiates the NF or NF service discovery by providing the type of the NF or the specific service is attempting to discover (e.g. SMF, PCF, UE location Reporting) and other service parameters e.g. slicing related information to discover the target NF. The detailed service parameter(s) used for specific NF discovery refer to the related NF discovery and selection clause.

Depending on the chosen message routing model, the NRF may provide the IP address or the FQDN or the identifier of relevant services and/or NF instance(s) to the requester NF for target NF instance selection. Based on that information, the requester NF can select one specific NF instance or a NF instance that is able to provide a particular NF Service (e.g., an instance of the PCF that can provide Policy Authorization).

For NF discovery across PLMNs, the requester NF provides the NRF the PLMN ID of the target NF. The NRF in the local PLMN reaches the NRF in the target PLMN by forming a target PLMN specific query using the PLMN ID provided by the requester NF.

NOTE 1: See TS 29.510 [58] for details on using the target PLMN ID specific query to reach the NRF in the target PLMN.

For NF discovery across PLMNs in the context of Network Slicing, the NRF in the local PLMN interacts with the appropriate NRF in the target PLMN identified as specified in clause 4.17.5 of TS 23.502 [3] and, for SMF in clause 4.3.2.2.3.3 of TS 23.502 [3].

The NRF in the local PLMN interacts with the NRF in the target PLMN to retrieve the IP address or the FQDN or the identifier of relevant services of the target NF instance (s).

NOTE 2: Due to network topology hiding or network configuration, it is possible that the IP address or the FQDN of proxy function(s) instead of the target NF instance(s) are provided to the requester NF. The proxy function is transparent to the requester NF. The proxy function may further discover the target NF instance via local NRF.

6.3.2 SMF selection function

The SMF selection function is supported by the AMF and is used to allocate an SMF that shall manage the PDU Session.

The SMF selection function in the AMF shall utilize the Network Repository Function to discover the SMF instance(s) unless SMF information is available by other means, e.g. locally configured on AMF. The NRF provides the IP address or the FQDN of SMF instance(s) to the AMF.

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

The SMF selection function in AMF is applicable to both 3GPP access and non-3GPP access.

The following factors may be considered during the SMF selection:

- Selected Data Network Name (DNN).
- S-NSSAI.
- Subscription information from UDM, e.g.
  - per DNN: whether LBO roaming is allowed
  - per S-NSSAI: the subscribed DNN(s)
  - per (S-NSSAI, subscribed DNN): whether LBO roaming is allowed
- Local operator policies.
- Load conditions of the candidate SMFs.
- Access technology being used by the UE

If there is an existing PDU Session for a UE to the same DNN and S-NSSAI used to derive the SMF, the same SMF may be selected. However, different SMF may be selected, for example, to support a SMF load balancing or to support a graceful SMF shutdown (e.g., a SMF starts to no more take new PDU Sessions).

In the home-routed roaming case, the SMF selection function selects an SMF in VPLMN as well as an SMF in HPLMN.

If the UDM provides a subscription context that allows for handling the PDU Session in the visited PLMN (i.e. using LBO) for this DNN and S-NSSAI and, optionally, the AMF is configured to know that the visited VPLMN has a suitable roaming agreement with the HPLMN of the UE, the SMF selection function selects an SMF from the visited PLMN. If an SMF in VPLMN cannot be derived for the DNN and S-NSSAI, or if the subscription does not allow for handling the PDU Session in visited PLMN using LBO, then both a SMF in VPLMN and SMF in HPLMN are selected, and the DNN and S-NSSAI is used to derive an SMF identifier from the HPLMN.

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

6.3.3 User Plane Function Selection

The selection and reselection of the UPF 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.

SMF may be locally configured with the information about the available UPFs, e.g. by OA&M system when UPF is instantiated or removed.

NOTE 1: UPF information can be updated e.g. by OA&M system any time after the initial provisioning, or UPF itself updates its information to the SMF any time after the node level interaction is established.

The UPF selection functionality in the SMF may optionally utilize the NRF to discover UPF instance(s). In this case, the SMF issues a request to the NRF that may include following parameters: DNN, S-NSSAI. In its answer, the NRF provides the IP address or the FQDN of corresponding UPF instance(s) to the SMF and may also provide the SMF with additional information to aid UPF selection such as UPF location, UPF capacity, and UPF optional functionalities and capabilities.

The NRF may be configured by OAM with information on the available UPF(s) or the UPF may register itself onto the NRF.

For home routed roaming case, the UPF(s) in home PLMN is selected by SMF(s) in H-PLMN, and the UPF(s) in visited PLMN is selected by SMF(s) in V-PLMN. The exact set of parameters used for the selection mechanism is deployment specific and controlled by the operator configuration, e.g. location information may be used for selecting UPF in some deployments while may not be used in other deployments.

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

- UPF's dynamic load.
- 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.
- Data Network Name (DNN).
- PDU Session Type (i.e. IPv4, IPv6, 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.
- 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.

The SMF, when selecting a UPF for a PDU Session or when analysing whether to reselect a UPF of an ongoing PDU session, shall be able to use information such as:

- 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;
- information regarding the N9 User Plane termination(s) of UPF(s) if needed;
- information regarding the User plane termination(s) corresponding to the DNAI(s).

Editor's note: To select UPF the SMF needs some "information on the User Plane connectivity between UPF(s), AN(s) and sub-networks supporting DNAI(s); the following is under debate:

What information 3gpp specifications define for this purpose: e.g. the full link/router topology between AN and UPF and DNAI or only UP addressing information (FQDN / IP addresses) or other information.

How the SMF gets this information: candidate source of such information are N4, NRF and OAM.

6.3.4 AUSF selection function

The AMF performs AUSF selection to allocate an AUSF that performs authentication between the UE and 5G CN in the HPLMN.

The AUSF selection function in the AMF shall utilize the NRF to discover the AUSF instance(s) unless AUSF information is available by other means, e.g. locally configured on AMF, and select an AUSF instance based on the obtained AUSF information

The AUSF selection function in AMF is applicable to both 3GPP access and non-3GPP access.

The following factors may be considered during the AUSF selection:

- SUPI.
- Home network identifier (e.g., MNC and/or MCC) of SUCI.

6.3.5 AMF selection

The AMF selection functionality is applicable to both 3GPP access and non-3GPP access. The AMF selection functionality can be supported by the 5G-AN (e.g. RAN, N3IWF) and is used to select an AMF for a given UE. An AMF supports the AMF selection functionality to select an AMF for relocation or because the initially selected AMF was not an appropriate AMF to serve the UE (e.g. due to change of Allowed NSSAI). Other CP NF(s), e.g. SMF, supports the AMF selection functionality to select an AMF from the AMF set when the original AMF serving a UE is unavailable.

5G-AN selects an AMF Set and an AMF from the AMF Set under the following circumstances:

1) When the UE provides no 5G-S-TMSI nor the GUAMI to the 5G-AN.
2) When the UE provides 5G-S-TMSI or GUAMI but the routing information (i.e. AMF identified based on AMF Set ID, AMF pointer) present in the 5G-S-TMSI or GUAMI is not sufficient and/or not usable (e.g. UE provides GUAMI with an AMF region ID from a different region).
3) AMF has instructed AN that the AMF (identified by GUAMI(s)) is unavailable and no target AMF is identified and/or AN has detected that the AMF has failed.

Other CP NFs selects an AMF from the AMF Set under the following circumstances:

4) When the AMF has instructed CP NF that a certain AMF identified by GUAMI(s) is unavailable and the CP NF was not notified of target AMF, and/or CP NF has detected that the AMF has failed.

The AMF selection functionality in the 5G-AN may consider the following factors for selecting the AMF Set:

- AMF Region ID and AMF Set ID derived from GUAMI.
- Requested NSSAI.

- Local operator policies.

AMF selection functionality in the 5G-AN or CP NFs considers the following factors for selecting an AMF from AMF Set:

- Availability of candidate AMFs.

- Load balancing across candidate AMFs (e.g. considering weight factors of candidate AMFs in the AMF Set).

When 5G-S-TMSI or GUAMI is provided by the UE to the 5G-AN contains an AMF Set ID that is usable, and the AMF identified by AMF pointer that is not usable (e.g. AN detects that the AMF has failed) or the corresponding AMF indicates it is unavailable (e.g. out of operation) then the 5G-AN uses the AMF Set ID for selecting another AMF from the AMF set considering the factors above.

The AMF selection functionality in the AMF or other CP NFs shall utilize the NRF to discover the AMF instance(s) unless AMF information is available by other means, e.g. locally configured on AMF or other CP NFs. The NRF provides the IP address or the FQDN of AMF instance(s) to the AMF or other CP NFs. In the context of Network Slicing, the AMF selection is described in clause 5.15.5.2.1.

- AMF selection functionality in AMF or other CP NFs use GUAMI to discover the AMF instance, the NRF provides the IP address, or the FQDN of the associated AMF instance if it is available. If the associated AMF is unavailable due to AMF planned removal, the backup AMF used for planned removal is provided. If the associated AMF is unavailable due to AMF failure, the backup AMF used for failure is provided. If none of AMF related to the indicated GUAMI can be found or no indicated GUAMI, a list of candidate AMF instances in the same AMF Set together with additional information (e.g. priority) is provided.

- AMF selection functionality in AMF use AMF Set ID to discover the AMF instance(s), the NRF provides a list of AMF instances in the same AMF Set together with additional information (e.g. priority).

- At intra-PLMN mobility, the AMF selection functionality in source AMF use source AMF Set ID, source AMF Region ID, and the target location information, S-NSSAI(s) of Allowed NSSAI to discover target AMF instance(s). The NRF provides the target AMF instance belonged to the target AMF set in target AMF Region which can be the mapping of the source AMF set in source AMF region.

- At inter PLMN mobility, the source AMF selects an AMF in the target PLMN via the PLMN level NRF. After the handover procedure the AMF may select a different AMF as specified in clause 4.2.2.2.3 in TS 23.502 [3].

6.3.6 N3IWF selection

6.3.6.1 General

When the UE supports connectivity with N3IWF but does not support connectivity with ePDG, as specified in TS 23.402 [43], the UE shall perform the procedure in clause 6.3.6.2 for selecting an N3IWF.

