3GPP TS 23.501 V0.3.0 (2017-02)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

System Architecture for the 5G System;

Stage 2

(Release 15)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP..  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

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

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2017, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 8

Introduction 8

1 Scope 9

2 References 9

3 Definitions, symbols and abbreviations 10

3.1 Definitions 10

3.2 Abbreviations 11

4 Architecture model and concepts 11

4.1 General concepts 11

4.2 Architecture reference model 12

4.2.1 General 12

4.2.2 Network Functions and entities 12

4.2.3 Non-roaming reference architecture 13

4.2.4 Roaming reference architectures 16

4.2.5 Data Storage architectures 19

4.2.6 Service-based interfaces 20

4.2.7 Reference points 20

4.2.7 Support of non-3GPP access 21

4.2.7.1 General Concepts to Support Non-3GPP Access 21

4.2.7.2 Architecture Reference Model for Non-3GPP Accesses 22

4.2.7.2.1 Non-roaming Architecture for LBO for Non-3GPP Accesses 22

4.2.7.2.2 Roaming Architecture for LBO for Non-3GPP Accesses, N3IWF in same PLMN as 3GPP access 23

4.2.7.2.3 Roaming Architecture for LBO for Non-3GPP Accesses, N3IWF in different PLMN from 3GPP access 24

4.2.7.3 Non-3GPP Access Reference Points 24

4.3 Interworking with E-UTRAN connected to EPC 25

4.3.1 Non-roaming architecture 25

4.3.2 Roaming architecture 25

4.4 Specific services 27

4.4.1 Public Warning System 27

4.4.2 SMS over NAS 27

4.4.2.1 Architecture to support SMS over NAS 27

4.4.2.2 Reference point to support SMS over NAS 28

4.4.2.3 Service based interface to support SMS over NAS 28

4.4.2.3 SMS over NAS transport 29

4.4.3 IMS support 29

4.4.4 Location services 29

5 High level features 29

5.1 General 29

5.2 Network Access Control 29

5.3 Registration and Connection Management 30

5.3.1 General 30

5.3.2 Registration Management 30

5.3.2.1 General 30

5.3.2.2 5GS Registration Management states 30

5.3.2.2.1 General 30

5.3.2.2.2 RM-DEREGISTERED state 30

5.3.2.2.3 RM-REGISTERED state 30

5.3.2.2.4 5GS Registration Management State models 31

5.3.2.3 Registration Area management 32

5.3.2.4 Support of an UE registered over both 3GPP and Non 3GPP access 32

5.3.3 Connection Management 32

5.3.3.1 General 33

5.3.3.2 5GS Connection Management states 33

5.3.3.2.1 General 33

5.3.3.2.2 CM-IDLE state 33

5.3.3.2.3 CM-CONNECTED state 33

5.3.3.2.4 5GS Connection Management State models 34

5.3.3.3 NAS signalling connection management 34

5.3.3.3.1 General 34

5.3.3.3.2 NAS signalling connection establishment 34

5.3.3.3.3 NAS signalling connection Release 34

5.3.3.4 Support of an UE connected over both 3GPP and Non 3GPP access 35

5.3.4 UE Mobility 35

5.3.4.1 Mobility Restrictions 35

5.3.4.1.1 General 35

5.3.4.1.2 Management of service area restrictions 36

5.4 3GPP access specific aspects 37

5.4.1 UE reachability in CM-IDLE 37

5.4.1.1 General 37

5.4.1.2 UE reachability allowing MICO data while the UE is CM-IDLE 37

5.4.1.2.1 General characteristics 37

5.4.1.3 Mobile Initiated Connection only (MICO) mode 37

5.4.1.4 Mobile Deregistration at the End of Communication 38

5.4.2 UE reachability in CM-CONNECTED 38

5.5 Non-3GPP access specific aspects 39

5.5.1 General 39

5.5.2 Registration Management 39

5.5.3 Connection Management 39

5.6 Session Management 39

5.6.1 Overview 39

5.6.2 Interaction between AMF and SMF 41

5.6.3 Roaming 42

5.6.4 Single PDU session with multiple PDU session anchors 43

5.6.4.1 General 43

5.6.4.2 Usage of an UL Classifier for a PDU session 43

5.6.4.3 Usage of IPv6 multi-homing for a PDU session 44

5.6.5 Support for connecting to a local area data network 45

5.6.6 DN authorization of the establishment of a PDU session 46

5.6.7 Application Function influence on traffic routing 46

5.6.8 Selective activation of UP connection of existing PDU session 47

5.6.9 Session and Service Continuity 47

5.6.9.1 General 47

5.6.9.2 SSC mode 47

5.6.9.2.1 SSC Mode 1 47

5.6.9.2.2 SSC Mode 2 48

5.6.9.2.3 SSC Mode 3 48

5.6.9.3 SSC mode selection 48

5.7 QoS model 49

5.7.1 General Overview 49

5.7.2 5G QoS Parameters 51

5.7.3 5G QoS characteristics 53

5.7.4 Standardized 5QI to QoS characteristics mapping 53