When the UE supports connectivity with N3IWF, as well as with ePDG, as specified in TS 23.402 [43], the UE shall perform the procedure in clause 6.3.6.3 for selecting either an N3IWF or an ePDG, i.e. for selecting a non-3GPP access node.

6.3.6.2 Stand-alone N3IWF selection

The UE performs N3IWF selection based on the ePDG selection mechanism as specified in the TS 23.402 [43] clause 4.5.4 except for the following differences:

- The Tracking/Location Area Identifier FQDN shall be constructed by the UE based only on the Tracking Area wherein the UE is located. The Location Area is not applicable on the 3GPP access.

- The ePDG FQDN format is substituted by with N3IWF FQDN format as specified in TS 23.003 [19].

- The ePDG identifier configuration and the ePDG selection information are substituted by the N3IWF identifier configuration and the N3IWF selection information respectively.

Network slice information cannot be used for N3IWF selection in this release.

6.3.6.3 Combined N3IWF/ePDG Selection

6.3.6.3.1 General

The N3IWF selection procedure is based on the ePDG selection mechanism specified in TS 23.402 [43], clause 4.5.4, enhanced to accommodate the N3IWF, as well as to support selection in PLMNs where both non-3GPP access node types (i.e. ePDG and N3IWF) are available.

For this purpose, the following modifications are introduced:

1) The N3IWF FQDN formats, similar to the corresponding ePDG FQDN formats defined in TS 23.003 [19]:

    - N3IWF Operator Identifier based FQDN; and

    - N3IWF Tracking Area Identity based FQDN.

Editor's note: The reference to TS 23.003 [19] might be revised if the definitions related to N3IWF are included in a different TS.

2) The N3IWF selection information, identical to the ePDG selection information defined in TS 23.402 [43], clause 4.5.4, for use in the stand-alone N3IWF selection procedure described in clause 6.3.6.2.

3) The Non-3GPP Access (N3A) selection information, based on the ePDG selection information defined in TS 23.402 [43], clause 4.5.4 extended for use in the combined ePDG/N3IWF selection procedure described in clause 6.3.6.3.2. The extension includes the N3IWF parameters similar to the respective ePDG parameters, as well as an additional parameter per PLMN in the selection information list:

    - The "Preference" parameter defining operator's preference for a specific non-3GPP access node type when both ePDG and N3IWF are supported.

Editor's note: The use of selection criteria other than the configured "preference", e.g. selecting the access to the same core network the UE is attached to over the 3GPP access, needs to be evaluated. The "preference" alone may be not enough to support transition options from ePDG based access to N3IWF based access other than an atomic switch-over for entire PLMN.

4) The N3IWF Identifier, similar in purpose and format to the ePDG Identifier defined in TS 23.402 [43], clause 4.5.4.

The "Preference" parameter described in point 3) above is also configured separately for HPLMN outside of the N3A selection information for use in the combined ePDG/N3IWF selection procedure described in clause 6.3.6.3.2 when the selection is based on the ePDG/N3IWF Identifiers, according to TS 23.402 [43], clause 4.5.4.

6.3.6.3.2 Combined N3IWF/ePDG Selection Procedure

The present procedure follows the logic specified in the ePDG selection procedure in TS 23.402 [43], clauses 4.5.4.4 and 4.5.4.5, to identify a candidate PLMN for non-3GPP access selection.

For identified candidate PLMN the selection performs as follows:

1. The UE shall determine if the non-3GPP access node selection is for an IMS service or for a non-IMS service. The means of that determination is implementation-specific.

2. For the IMS service, the UE shall choose a non-3GPP access node type (i.e. ePDG or N3IWF) based on the "Preference" parameter specified in clause 6.3.6.3.1, unless the UE has its 5GS capability disabled in which case it shall choose ePDG independent of the "Preference" parameter setting.

    The resulting non-3GPP access node type choice is used for the selection.

    If the selection fails, including the case when during the registration over non-3GPP access the UE receives the IMS Voice over PS session Not Supported over Non-3GPP Access indication (specified in clause 5.16.3.2a), the UE attempts selecting the other non-3GPP access node type defined for that PLMN, if any. If that selection fails or is not possible, the UE proceeds to the next PLMN, according to the mechanism specified in TS 23.402 [43], clause 4.5.4.5.

3. For the non-IMS service, the UE shall perform the selection by giving preference to the N3IWF independent of the "Preference" parameter setting. If N3IWF selection fails or is not possible, the UE should attempt selecting an ePDG in the same PLMN, if configured. If ePDG selection fails or is not possible the UE proceeds to the next PLMN, according to the mechanism specified in TS 23.402 [43], clause 4.5.4.5.

NOTE: A UE performing both selections for an IMS service and for a non-IMS service could get simultaneously attached to non-3GPP access nodes of both type (i.e. to a N3IWF and an ePDG) in the same PLMN or in different PLMNs.

6.3.7 PCF selection

Editor's note: Potential relation with slicing are FFS.

6.3.7.0 General principles

Clause 6.3.7.10 describes the underlying principles for PCF selection and discovery:

- There may be multiple and separately addressable PCFs in a PLMN.
- The PCF must be able to correlate the AF service session established over N5 or Rx with the associated PDU Session (Session binding) handled over N7.
- It shall be possible to deploy a network so that the PCF may serve only specific DN(s). For example, Policy Control may be enabled on a per DNN basis.
- Unique identification of a PDU Session in the PCF shall be possible based on the (UE ID, DNN)-tuple, the (UE IP Address(es), DNN)-tuple and the (UE ID, UE IP Address(es), DNN).

6.3.7.1 PCF selection for a UE or a PDU Session

The AMF selects the PCF for a UE, the SMF selects the PCF for a PDU Session. The selected PCF may be the same or may be a different one, following one of the alternatives below:

- The AMF utilizes the NRF to discover the PCF instance(s) for a UE unless PCF information is available by other means, e.g. locally configured on AMF based on operator policies.
- The SMF utilizes the NRF to discover the PCF instance(s) for a PDU Session unless PCF information is available by other means, e.g. locally configured on SMF or received from the AMF. The following factors may be considered during the PCF selection by the SMF:

  a) Local operator policies.

  b) Selected Data Network Name (DNN).

  c) PCF selected by the AMF. This is to select the same PCF for the AMF and the SMF.

6.3.7.2 Providing policy requirements that apply to multiple UE and hence to multiple PCF

An authorized Application Function may, via the NEF, provide policy requirements that apply to multiple UE (which, for example, belong to group of UE(s) defined by subscription or to any UE) and hence may apply to multiple PCF.

NOTE: Application Function influence on traffic routing described in clause 5.6.7 is an example of such requirement.

After relevant validation of the AF request (and possible parameter mapping), the NEF stores this request received from the AF. The possible parameter mapping includes mapping UE (group) identifiers provided by the AF to identifiers used within the 5GC, e.g. from GPSI to SUPI and/or from External Group Identifier to IMSI-Group Identifier. When UDR(s) are deployed, NEF stores the AF request into the selected UDR.

PCF(s) that need to receive AF requests that targets a DNN (and slice), and / or a group of UEs subscribe to receive notifications from the NEF about such AF request information. When UDR(s) are deployed and store(s) AF requests, the PCF(s) can be configured (e.g. by OAM) to subscribe to receive notification of such AF request information directly from the UDR(s). The PCF(s) take(s) the received AF request information into account when making policy decisions for existing and future relevant PDU Sessions. In the case of existing PDU Sessions, the PCF's policy decision may trigger a PCC rule change from the PCF to the SMF.

The PCF subscription to notifications of AF requests (from the NEF or the UDR(s)) described above take place during PDU Session establishment or PDU Session modification, when the PCF(s) receive request from the SMF for policy information related to the DNN (and slice), and/or the group of UEs. For the PCF(s) that have subscribed to such notifications, the UDR(s) notify the PCFs of any AF request update.

The NEF associates the AF request with information allowing to later modify and delete the AF request; it associates the AF request with:

- When the AF request targets PDU Sessions established by "any UE": the DNN, the slicing information target of the AF request,
- When the request targets PDU Sessions established by UE within a predefined/subscribed group of UE: the DNN, the slicing information and the group of UE target of the application request.
- The AF transaction identifier in the AF request.

6.3.7.3 Binding an AF request targeting an IP address to the relevant PCF

The BSF is used for binding an AF request to the relevant PCF as described in TS 23.503 [45].

6.3.8 UDM discovery function

The NF consumer performs UDM discovery to discover a UDM that manages the user subscriptions in the HPLMN.

The UDM discovery function shall utilize the NRF to discover the UDM instance(s) unless UDM information is available by other means, e.g. locally configured on NF consumers, and select a UDM instance based on the obtained UDM information. The UDM discovery function in NF consumers is applicable to both 3GPP access and non-3GPP access.

One of the following factors may be used during the UDM discovery:

- Home network identifier (e.g. MNC and/or MCC) of SUPI.
- GPSI (e.g., by the NEF/PCF if received in AF requests)
- Home network identifier (e.g. MNC and/or MCC) of SUCI

Editor's note: Whether SUCI needs to be considered during the UDM discovery depends on the conclusion of SA3 work.

6.3.9 UDR discovery and selection function

Multiple instances of UDR may be deployed, each one storing specific data or providing service to a specific set of NF consumers as described in clause 4.2.5.

The NF consumer shall utilize the NRF to discover the appropriate UDR instance(s) unless UDR instance information is available by other means, e.g. locally configured on NF consumer. The NF consumer shall select a UDR instance based on this information. The UDR discovery function in NF consumers is applicable to both 3GPP access and non-3GPP access.

The NF consumer shall select a UDR instance that contains relevant information for the consumer, e.g. UDM selects a UDR instance that contains subscription data, while NEF (when used to access data for exposure) selects a UDR that contains data for exposure; or PCF selects a UDR that contains Policy Data and/or Application Data.

The following factors shall be considered for UDR discovery and selection:

- SUPI or GPSI or External Group Identifier.
- A Data Set Identifier (see UDR service definition in TS 23.502 [3] clause 5.2.12).