5.7.5 Reflective QoS 54

5.7.5.1 General 54

5.7.5.2 UE Reflective QoS Procedures 54

5.7.5.2.1 General 54

5.7.5.2.2 UE Derived QoS Rule 54

5.7.5.3 UPF Procedures for Supporting Reflective QoS 55

5.7.5.4 Enabling Reflective QoS 55

5.7.5.4.1 General 55

5.7.5.4.2 Reflective QoS Activation via User Plane 55

5.7.5.4.3 Reflective QoS Activation via Control Plane 55

5.7.5.5 Disabling Reflective QoS 55

5.7.5.5.1 General 55

5.8 User plane Management 55

5.8.1 IP address management 55

5.8.1.1 General 55

5.8.1.2 Routing rules configuration 56

5.8.2 User Plane Function(s) 56

5.9 Identities 57

5.9.1 Subscriber Permanent Identity 57

5.9.2 Permanent Equipment Identifier 57

5.10 Security aspects 57

5.10.1 General 57

5.11 Support for Dual connectivity, Multi-connectivity 58

5.12 Charging 58

5.13 Support for Edge Computing 58

5.14 Policy Control 58

5.15 Network slicing 59

5.15.1 General 59

5.15.2 Identification and selection of a Network Slice: The S-NSSAI and the NSSAI 59

5.15.3 Subscription aspects 60

5.15.4 UE NSSAI configuration and NSSAI storage aspects 60

5.15.5 Detailed Operation Overview 60

5.15.6 Network Slicing Support for Roaming 61

5.16 Support for specific services 62

5.16.1 Public Warning System 62

5.16.2 SMS over NAS 62

5.16.2.1 General 62

5.16.2.2 SMS over NAS transport 62

5.16.3 IMS support 62

5.16.3.1 General 62

5.16.3.2 IMS voice over PS Session Supported Indication 63

5.16.3.3 P-CSCF address delivery 63

5.16.4 Emergency services 63

5.16.5 Multimedia Priority Services 63

5.17 Interworking and Migration 63

5.17.1 Support for Migration from EPC to 5GC 63

5.17.1.1 General 63

5.17.2 Interworking with EPC 65

5.17.2.1 General 65

5.17.2.2 Mobility in single-registration mode 65

5.17.2.3 Mobility in dual-registration mode 65

5.18 Network Sharing 66

5.19 Control Plane Congestion and Overload Control 66

5.20 External Exposure of Network Capability 66

5.21 xxxx 66

6 Network Functions 67

6.1 General 67

6.2 Network Function Functional description 67

6.2.1 AMF 67

6.2.2 SMF 68

6.2.3 UPF 69

6.2.4 PCF 69

6.2.5 NEF 69

6.2.6 NRF 69

6.2.7 UDM 70

6.2.8 AUSF 70

6.2.9 N3IWF 70

6.2.10 AF 71

6.2.11 SDSF 71

6.2.12 UDSF 71

6.3 Network function discovery and selection 71

6.3.1 General 71

6.3.2 SMF selection function 72

6.3.3 User Plane Function Selection 72

6.3.4 AUSF selection function 73

6.3.x <NF name> selection 73

7 Network Function Services and descriptions 74

7.1 Network Function Service Framework 74

7.1.1 General 74

7.1.2 Network Function Service discovery 74

7.1.3 Network Function Service authorization 75

7.1.4 Network Function Service registration and de-registration 75

7.2 Network Function Services 75

7.2.1 General 75

7.2.2 AMF Services 75

7.2.3 SMF Services 75

7.2.4 PCF Services 76

7.2.5 UDM Services 76

7.2.6 NRF Services 76

7.2.7 AUSF Services 76

7.2.8 NEF Services 76

7.3 Network Internal Exposure 77

7.4 External Exposure 77

8 Control and User plane Protocol Stacks 77

8.1 General 77

8.2 Control plane Protocol stacks 78

8.2.x Control Plane for untrusted non 3GPP Access 78

8.3 User Plane Protocol stacks 79

8.3.1 User Plane Protocol stack for a PDU session 79

8.3.2 User Plane for untrusted non 3GPP Access 80

Annex A (informative): Policy framework 81

A.1 High level architectural requirements 81

A.2 Architecture model and reference points 82

A.2.1 Reference architecture 82

A.2.2 Reference points 85

A.2.2.1 N5 reference point 85

A.2.2.2 N7 reference point 85

A.2.2.3 N15 reference point 86

A.2.2.4 N7r reference point 86

A.2.2.5 PUd reference point 86

A.2.2.6 N23 reference point 86

A.3 Functional description 87

A.3.1 Overall description 87

A.3.1.1 UE Access and Mobility Management Control 87

A.3.1.2 Roaming impacts to Policy 87

A.3.1.3 UE Policy 88

A.3.1.3.1 General 88

A.3.1.3.2 Access network discovery & selection policy 88

A.3.1.3.3 Grouping the Route Selection Policies 88

A.3.1.4 Policy Control Subscription information management 90

Annex B (informative): Location Services temporary placeholder 92

B.1 Abbreviations 92

B.2 Non-Roaming Reference Architecture 92

B.3 Roaming Reference Architecture 93

B.4 Reference Points 93

B.5 LMF Functions 93

Annex C (informative): Multimedia Priority Services temporary placeholder 94

C.1 References 94

C.2 General MPS Functionality 94