7 Network Function Services and descriptions

7.1 Network Function Service Framework

7.1.1 General

An NF service is one type of capability exposed by an NF (NF Service Producer) to other authorized NF (NF Service Consumer) through a service-based interface. Network Function may expose one or more NF services. Following are criteria for specifying NF services:

- NF services are derived from the system procedures that describe end to end functionality, where applicable (see 3GPP TS 23.502 [3], Annex B drafting rules). Services may also be defined based on information flows from other 3GPP specifications.

- System procedures can be described by a sequence of NF service invocations.

NOTE: While the use of NF services is not restricted to the identified consumers, no specific effort will be made in this release of the specification, to develop the description of NF services beyond what is necessary to support their use in information flows.

7.1.2 NF Service Consumer-NF Service Producer interactions

The interaction between two Network Functions (Consumer and Producer) within this NF service framework follows two mechanisms:

- "Request-response": A Control Plane NF_B (NF Service Producer) is requested by another Control Plane NF_A (NF Service Consumer) to provide a certain NF service, which either performs an action or provides information or both. NF_B provides NF service based on the request by NF_A. In order to fulfil the request, NF_B may in turn consume NF services from other NFs. In Request-response mechanism, communication is one to one between two NFs (consumer and producer) and a one-time response from producer to a request from consumer is expected within a certain timeframe.

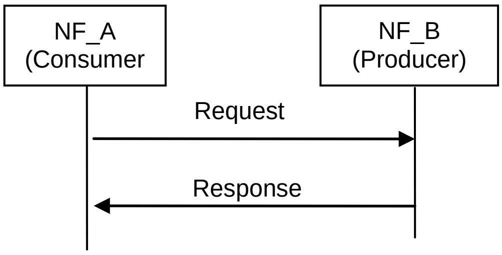


Figure 7.1.2-1: "Request-response" NF Service illustration

- "Subscribe-Notify": A Control Plane NF_A (NF Service Consumer) subscribes to NF Service offered by another Control Plane NF_B (NF Service Producer). Multiple Control Plane NFs may subscribe to the same Control Plane NF Service. NF_B notifies the results of this NF service to the interested NF(s) that subscribed to this NF service. The subscription request shall include the notification endpoint (e.g. the notification URL) of the NF Service Consumer to which the event notification from the NF Service Producer should be sent to. In addition, the subscription request may include notification request for periodic updates or notification triggered through certain events (e.g., the information requested gets changed, reaches certain threshold etc.). The subscription for notification can be done through one of the following ways:

- A separate request/response exchange between the NF Service Consumer and the NF Service Producer; or

- The subscription for notification is included as part of another NF service operation of the same NF Service; or

- Registration of a notification endpoint for each type of notification the NF consumer is interested to receive, as a NF service parameter with the NRF during the NF and NF service registration procedure as specified in TS 23.502 [3] clause 4.17.1.

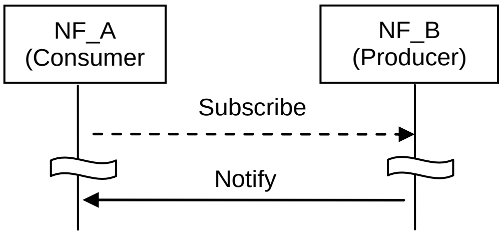


Figure 7.1.2-2: "Subscribe-Notify" NF Service illustration 1

A Control Plane NF_A may also subscribe to NF Service offered by Control Plane NF_B on behalf of Control Plane NF_C, i.e. it requests the NF Service Producer to send the event notification to another consumer(s). In this case, NF_A includes the notification endpoint of the NF_C in the subscription request.

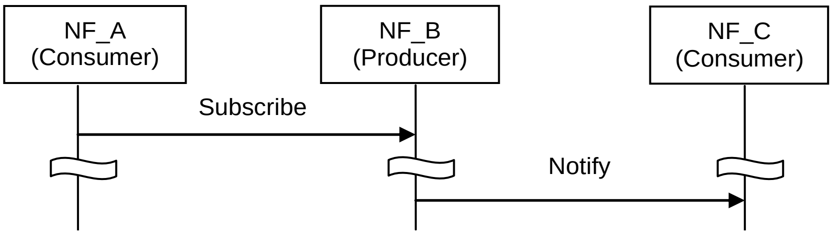


Figure 7.1.2-3: "Subscribe-Notify" NF Service illustration 2

7.1.3 Network Function Service discovery

A Control Plane Network function (NF) within the 5G Core network may expose its capabilities as services via its service based interface, which can be re-used by Control Plane CN NFs.

The NF service discovery enables a CN NFs to discover NF instance(s) that provide the expected NF service(s). The NF service discovery is implemented via the NF discovery functionality.

For more detail NF discovery refer to clause 6.3.1.

7.1.4 Network Function Service Authorization

NF service authorization shall ensure the NF Service Consumer is authorized to access the NF service provided by the NF Service Provider, according to e.g. the policy of NF, the policy from the serving operator, the inter-operator agreement.

Service authorization information shall be configured as one of the components in NF profile of the NF Service Producer. It shall include the NF type (s) and NF realms/origins allowed to consume NF Service(s) of NF Service Producer.

Due to roaming agreements and operator policies, a NF Service Consumer shall be authorised based on UE/subscriber/roaming information and NF type, the Service authorization may entail two steps:

- Check whether the NF Service Consumer is permitted to discover the requested NF Service Producer instance during the NF service discovery procedure. This is performed on a per NF granularity by NRF.

NOTE 1: When NF discovery is performed based on local configuration, it is assumed that locally configured NFs are authorized.

- Check whether the NF Service Consumer is permitted to access the requested NF Service Producer for consuming the NF service, with a request type granularity. This is performed on a per UE, subscription or roaming agreements granularity. This type of NF Service authorization shall be embedded in the related NF service logic.

NOTE 2: The security of the connection between NF Service Consumer and NF Service Producer is specified in SA WG3.

NOTE 3: It is expected that an NF authorisation framework exists in order to perform consumer NF authorisation considering UE, subscription or roaming agreements granularity. This authorisation is assumed to be performed without configuration of the NRF regarding UE, subscription or roaming information.

7.1.5 Network Function and Network Function Service registration and de-registration

For the NRF to properly maintain the information of available NF instances and their supported services, each NF instance informs the NRF of the list of NF services that it supports.

NOTE: The NF informs the appropriate NRF based on configuration.

The NF instance may make this information available to NRF when the NF instance becomes operative for the first time (registration operation) or upon individual NF service instance activation/de-activation within the NF instance (update operation) e.g. triggered after a scaling operation. The NF instance while registering the list of NF services it supports, for each NF service, may provide a notification endpoint information for each type of notification service that the NF service is prepared to consume, to the NRF during the NF instance registration. The NF instance may also update or delete the NF service related parameters (e.g. to delete the notification endpoint information). Alternatively, another authorised entity (such as an OA&M function) may inform the NRF on behalf of an NF instance triggered by an NF service instance lifecycle event (register or de-registration operation depending on instance instantiation, termination, activation, or de-activation). Registration with the NRF includes capacity and configuration information at time of instantiation.

The NF instance may also de-registers from the the NRF when it's about to gracefully shut down or disconnect from the network in a controlled way. If an NF instance become unavailable or unreachable due to unplanned errors (e.g. NF crashes or there are network issues), an authorised entity shall deregister the NF instance with the NRF.

7.2 Network Function Services

7.2.1 General

In the context of this specification, an NF service is offering a capability to authorised consumers.

Network Functions may offer different capabilities and thus, different NF services to distinct consumers. Each of the NF services offered by a Network Function shall be self-contained, reusable and use management schemes independently of other NF services offered by the same Network Function (e.g. for scaling, healing, etc).

NOTE: There can be dependencies between NF services within the same Network Function due to sharing some common resources, e.g. context data. This does not preclude that NF services offered by a single Network Function are managed independently of each other.

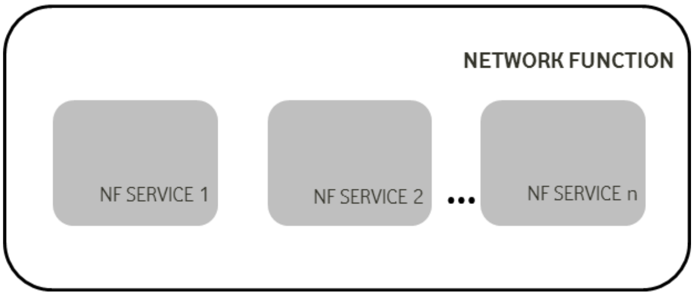


Figure 7.2.1-1: Network Function and NF Service

Each NF service shall be accessible by means of an interface. An interface may consist of one or several operations.

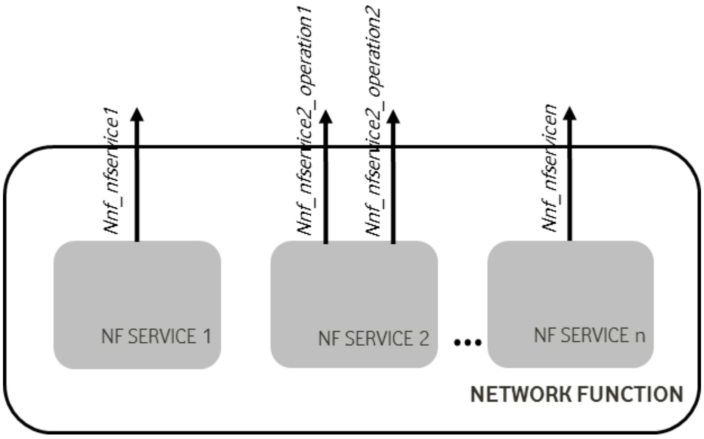


Figure 7.2.1-2: Network Function, NF Service and NF Service Operation

System procedures, as specified in TS 23.502 [3] can be built by invocation of a number of NF services. The following figure shows an illustrative example on how a procedure can be built; it is not expected that system procedures depict the details of the NF Services within each Network Function.