Annex D (informative): IMS specific placeholder for TS 23.228 [15] 96

D. IP-Connectivity Access Network specific concepts when using 5GS to access IMS 96

D.0 General 96

D.1 Mobility related concepts 96

D.2 QoS related concepts 96

Annex <Z> (informative): Change history 97

# 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.

# Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

# 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".

# 3 Definitions, symbols 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 5G-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 Indicator (5QI):** 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-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.

Editor's note: The definition will be revisited after RAN decision on 5G-RAN.

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

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

**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.

**Mobility pattern:** Network concept of determining within an NF 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.

**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.

**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.

**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. The type of association can be IP, Ethernet or unstructured.

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

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

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

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

## 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

5QI 5G QoS Indicator

5G-RAN 5G Radio Access Network

AF Application Function

AMF Access and Mobility Management Function

AS Access Stratum

CP Control Plane

DL Downlink

DN Data Network

FQDN Fully Qualified Domain Name

GFBR Guaranteed Flow Bit Rate

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

NEF Network Exposure Function

NF Network Function

NR New Radio

NRF Network Repository Function

PCF Policy Control Function

QFI QoS Flow Identity

PFDF Packet Flow Description Function

QoE Quality of Experience

SA NR Standalone New Radio

SDSF Structured Data Storage Function

SMF Session Management Function

UDSF Unstructured Data Storage Function

UL Uplink

UPF User Plane Function

# 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 access-agnostic core network with a common AN - CN interface which integrates different 3GPP and non-3GPP access types.

- 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 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, focusing on the interactions between pairs of network functions described by point-to-point reference point (e.g. N11) between any two network functions (e.g. AMF and SMF) is depicted when some interaction exists between these two network functions.

Service-based interfaces are listed in clause 4.2.4. Reference points are listed in clause 4.2.6.

Network functions within the 5G Core Control shall exhibit service-based interfaces for services that can be used by other authorized network functions, unless explicitly stated otherwise.

Editor's note 1: This will be evaluated on a case by case basis when specifying the procedure.

Editor's note 2: The above two statements will be revisited when the work on system procedure is stable.

### 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)

- Core Access and Mobility Management Function (AMF)

- Data network (DN), e.g. operator services, Internet access or 3rd party services

- Structured Data Storage network function (SDSF)

- Unstructured Data Storage network function (UDSF)

- Network Exposure Function (NEF)

- NF Repository Function (NRF)

- Policy Control function (PCF)

- Session Management Function (SMF)

- Unified Data Management (UDM)

- User plane Function (UPF)

- Application Function (AF)

- User Equipment (UE)

- (Radio) Access Network ((R)AN)

### 4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture with service-based interfaces within the Control Plane.



Figure 4.2.3-1: 5G System Service-based architecture

NOTE: The AF can use the services exposed by the PCF or the NEF based on the operator deployment as described in clause 6.2.X.

Editor's note: It is FFS whether there is a scenario in Rel-15 where the AF exposes services to the other CN CP Network Functions.

Editor's note: It is FFS whether there is a scenario in Rel-15 where the AF may use services exposed by the SMF

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

NOTE 3: For the sake of clarity of the point-to-point diagrams, the UDSF, SDSF, NEF and NRF have not been depicted. However, all depicted Network Functions can interact with the UDSF, NEF and NRF as necessary.

NOTE 4: The UDM contains UDR. 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.

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 with AF in VPLMN in service-based interface representation

Figure 4.2.4-2 depicts the 5G System roaming architecture with local breakout with AF in HPLMN in service-based interfaces within the Control Plane.



Figure 4.2.4-2 Roaming 5G System architecture - local breakout scenario with AF in HPLMN in service-based interface representation

Figure 4.2.4-2 depicts the 5G System roaming architecture in case of home routed scenario when 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 with AF in VPLMN using the reference point representation.



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

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



Figure 4.2.4-5: Roaming 5G System architecture -local breakout scenario with AF in the HPLMN in reference point representation

Following figure 4.2.4-4 depicts the 5G System roaming architecture in case of home routed scenario using the reference point representation.



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

### 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. 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 interface.

As depicted in Figure 4.2.5-2, the 5G system architecture allows the NEF to store structured data in the SDSF intended for network external and network internal exposure by the NEF. SDSF belongs to the same PLMN where the NEF is located.



Figure 4.2.5-2: Data storage architecture for structured data from the NEF

NOTE 2: Deployments can choose to collocate SDSF with other NFs (e.g. UDR, UDSF).

### 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.

**Nausf:** Service-based interface exhibited by AUSF.

### 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.

**N5:** Reference point between the PCF and an AF.

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

NOTE: 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.

**N7:** Reference point between the SMF and the PCF.

**N7r:** 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.

**N9:** Reference point between two Core UPFs.

**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 EIR.

**N18:** Reference point between any NF and UDSF.

**N19:** Reference point between NEF and SDSF.

Editor's note: The nature of N18 is FFS and it will be determined in coordination with Stage 3 groups. Depending on the conclusion, the N18 reference point may need to be renamed.

Editor's note: Whether the N19 reference point between the NEF and the SDSF is a service-based interface or not is FFS. Depending on the conclusion the N19 reference point may also be renamed.

### 4.2.7 Support of non-3GPP access

Editor's note: This should include non-roaming and roaming reference architecture for support of non-3GPP access. To start with, Rel-15 will include support for untrusted access.

#### 4.2.7.1 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 5G-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.

The N2 and N3 reference points are used to connect standalone non-3GPP accesses to 5G core network control-plane functions 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 5G-RAN and via standalone non-3GPP accesses, multiple N1 instances shall exist for the UE i.e. there shall be one N1 instance over 5G-RAN and one N1 instance over non-3GPP access.

A UE simultaneously connected to the same 5G core network of a PLMN over 3GPP access and 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. a different VPLMN or 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 is independent of the N3IWF selection.

Editor's note: It is FFS whether there exists a case that a UE is served by different PLMNs simultaneously due to roaming condition, e.g., a UE is roaming and connected over 3GPP access and non-3GPP access through N3IWF located in HPLMN, and it is also FFS how the system and the UE behave in such a case.

Non-3GPP access networks shall be connected to the 5G core network via a Non-3GPP InterWorking Function (N3IWF). The N3IWF interfaces to 5G core network control-plane functions and user-plane functions via N2 interface and N3 interface, respectively.

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 4.12.2 in TS 23.502 [3].

Editor's note: it is FFS whether the UE attaches to non-3GPP access without establishing any PDU sessions, or if the UE always performs an attach with a PDU session establishment.

It shall be possible to maintain the UE signalling connection with the AMF after all the PDU sessions for the UE over the non-3GPP 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.

Editor's note: Name of N3IWF may need to be changed.

Editor's note: How QoS is supported via the N3IWF and untrusted non-3GPP accesses is FFS.

#### 4.2.7.2 Architecture Reference Model for Non-3GPP Accesses

#### 4.2.7.2.1 Non-roaming Architecture for LBO for Non-3GPP Accesses



Figure 4.2.7.2.1-1: Non-roaming architecture for 5G core network with non-3GPP access

NOTE 1: The reference architecture in figure 4.2.7.2.1-1 only shows the architecture and the network functions directed connected to non-3GPP access, and other parts of the architecture are the same as defined in section 4.2.