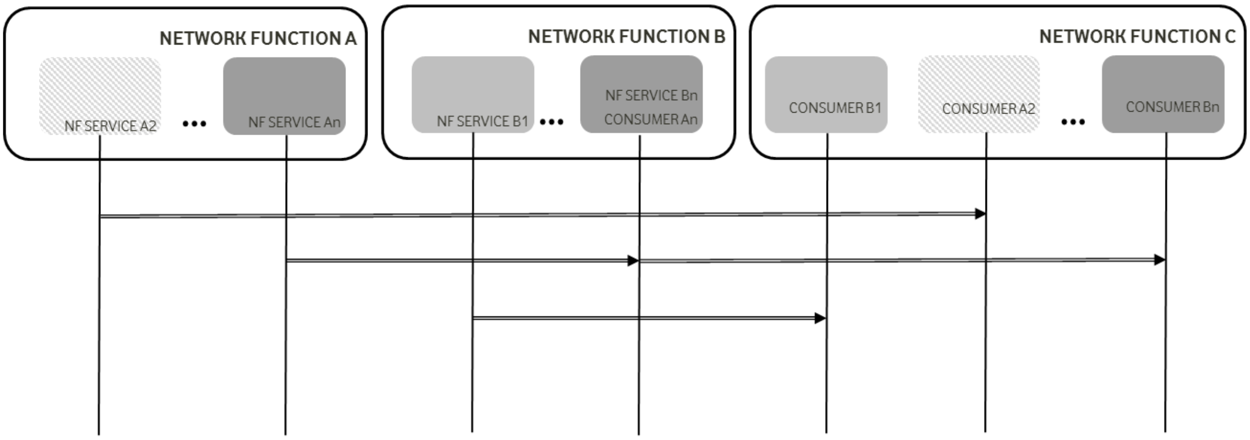


Figure 7.2.1-3: System Procedures and NF Services

The following subsections provide for each NF the NF services it exposes through its service based interfaces.

7.2.2 AMF Services

The following NF services are specified for AMF:

Table 7.2.2-1: NF Services provided by AMF

Service Name	Description	Reference in TS 23.502 [3]
Namf_Communication	This service enables an NF to communicate with the UE and/or the AN through the AMF. This service enables SMF to request EBI allocation to support interworking with EPS.	5.2.2.2
Namf_EventExposure	This service enables other NFs to subscribe or get notified of the mobility related events and statistics.	5.2.2.3
Namf_MT	This service enables an NF to make sure UE is reachable.	5.2.2.4

7.2.3 SMF Services

The following NF services are specified for SMF:

Table 7.2.3-1: NF Services provided by SMF

Service Name	Description	Reference in TS 23.502 [3]
Nsmf_PDUSession	This service manages the PDU Sessions and uses the policy and charging rules received from the PCF. The service operations exposed by this NF service allows the consumer NFs to handle the PDU Sessions.	Clause 5.2.8.2
Nsmf_EventExposure	This service exposes the events happening on the PDU Sessions to the consumer NFs.	Clause 5.2.8.3

7.2.4 PCF Services

The following NF services are specified for PCF:

Table 7.2.4-1: NF Services provided by PCF

Service Name	Description	Reference in TS 23.502 [3]
Npcf_AMPolicyControl	This PCF service provides Access Control, network selection and Mobility Management related policies, UE Route Selection Policies to the NF consumers.	5.2.5.2
Npcf_SMPolicyControl	This PCF service provides session related policies to the NF consumers.	5.2.5.4
Npcf_Policy Authorization	This PCF service authorises an AF request and creates policies as requested by the authorised AF for the PDU Session to which the AF session is bound to. This service allows the NF consumer to subscribe/unsubscribe to the notification of Access Type and RAT type, PLMN identifier, access network information, usage report etc.	5.2.5.3
Npcf_BDTPolicyControl	This PCF service provides background data transfer policy to the NF consumers	5.2.5.5

7.2.5 UDM Services

The following NF services are specified for UDM:

Table 7.2.5-1: NF Services provided by UDM

Service Name	Description	Reference in TS 23.502 [3]
Nudm_UE Context Management	1. Provide the NF consumer of the information related to UE's transaction information, e.g. UE's serving NF identifier, UE status, etc. 2. Allow the NF consumer to register and deregister its information for the serving UE in the UDM. 3. Allow the NF consumer to update some UE context information in the UDM.	5.2.3.2
Nudm_Subscriber Data Management	1. Allow NF consumer to retrieve user subscription data when necessary 2. Provide updated user subscriber data to the subscribed NF consumer;	5.2.3.3
Nudm_UEAuthentication	1. Provide updated authentication related subscriber data to the subscribed NF consumer.	5.2.3.4
Nudm_EventExposure	1. Allow NF consumer to subscribe to receive an event. 2. Provide monitoring indication of the event to the subscribed NF consumer.	5.2.3.5

7.2.6 NRF Services

The following NF services are specified for NRF:

Table 7.2.6-1: NF Services provided by NRF

Service Name	Description	Reference in TS 23.502 [3]
Nnrf_NFManagement	Provides support for register, deregister and update service to NF, NF services. Provide consumers with notifications of newly registered NF along with its NF services.	5.2.7.2
Nnrf_NFDiscovery	Enables one NF service consumer to discover a set of NF instances with specific NF service or a target NF type. Also enables one NF service to discover a specific NF service.	5.2.7.3

7.2.7 AUSF Services

The following NF services are specified for AUSF:

Table 7.2.7-1: NF Services provided by AUSF

Service Name	Description	Reference in TS 23.502 [3]
Nausf UEauthentication	The AUSF provides UE authentication service to requester NF	5.2.10.1

7.2.8 NEF Services

The following NF services are specified for NEF:

Table 7.2.8-1: NF Services provided by NEF

Service Name	Description	Reference in TS 23.502 [3]
Nnef_EventExposure	Provides support for event exposure	

7.2.9 SMSF Services

The following NF services are specified for SMSF:

Table 7.2.9-1: NF Services provided by SMSF

Service Name	Description	Reference in TS 23.502 [3]
Nsmsf_ SMService	This service allows AMF to authorize SMS and activate SMS for the served user on SMSF.	5.2.9.1

7.2.10 UDR Services

The following NF services are specified for UDR:

Table 7.2.10-1: NF Services provided by UDR

Service Name	Description	Reference in TS 23.502 [3]
Nudr_Unified Data Management	This service allows NF service consumers to retrieve, create, update, subscribe for change notifications, unsubscribe for change notifications and delete data stored in the UDR, based on the set of data applicable to the consumer. This service may also be used to manage operator specific data.	5.2.11

7.2.11 5G-EIR Services

The following NF services are specified for 5G-EIR:

Table 7.2.11-1: NF Services provided by 5G-EIR

Service Name	Description	Reference in TS 23.502 [3]
N5g-eir_Equipment Identity Check	This service enables the 5G-EIR to check the PEI and check whether the PEI is in the black list or not.	Clause 4.2.2.2.2

7.2.12 NWDAF Services

The following NF services are specified for NWDAF:

Table 7.2.12-1: NF Services provided by NWDAF

Service Name	Description	Reference in TS 23.502 [3]
Nnwdaf_Events_Subscription	This service enables the NF service consumers to subscribe/unsubscribe for different type of analysis information (i.e., load level information of Network Slice instance) from NWDAF.	5.2.11.2
Nnwdaf_Analytics_Info	This service enables the NF service consumers to request and get different type of analysis information (i.e., load level information of Network Slice instance) s from NWDAF.	5.2.11.3

7.2.13 UDSF Services

The following NF services are specified for UDSF:

Table 7.2.13-1: NF Services provided by UDSF

Service Name	Description	Reference in TS 23.502 [3]	Example Consumer
Unstructured Data Management	This service allows NF service consumers to retrieve, create, update, and delete data stored in the UDSF.	5.2.14	Any NF

7.2.14 NSSF Services

The following NF services are specified for NSSF:

Table 7.2.14-1: NF Services provided by NSSF

Service Name	Description	Reference in TS 23.502 [3]	Example Consumer
Nnssf_NSSelection	Provides the requested Network Slice information to the Requester.	5.2.13	AMF, NSSF in a different PLMN, NRF

7.3 Exposure

Network exposure is described in clause 5.20 and in TS 23.502 [3] clause 4.15.

8 Control and User Plane Protocol Stacks

8.1 General

Clause 8 specifies the overall protocol stacks between 5GS entities, e.g. between the UE and the 5GC Network Functions, between the 5G-AN and the 5GC Network Functions, or between the 5GC Network Functions.

8.2 Control Plane Protocol Stacks

8.2.1 Control Plane Protocol Stacks between the 5G-AN and the 5G Core: N2

8.2.1.1 General

NOTE 1: N2 maps to NG-C as defined in TS 38.413 [34].

Following procedures are defined over N2:

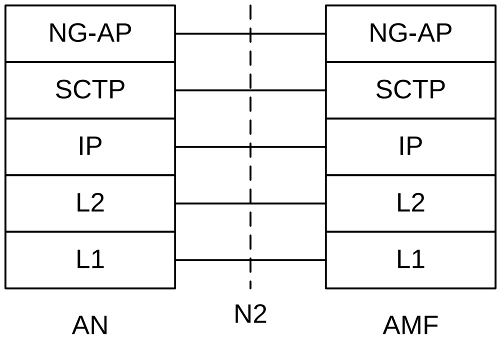
- Procedures related with N2 Interface Management and that are not related to an individual UE, such as for Configuration or Reset of the N2 interface. These procedures are intended to be applicable to any access but may correspond to messages that carry some information only on some access (such as information on the default Paging DRX used only for 3GPP access).
- Procedures related with an individual UE:
  - Procedures related with NAS Transport. These procedures are intended to be applicable to any access but may correspond to messages that for UL NAS transport carry some access dependent information such as User Location Information (e.g. Cell-Id over 3GPP access or other kind of User Location Information for Untrusted Non 3GPP access).
  - Procedures related with UE context management. These procedures are intended to be applicable to any access. The corresponding messages may carry:
    - some information only on some access (such as Handover Restriction List used only for 3GPP access).
    - some information (related e.g. with N3 addressing and with QoS requirements) that is to be transparently forwarded by AMF between the 5G-AN and the SMF.
  - Procedures related with resources for PDU Sessions. These procedures are intended to be applicable to any access. They may correspond to messages that carry information (related e.g. with N3 addressing and with QoS requirements) that is to be transparently forwarded by AMF between the 5G-AN and the SMF.
  - Procedures related with Hand-Over management. These procedures are intended for 3GPP access only.