NOTE 2: The reference architecture in figure 4.2.7.2.1-1 supports both the point-to-point and service based model reference point between AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.7.2.1-1 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 4.2.7.2.1-1 may apply to different UPFs when different PDU sessions are activated over 3GPP access and non-3GPP access.

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



Figure 4.2.7.2.2-1: Roaming architecture for 5G core network with non-3GPP access - N3IWF in the VPLMN

NOTE 1: The reference architecture in figure 4.2.7.2.2-1 only shows the architecture and the network functions directed connected to support non-3GPP access, and other parts of the architecture are the same as defined in section 4.2 with involvement of an SMF and of UPF(s) in HPLMN in case of Home Routed.

NOTE 2: The reference architecture in figure 4.2.7.2.2-1 supports both the point-to-point and service based model reference point between AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.7.2.2-1 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 4.2.7.2.2-1 may apply to different UPFs when different PDU sessions are activated over 3GPP access and non-3GPP access.

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



Figure 4.2.7.2.3-1: 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 4.2.7.2.3-1 only shows the architecture and the network functions directed connected to support non-3GPP access, and other parts of the architecture are the same as defined in section 4.2 with involvement of an SMF and of UPF(s) in HPLMN in case of Home Routed.

NOTE 2: The reference architecture in figure 4.2.7.2.2-1 supports both the point-to-point and service based model reference point between AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.7.2.2-1 apply to two different AMFs for a UE which is connected to the 5G core network over 3GPP access and non-3GPP access simultaneously.

#### 4.2.7.3 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 E-UTRAN connected to 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: Nx 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 Nx interface in the network is optional for interworking.

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 NG9 towards an additional UPF, if needed.

Editor's note: The final name for Nx and whether Nx is a new NG Core interface or S10/N14 is FFS.

### 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 NG9 towards the additional UPF, if needed.



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

## 4.4 Specific services

### 4.4.1 Public Warning System

Editor's note: This should include potential reference model for PWS (e.g. to show connectivity to CBC).

Editor's note: Public Warning System architecture in TS 23.041 will be enhanced under the responsibility of CT WG1.

Editor's note: Whether NR in Rel-15 supports PWS or not depends on the decision of TSG RAN.

### 4.4.2 SMS over NAS

Editor's note: This should include potential reference model for SMS over NAS.

#### 4.4.2.1 Architecture to support SMS over NAS

Figure 4.4.2.1-1 shows the architecture to support SMS over NAS.



Figure 4.4.2.1-1: System Architecture for SMS over NAS

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/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: When serving AMF is relocated for a given UE, SMS function for a given UE does not need to change. Thus the source AMF includes SMSF identifier as part of UE context transfer during AMF relocation to target AMF.

Figure 4.4.2.1-2 shows the roaming architecture to support SMS over NAS.



Figure 4.4.2.2-2: Roaming architecture for SMS over NAS

#### 4.4.2.2 Reference point to support SMS over NAS

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

**N8:** Reference point for SMS function address retrieval between AMF and UDM.

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

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

#### 4.4.2.3 Service based interface to support SMS over NAS

**Nsmsf:** Service-based interface exhibited by SMSF.

#### 4.4.2.3 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. If the core network supports SMS, and the AMF decides to provide SMS available to the UE, the AMF provides an "SMS supported" indication to the UE.

SMS is transported over NAS without the need to establish data radio bearers, via MM transport message, which can carry SMS messages as payload. The MM transport message can be transmitted as initial NAS message both in downlink and uplink direction. The MM transport message should be at least integrity protected and the SMS payload shall be ciphered. The MM transport header shall inform that the MM transport payload is an SMS message. MM security keys are used for the ciphering/de-ciphering of the SMS payload.

The UE and AMF only send SMS payload over MM transport after successful negotiation of SMS during the last registration/registration update.

NOTE: The MM transport message used for SMS payload is the same as the MM transport message that transport SM signalling.

The MM layer in the AMF integrity checks the MM transport message containing SMS payload received from a UE. If integrity check is successful, and the MM transport message header indicates SMS, the AMF deciphers and forwards the SMS payload to the SMS Function via Nsms.

The MM layer in the UE integrity checks the MM transport message containing SMS payload received from the AMF. If integrity check is successful, and the MM transport message header indicates SMS, the UE deciphers and forwards to SMS stack in the UE.

Editor's note: Security aspects will depend on SA WG3.

### 4.4.3 IMS support

Editor's note: This should include potential architecture level interactions for IMS support.

### 4.4.4 Location services

Editor's note: This should include potential reference model for location services. A temporary placeholder defined in Annex B.