The Control Plane interface between the 5G-AN and the 5G Core supports:

- The connection of multiple different kinds of 5G-AN (e.g. 3GPP RAN, N3IWF for Un-trusted access to 5GC) to the 5CG via an unique Control Plane protocol: A single NGAP protocol is used for both the 3GPP access and non-3GPP access;
- There is a unique N2 termination point in AMF per access for a given UE regardless of the number (possibly zero) of PDU Sessions of the UE;
- The decoupling between AMF and other functions such as SMF that may need to control the services supported by 5G-AN(s) (e.g. control of the UP resources in the 5G-AN for a PDU Session). For this purpose, NGAP may support information that the AMF is just responsible to relay between the 5G-AN and the SMF. The information can be referred as N2 SM information in TS 23.502 [3] and this specification.

NOTE 2: The N2 SM information is exchanged between the SMF and the 5G-AN transparently to the AMF.

8.2.1.2 AN - AMF

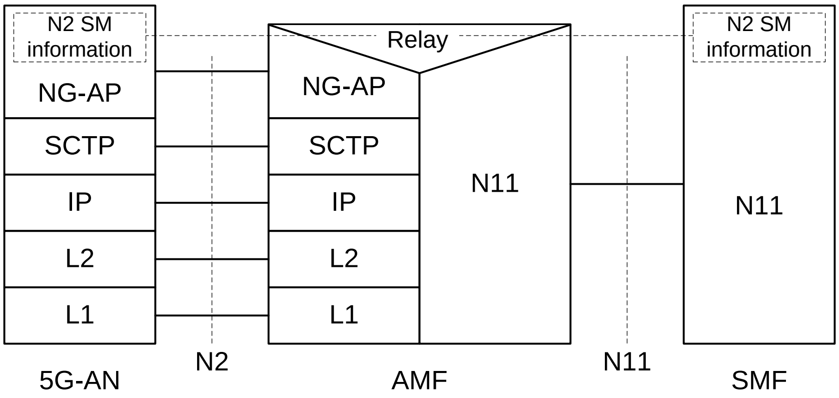


Legend:

- **NG Application Protocol (NG-AP):** Application Layer Protocol between the 5G-AN node and the AMF. NG-AP is defined in TS 38.413 [34].
- **Stream Control Transmission Protocol (SCTP):** This protocol guarantees delivery of signalling messages between AMF and 5G-AN node (N2). SCTP is defined in RFC 4960 [44].

Figure 8.2.1.2-1: Control Plane between the 5G-AN and the AMF

8.2.1.3 AN - SMF



Legend:

- **N2 SM information:** This is the subset of NG-AP information that the AMF transparently relays between the AN and the SMF, and is included in the NG-AP messages and the N11 related messages.

Figure 8.2.1.3-1: Control Plane between the AN and the SMF

NOTE 1: From the AN perspective, there is a single termination of N2 i.e. the AMF.

NOTE 2: For the protocol stack between the AMF and the SMF, see clause 8.2.3.

8.2.2 Control Plane Protocol Stacks between the UE and the 5GC

8.2.2.1 General

A single N1 NAS connection is used for each access to which the UE is connected. The single N1 termination point is located in AMF. The single N1 NAS connection is used for both Registration Management and Connection Management (RM/CM) and for SM-related messages and procedures for a UE.

The NAS protocol on N1 comprises a NAS-MM and a NAS-SM components.

There are multiple cases of protocols between the UE and a core network function (excluding the AMF) that need to be transported over N1 via NAS-MM protocol. Such cases include:

- Session Management Signalling.
- SMS.

Editor's note: It is FFS if other protocols (e.g. LCS) are defined in this Release.

RM/CM NAS messages in NAS-MM and other types of NAS messages (e.g. SM), as well as the corresponding procedures, are decoupled.

The NAS-MM supports generic capabilities:

- NAS procedures that terminate at the AMF. This includes:
    - Handles Registration Management and Connection Management state machines and procedures with the UE, including NAS transport; the AMF supports following capabilities:
        - Decide whether to accept the RM/CM part of N1 signalling during the RM/CM procedures without considering possibly combined other non NAS-MM messages (e.g., SM) in the same NAS signalling contents;
        - Know if one NAS message should be routed to another NF (e.g., SMF), or locally processed with the NAS routing capabilities inside during the RM/CM procedures;
    - Provide a secure NAS connection (integrity protection, ciphering) between the UE and the AMF, including for the transport of payload;
    - Provide access control if it applies;
- It is possible to transmit the other type of NAS message (e.g., NAS SM) together with an RM/CM NAS message by supporting NAS transport of different types of payload or messages that do not terminate at the AMF, e.g. NAS-SM, SMS, between the UE and the AMF. This includes:
    - Information about the Payload type;
    - Additional Information for forwarding purposes
    - The Payload (e.g. the SM message in case of SM signalling);
- There is a Single NAS protocol that applies on both 3GPP and non-3GPP access. When an UE is served by a single AMF while the UE is connected over multiple (3GPP/Non 3GPP) accesses, there is a N1 NAS connection per access.

Security of the NAS messages is provided based on the security context established between the UE and the AMF.

Figure 8.2.2.1-1 depicts NAS transport of SM signalling and SMS.

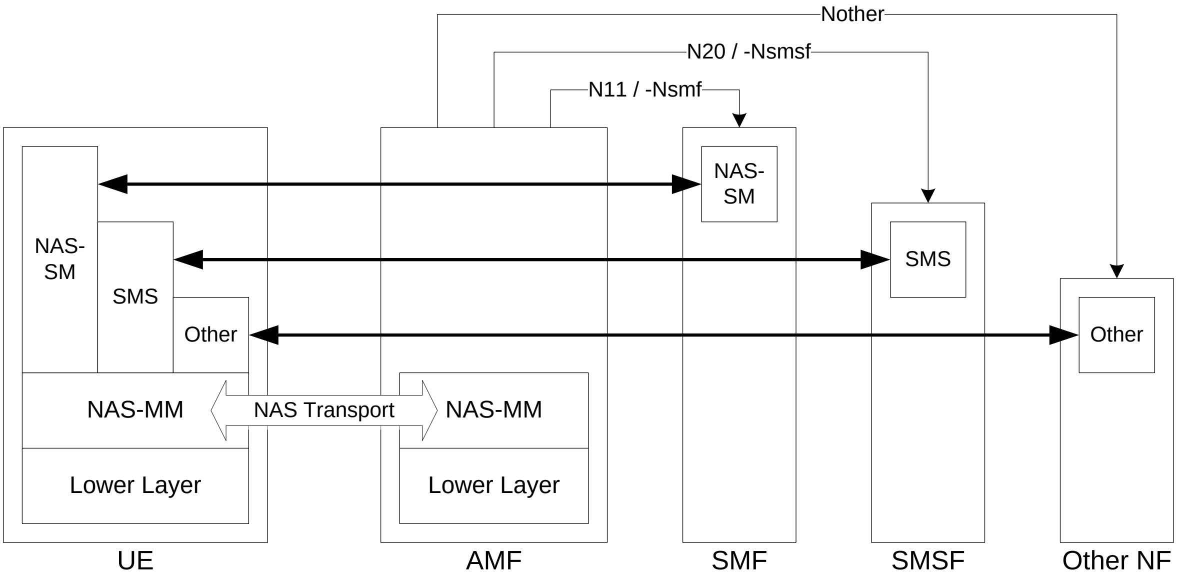
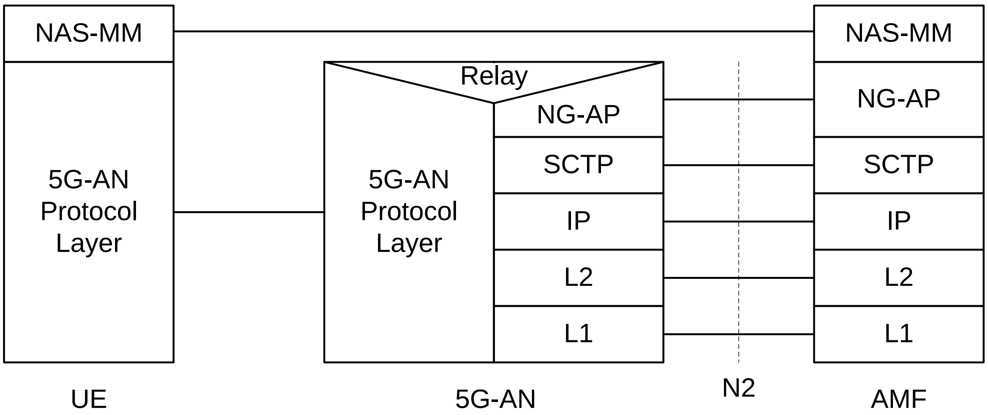


Figure 8.2.2.1-1 NAS transport for SM, SMS and other services

8.2.2.2 UE - AMF



Legend:

- **NAS-MM:** The NAS protocol for MM functionality supports registration management functionality, connection management functionality and user plane connection activation and deactivation. It is also responsible of ciphering and integrity protection of NAS signalling. 5G NAS protocol is defined in TS 24.501 [47]
- 5G-**AN Protocol layer:** This set of protocols/layers depends on the 5G-AN. In case of NG-RAN, the radio protocol between the UE and the NG-RAN node (eNodeB or gNodeB) is specified in TS 36.300 [30] and TS 38.300 [27]. In case of non-3GPP access, see clause 8.2.4.

Figure 8.2.2.2-1: Control Plane between the UE and the AMF

8.2.2.3 UE – SMF

The NAS-SM supports the handling of Session Management between the UE and the SMF.

The SM signalling message is handled, i.e. created and processed, in the NAS-SM layer of UE and the SMF. The content of the SM signalling message is not interpreted by the AMF.

The NAS-MM layer handles the SM signalling is as follows:

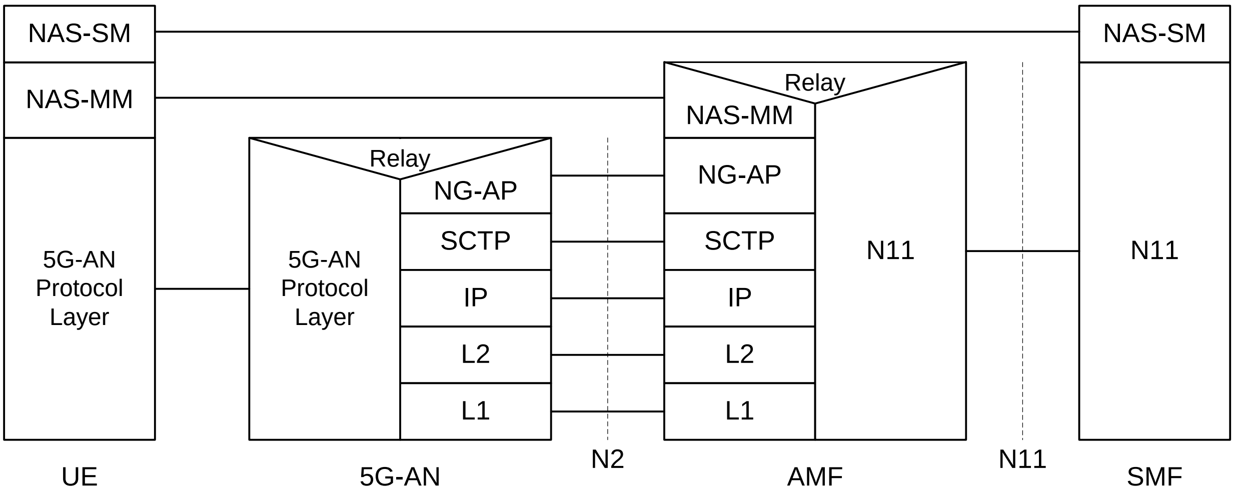
- For transmission of SM signalling:

  - The NAS-MM layer creates a NAS-MM message, including security header, indicating NAS transport of SM signalling, additional information for the receiving NAS-MM to derive how and where to forward the SM signalling message.

- For reception of SM signalling:

  - The receiving NAS-MM processes the NAS-MM part of the message, i.e. performs integrity check, and interprets the additional information to derive how and where to derive the SM signalling message.

The SM message part shall include the PDU Session ID.



Legend:

- **NAS-SM:** The NAS protocol for SM functionality supports user plane PDU Session establishment, modification and release. It is transferred via the AMF, and transparent to the AMF. 5G NAS protocol is defined in TS 24.501 [47]

Figure 8.2.2.3-1: Control Plane protocol stack between the UE and the SMF

8.2.3 Control Plane Protocol Stacks between the network functions in 5GC

8.2.3.1 The Control Plane Protocol Stack for the service based interface

The control plane protocol(s) for the service-based interfaces listed in clause 4.2.6 is defined in the TS 29.500 [49]

8.2.3.2 The Control Plane protocol stack for the N4 interface between SMF and UPF

The control plane protocol for SMF-UPF (i.e. N4 reference point) is defined in TS 29.502 [59].

8.2.4 Control Plane for untrusted non 3GPP Access

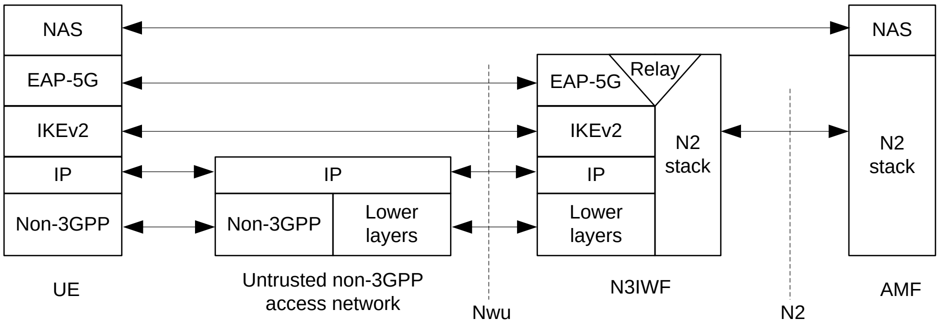


Figure 8.2.4-1: Control Plane before the signalling IPsec SA is established between UE and N3IWF

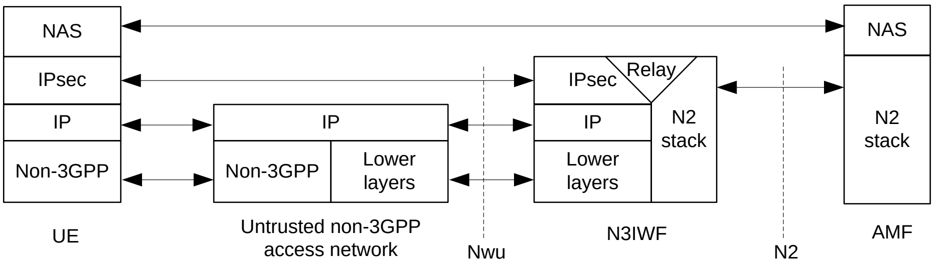


Figure 8.2.4-2: Control Plane after the signalling IPsec SA is established between UE and N3IWF

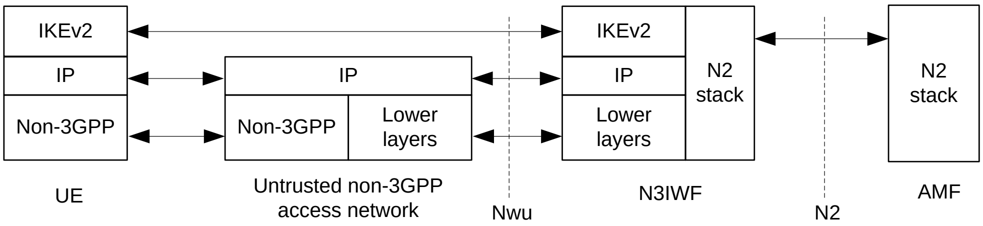


Figure 8.2.4-3: Control Plane for establishment of user-plane via N3IWF

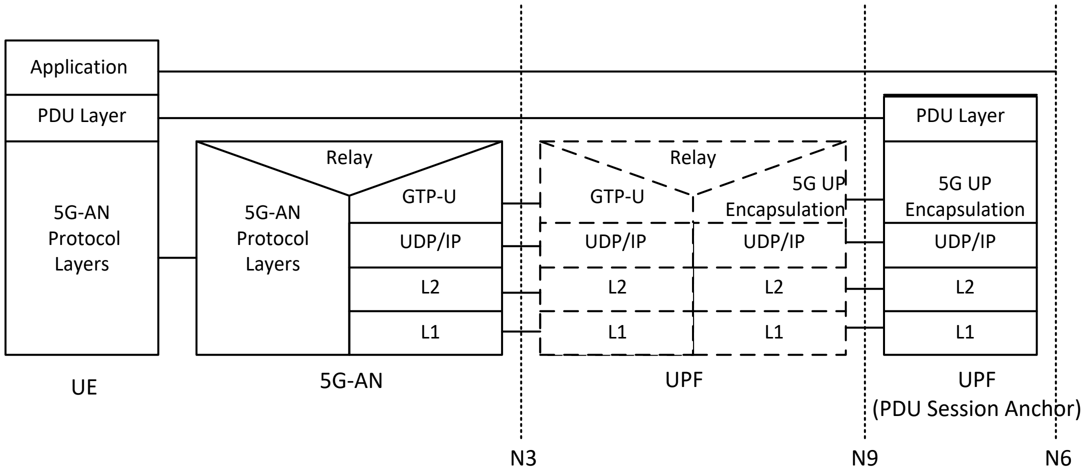
In the above figures 8.2.4-1, 8.2.4-2 and 8.2.4-3, the UDP protocol may be used between the UE and N3IWF to enable NAT traversal for IKEv2 and IPsec traffic.

The "signalling IPsec SA" is defined in TS 23.502 [3], clause 4.12.2.

8.3 User Plane Protocol Stacks

8.3.1 User Plane Protocol Stack for a PDU Session

This clause illustrates the protocol stack for the User plane transport related with a PDU Session.



Legend:

- **PDU layer:** This layer corresponds to the PDU carried between the UE and the DN over the PDU Session. When the PDU Session Type is IPV6, it corresponds to IPv6 packets; When the PDU Session Type is Ethernet, it corresponds to Ethernet frames; etc.
- **GPRS Tunnelling Protocol for the user plane (GTP-U):** This protocol supports multiplexing traffic of different PDU Sessions (possibly corresponding to different PDU Session Types) by tunnelling user data over N3 (i.e. between the 5G-AN node and the UPF) in the backbone network. GTP shall encapsulate all end user PDUs. It provides encapsulation on a per PDU Session level. This layer carries also the marking associated with a QoS Flow defined in clause 5.7.
- **5G Encapsulation:** This layer supports multiplexing traffic of different PDU Sessions (possibly corresponding to different PDU Session Types) over N9 (i.e. between different UPF of the 5GC). It provides encapsulation on a per PDU Session level. This layer carries also the marking associated with a QoS Flow defined in clause 5.7.

Figure 8.3.1-1: User Plane Protocol Stack

- **5G-AN protocol stack**: This set of protocols/layers depends on the AN:
  - When the 5G-AN is a 3GPP NG-RAN, these protocols/layers are defined in TS 38.401 [42]. The radio protocol between the UE and the 5G-AN node (eNodeB or gNodeB) is specified in TS 36.300 [30] and TS 38.300 [27].
  - When the AN is an Untrusted non 3GPP access to 5GC the 5G-AN interfaces with the 5GC at a N3IWF defined in clause 4.3.2 and the 5G-AN protocol stack is defined in clause 8.3.2.
- **UDP/IP:** These are the backbone network protocols.

NOTE 1: The number of UPF in the data path is not constrained by 3GPP specifications: there may be in the data path of a PDU Session 0, 1 or multiple UPF that do not support a PDU Session Anchor functionality for this PDU Session.

NOTE 2: The "non PDU Session Anchor" UPF depicted in the Figure 8.3.1-1 is optional.

NOTE 3: The N9 interface may be intra-PLMN or inter PLMN (in case of Home Routed deployment).

In case there is an UL CL (Uplink Classifier) or a Branching Point (both defined in clause 5.6.4) in the data path of a PDU Session, the UL CL or Branching Point acts as the non PDU Session Anchor UPF of Figure 8.3.1-1. In that case there are multiple N9 interfaces branching out of the UL CL / Branching Point each leading to different PDU Session anchors.

NOTE 4: Co-location of the UL CL or Branching Point with a PDU Session Anchor is a deployment option.

8.3.2 User Plane for untrusted non 3GPP Access

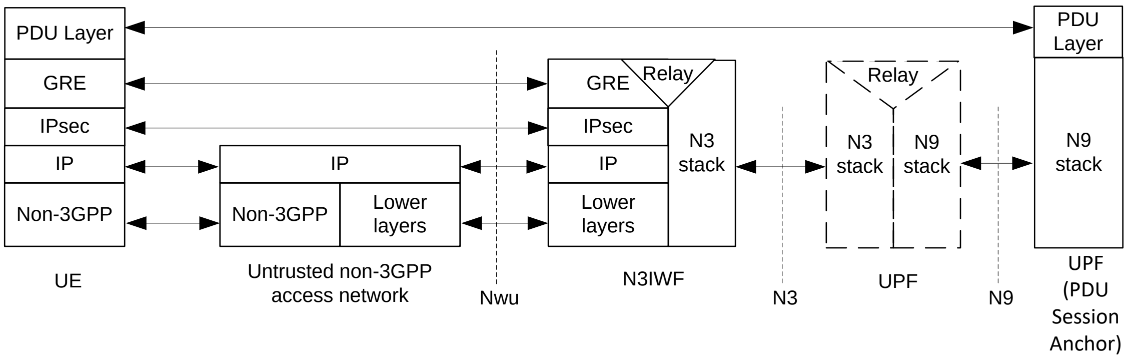


Figure 8.3.2-1: User Plane via N3IWF

Details about the PDU Layer, the N3 stack and the N9 stack are included in clause 8.3.1. The UDP protocol may be used below the IPsec layer to enable NAT traversal.

Annex A (informative): Relationship between Service-Based Interfaces and Reference Points

Service-Based Interfaces and Reference Points are two different ways to model interactions between architectural entities. A Reference Point is a conceptual point at the conjunction of two non-overlapping functional groups (see TR 21.905 [1]). In figure A-1 the functional groups are equivalent to Network Functions.

A reference point can be replaced by one or more service-based interfaces which provide equivalent functionality.

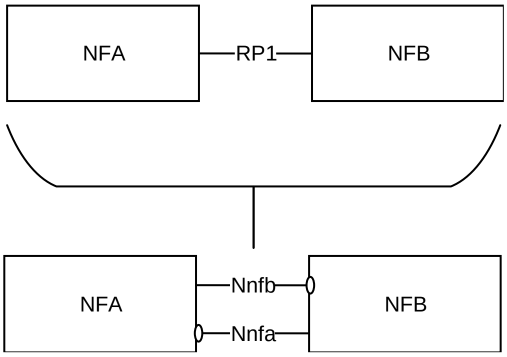


Figure A-1: Example show a Reference Point replaced by two Service based Interfaces

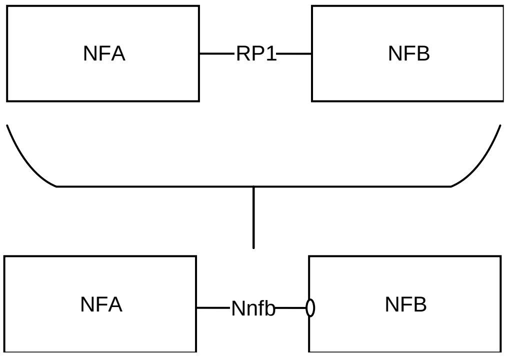


Figure A-2: Example showing a Reference Point replaced by a single Service based Interface

Reference points exist between two specific Network Functions. Even if the functionality is equal on two reference points between different Network Functions there has to be a different reference point name. Using the service-based interface representation it is immediately visible that it is the same service-based interface and that the functionality is equal on each interface.

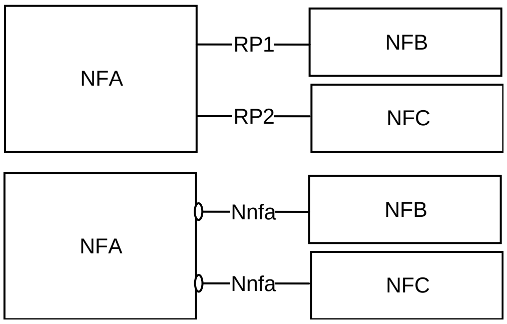


Figure A-3: Reference Points vs. Service-based Interfaces representation of equal functionality on the interfaces

A NF may expose one or more services through Service based interfaces.

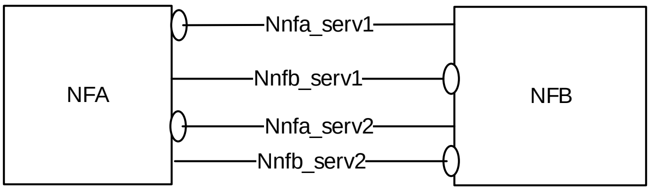


Figure A-4: One or more Services exposed by one Network Function

Annex B (normative): Mapping between temporary identities

When interworking procedures with N26 are used and the UE performs idle-mode mobility from 5GC to EPC the following mapping from 5G GUTI to EPS GUTI applies:

- 5G <MCC> maps to EPS <MCC>
- 5G <MNC> maps to EPS <MNC>
- 5G <AMF Region ID> maps to EPS <MMEGI>
- 5G <AMF Set ID> and 5G <AMF Pointer> map to EPS <MMEC>
- 5G <5G-TMSI> maps to EPS <TMSI>

NOTE: The mapping described above does not necessarily imply the same size for the 5G GUTI and EPS GUTI fields that are mapped. The size of 5G GUTI fields and other mapping details will be defined in TS 23.003 [19].

Annex C (informative): Change history

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
01-2017	S2#118BIS	S2-170625	-	-	-	TS Skeleton for 5G System Architecture	0.0.0
01-2017	SA2#118 BIS	-	-	-	-	Incorporated agreed P-CRs for TS 23.501 from SA2#118bis - S2-170625, S2-170626, S2-170629, S2-170663, S2-170686, S2-170668, S2-170633, S2-170651, S2-170607, S2-170652, S2-170667, S2-170613, S2-170611, S2-170656, S2-170675, S2-170616, S2-170676, S2-170659, S2-170623, S2-170679, S2-170680, S2-170622, S2-170671, S2-170586, S2-170672, S2-170650, S2-170673, S2-170588, S2-170529, S2-170681, S2-170505, S2-170696, S2-170531, S2-170684, S2-170685, S2-170448, S2-170449, S2-170439, S2-170444, S2-170441, S2-170425 plus editorial clean-up by Rapporteur	0.1.0
01-2017						Fixing Editorial errors from v0.1.0	0.1.1
01-2017						Incorporated agreed P-CR - S2-170431	0.2.0
02-2017	SA2#119					Incorporated agreed P-CRs for TS 23.501 from SA2#119 - S2-171314, S2-171255, S2-171290, S2-171316, S2-171620, S2-171319, S2-171604, S2-171295, S2-171307, S2-171607, S2-171270, S2-171311, S2-171262, S2-171312, S2-171313, S2-171275, S2-171276, S2-171277, S2-171278, S2-171279, S2-171303, S2-171304, S2-171562, S2-171568, S2-171585, S2-171616, S2-171623, S2-171536, S2-171612, S2-171602, S2-171603, S2-171532, S2-171344, S2-171345, S2-171346, S2-171548, S2-171346, S2-171548, S2-171549, S2-171543, S2-171622, S2-171451, S2-171514, S2-171515, S2-171552, S2-171513, S2-170895, S2-171475, S2-171476, S2-171478, S2-171553, S2-171554, S2-171555, S2-170717, S2-171461, S2-171557, S2-171465, S2-170887, S2-171521, S2-171468, S2-171469, S2-171558, S2-171124, S2-171525, S2-171528, S2-171490, S2-171529, S2-171614. Plus editorial clean up by Rapporteur	0.3.0
03-2017						Fixing Editorial errors from v0.3.0	0.3.1
04-2017	SA2#120					Incorporated agreed P-CRs for TS 23.501 from SA#120 - S2-172166 S2-172726, S2-172725, S2-172717, S2-172728, S2-172718, S2-172723, S2-172731, S2-172732, S2-172783, S2-172020, S2-172633, S2-172781, S2-172641, S2-172455, S2-172496, S2-172512, S2-172494, S2-172495, S2-172034, S2-172510, S2-171726, S2-172473, S2-172476, S2-172519, S2-172748, S2-172320, S2-172392, S2-172394, S2-172376, S2-172378, S2-172379, S2-172341, S2-172342, S2-172356, S2-172852, S2-172857, S2-172863, S2-172867, S2-172869, S2-172870, S2-172872, S2-172876, S2-172877, S2-172846, S2-172831, S2-172656, S2-172784, S2-172787, S2-172660, S2-172663, S2-172821, S2-172824, S2-172825, S2-172863 plus implementation of "Update "5G Core" to 5GC and use "Control Plane" throughout 501" as indicated in Chairman's notes and some editorial cleanup by Rapporteur	0.4.0
05-2017	SA2#121					Incorporated agreed P-CRs for TS 23.501 from SA2#121 - S2-173792, S2-173689, S2-173846, S2-173990, S2-173986, S2-174035, S2-173989, S2-173276, S2-173841, S2-173278, S2-173279, S2-173280, S2-174054, S2-173602, S2-173624, S2-173810, S2-173950, S2-174028, S2-173437, S2-173993, S2-173987, S2-174076, S2-174058, S2-173881, S2-173677, S2-173705, S2-173626, S2-173683, S2-174024, S2-173836, S2-174044, S2-173706, S2-173708, S2-173812, S2-174047, S2-174043, S2-174042, S2-174038, S2-174040, S2-174039, S2-174037, S2-173918, S2-174048, S2-173971, S2-173968, S2-174034, S2-174033, S2-174050, S2-174055, S2-173620, S2-174036, S2-173972, S2-173777, S2-174008, S2-173805, S2-174026, S2-173803, S2-173804, S2-173806, S2-173629, S2-173774, S2-173636, S2-173951, S2-173796, S2-173763, S2-173772, S2-173798, S2-173799, S2-173759, S2-173926, S2-173956, S2-173616, S2-173658, S2-173659, S2-173727, S2-173994, S2-173944 plus editorial cleanup by Rapporteur. Fixing one occurrence of NGC->5GC (reminiscence from SA2#120 rapporteur action).	0.5.0
06-2017	SP#76	SP-170384	-	-	-	MCC Editorial Update for presentation to TSG SA#76 for Information	1.0.0

07-2017	SA2#122					Incorporated agreed P-CRs for TS 23.501 from SA2#122- S2-175296, S2-175222, S2-175217, S2-175218, S2-175219, S2-175025, S2-174547, S2-175027, S2-175193, S2-175029, S2-175020, S2-175195, S2-175023, S2-175252, S2-175246, S2-175249, S2-175262, S2-175254, S2-175170, S2-175171, S2-175255, S2-175260, S2-174984, S2-175198, S2-175208, S2-175206, S2-175044, S2-175200, S2-175282, S2-175207, S2-175038, S2-175041, S2-175283, S2-175000, S2-174998, S2-175242, S2-175238, S2-175243, S2-175016, S2-175292, S2-175211, S2-175161, S2-174786, S2-175096, S2-175098, S2-174829, S2-174822, S2-175085, S2-175086, S2-174805, S2-175087, S2-175121, S2-174754, S2-174753, S2-175130, S2-174355, S2-175070, S2-175101, S2-175102, S2-175298, S2-175112, S2-175104, S2-175061, S2-174833, S2-174899, S2-174835, S2-174900, S2-174839, S2-174840, S2-174894, S2-174902, S2-174888, S2-174889, S2-174904, S2-174895, S2-174892, S2-175302, S2-175304, S2-175305, S2-175306, S2-175307, S2-175308, S2-175312, S2-175313 plus editorial clean up by Rapporteur.	1.1.0
07-2017						Incorporated approved P-CRs from SA2#122 - S2-174309, S2-174901. Fixed implementation errors of S2-175222, S2-175296.	1.2.0
09-2017	SA2#122 bis					Incorporated approved P-CRs from SA2#122bis - S2-175388, S2-175438, S2-176350, S2-176524, S2-176352, S2-176353, S2-176399, S2-176532, S2-176400, S2-175934, S2-176525, S2-176526, S2-176528, S2-176529, S2-176401, S2-176389, S2-176530, S2-176531, S2-176397, S2-176398, S2-176534, S2-175912, S2-176386, S2-176539, S2-176568, S2-176582, S2-176406, S2-176537, S2-176360, S2-176361, S2-176648, S2-176573, S2-176572, S2-176517, S2-176575, S2-176368, S2-176579, S2-176580, S2-176510, S2-176414, S2-176418, S2-176419, S2-176420, S2-176417, S2-176569, S2-176412, S2-176570, S2-176558, S2-176481, S2-176485, S2-176488, S2-176559, S2-175977, S2-176653, S2-176459, S2-176635, S2-176456, S2-176458, S2-176464, S2-176461, S2-176644, S2-176422, S2-176424, S2-176425, S2-176540, S2-176431, S2-176500, S2-176551, S2-176545, S2-176479, S2-176546, S2-176547, S2-176567, S2-175990, S2-176079, S2-175954, S2-175708, S2-176080, S2-176150, S2-176154, S2-176156, S2-176056, S2-176097, S2-176160, S2-176167, S2-176133, S2-176136, S2-176135, S2-176141, S2-176137, S2-176140, S2-176142, S2-176139, S2-175809, S2-176062, S2-176651, S2-176696, S2-176697, S2-176698, S2-176699, S2-176700, S2-176702, S2-176703, S2-176704, S2-176706, S2-176707, S2-176708, S2-176709, S2-176710, S2-176711, S2-176717, S2-176718, S2-176719, S2-176721, S2-176722, S2-176577, S2-176656, S2-176200, S2-176188, S2-176266, S2-176252, S2-176260, S2-176263, S2-176218, S2-176270, S2-176220 plus editorial clean up by Rapporteur. Note 1: S2-176704 approved by email based on S2-176633Rev7 had some discrepancy thus S2-176704 was implemented based on S2-176633Rev7 approved version. Note 2: S2-176200 showed 2 duplicate figures for figure 4.2.4-1 (due to issues with word rev. marks) thus Editor deleted one of the figure based on intent for 4.2.4-1 behind 6200 expressed by author.	1.3.0
09-2017	SA2#122 E					Incorporated approved P-CRs from SA2#122E - S2-176728, S2-176731, S2-176743, S2-176746, S2-176751, S2-176752, S2-176754, S2-176757, S2-176758, S2-176760, S2-176762, S2-176764, S2-176765, S2-176769, S2-176771, S2-176774, S2-176779, S2-176781, S2-176795, S2-176804, S2-176805, S2-176806, S2-176807, S2-176808, S2-176809, S2-176810, S2-176811, S2-176812, S2-176813, S2-176817, S2-176829, S2-176819, S2-176820, S2-176824, S2-176825, S2-176826. Parts of S2-176651 (missed in v1.3.0) approved during SA2#122bis incorporated plus editorial clean up by Rapporteur. In addition, Rapporteur has also deleted Annex A (except section A.1, A.2) as per Agenda item SA2#122E AI 34.	1.4.0
11-2017	SA2#123					Incorporated approved P-CRs from SA2#123 - S2-178184, S2-177830, S2-178022, S2-178200, S2-178161, S2-178114, S2-177625, S2-178132, S2-177631, S2-178151, S2-177839, S2-177987, S2-177711, S2-177063, S2-177225, S2-178139, S2-177378, S2-178159, S2-177275, S2-177633, S2-177811, S2-178197, S2-177237, S2-178073, S2-177853, S2-177855, S2-177978, S2-178064, S2-177597, S2-177922, S2-177923, S2-	1.5.0

						177925, S2-177928, S2-178120, S2-177412, S2-177964, S2-178147, S2-177595, S2-178117, S2-177895, S2-178115, S2-178145, S2-178193, S2-177123, S2-178134, S2-178194, S2-177311, S2-177277, S2-177854, S2-177097, S2-177817, S2-177006, S2-178111, S2-178107, S2-178156, S2-178195, S2-178071, S2-178029, S2-178025, S2-178103, S2-178027, S2-178019, S2-177307, S2-177481, S2-177974, S2-178024, S2-177847, S2-178055, S2-178053, S2-178051, S2-178060, S2-178050, S2-178045, S2-178058, S2-177867, S2-178048, S2-178097, S2-177355, S2-178106, S2-178196, S2-177971, S2-178004, S2-177834, S2-178183, S2-178138, S2-178038, S2-178042, S2-178030, S2-178152, S2-178040, S2-177915, S2-178130, S2-177918, S2-178047, S2-177592, S2-177665, S2-177663, S2-177664, S2-177475, S2-178208, S2-177941, S2-177940, S2-177446, S2-177524, S2-178127, S2-178070, S2-177845, S2-178065, S2-177784, S2-178062, S2-178069, S2-178154, S2-177792, S2-177690, S2-177393, S2-178035, S2-178109, S2-177414, S2-178171, S2-177274, S2-178164, S2-177856, S2-177819, S2-177762, S2-178204, S2-178209 plus editorial clean up by Rapporteur. This includes terminology clean up – 5GAN->5G-AN, 5G AN->5G-AN, PDU session anchor -> PDU Session Anchor (as agreed in pCR S2-178184), some reference clean up.	
12-2017	SA2#124					Incorporated approved P-CRs from SA2#124 - S2-179093, S2-179417, S2-178274, S2-178396, S2-179563, S2-179569, S2-179464, S2-179420, S2-179466, S2-178432, S2-179422, S2-179423, S2-179468, S2-179566, S2-179426, S2-178543, S2-179520, S2-179521, S2-179523, S2-179378, S2-179567, S2-178270, S2-179348, S2-179279, S2-179278, S2-179435, S2-179448, S2-179436, S2-179288, S2-179603, S2-179441, S2-179442, S2-178296, S2-179313, S2-178528, S2-179314, S2-179319, S2-179456, S2-179321, S2-179322, S2-179453, S2-179606, S2-179460, S2-179458, S2-179388, S2-178812, S2-178601, S2-178256, S2-179557, S2-179331, S2-179403, S2-179336, S2-179404, S2-178722, S2-179405, S2-179559, S2-179357, S2-179358, S2-179360, S2-179365, S2-178721, S2-179366, S2-179368, S2-179369, S2-178626, S2-179494, S2-179495, S2-179409, S2-179110, S2-179119, S2-179593, S2-178999, S2-179000, S2-179062, S2-179004, S2-179005, S2-178577, S2-179052, S2-179046, S2-178849, S2-178460, S2-179595, S2-179057, S2-179477, S2-178960, S2-179051, S2-179080, S2-179083, S2-179582, S2-179087, S2-179089, S2-179018, S2-178965, S2-179584, S2-179021, S2-179585, S2-178655, S2-178327, S2-179598, S2-179184, S2-179193, S2-179270, S2-179177, S2-179232, S2-179236, S2-179159, S2-179549, S2-179261, S2-179544, S2-179546, S2-178421, S2-179218, S2-178356, S2-179027, S2-179602, S2-178635, S2-178719, S2-179619, S2-179624, S2-179626, S2-179627 plus RFC, 3GPP TS, clause references, editorial clean up by Rapporteur.	1.6.0
12-2017	SP#78	-	-	-	-	MCC Editorial Update	2.0.0
12-2017	SP#78	SP-170931	-	-	-	Correction of Annex A figure numbers for presentation to TSG SA#76 for Approval	2.0.1