# 5 High level features

Editor's note: This should include high level functionality for features and functionalities supported by the architecture e.g. Network access control, Network slicing, dual/multi-connectivity, MM, SM, Overall QoS Concept, Identities, Authentication, security aspects, interworking, migration, PDU session, architecture impact due to virtualization etc. Individual section such as connection management, registration management, identities should include enablers for stateless NFs, virtualized NF etc. If needed, separate section could be considered to provide an overview.

## 5.1 General

## 5.2 Network Access Control

Editor's note: this should include network selection aspects, description of access control, LI, authentication/authorization, policy control etc. Level of detail expected for this section is similar to Network access control clause in TS 23.401 clause 4.3.2.

## 5.3 Registration and Connection Management

### 5.3.1 General

The Registration Management is used to register or de-register 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 registration management procedures are applicable over both 3GPP access and non 3GPP access.

#### 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 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 rregistration 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).

In the RM-DEREGISTERED state, 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 (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:

- When MO signaling is allowed (see clause 5.3.4.3), perform mobility Registration Update procedure if the current TA I of the serving cell (see TS 37.nnn) 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 5GC 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 the UE at any time.

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

In the RM-REGISTERED state, 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, 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 after Implicit Deregistration;

- when applicable, accept or reject Registration Updates from the UE. The AMF may reject a UE registration upon rejecting a Registration Update from the UE;

- when applicable, reject a UE registration by sending a Registration Reject message to the UE. The actions of the AMF upon the 'cause value' in the Registration Reject message. See TS 23.502 [3] clause 4.2.2.

Editor's note: The detailed condition for the network to start the implicit Deregistration timer is FFS.

Editor's note: The detailed condition of implicit Deregistration is FFS.

##### 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

Editor's note: More transition case (e.g. Handover from/to EPS) will be added upon discussion result on Interworking.

#### 5.3.2.3 Registration Area management

Registration Area management comprises the functions to allocate and reallocate a Tracking Area Identity List to a UE. All the tracking areas in a TAI List to which a UE is registered are served by the same serving AMF.

When a UE registers with the network, 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 5.3.4.1)).

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

#### 5.3.2.4 Support of an UE registered over both 3GPP and Non 3GPP access

For a given serving PLMN there is one RM context for an UE even though the UE may be consecutively or simultaneously served by a 3GPP access and a Non 3GPP access (N3IWF) of this PLMN.

An AMF associates the RM context for an UE with:

- a Temporary Identifier that is common between 3GPP and Non 3GPP. This Temporary Identifier is globally unique.

- a registration state per access type (3GPP / Non 3GPP)

Editor's note: It is FFS where it is possible to define an Unique registration state applying to both 3GPP access and Non 3GPP access.

- a registration areas per access type: one registration area for 3GPP access and another registration areas for non 3GPP access.

- A registration timer for 3GPP access.

Editor's note: It is FFS whether a registration timer is used for the registration over Non 3GPP access

The registration area for 3GPP access corresponds to a TA list. The registration area for Non 3GPP access corresponds to a unique reserved TA value (i.e. dedicated to non 3GPP access). There is thus an unique Tracking Area for the non 3GPP access to 5GC.

The TA list provided to the UE over 3GPP access does not refer to the TAI that is associated with non 3GPP access

The AMF assigns a single Temporary Identifier to the UE. The Temporary Identifier is assigned upon the first successful registration of the UE, and is valid over any of both 3GPP and Non 3GPP access for the UE. Upon performing a Registration procedure over the non-3GPP access or the 3GPP access, the UE provides the temporary ID it has received in earlier successful registration over any access. This enables the AN to select an AMF that maintains the UE context created at the first registration procedure, and enables the AMF to correlate the registration request to the existing UE context. The temporary identifier may be re-assigned over any of the 3GPP and Non 3GPP access.

Editor's note: In case Temporary Identifier assigned over 3gpp access refer to a geographical Group Id, a procedure needs to be defined in TS 23.502 [3] to cover following case: an UE whose Temporary Identifier assigned over Non 3GPP access refers to a non geographical Group Id, issues a registration procedure over 3GPP access. In that case an AMF relocation is needed.

The deregistration request may be associated with an indication of whether it applies only to the access on which the de-registration procedure is run or to all accesses of the UE (3GPP and Non 3GPP access).

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

### 5.3.3 Connection Management

Editor's note: Access independent aspects.

#### 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 (e.g. RRC connection over 3GPP 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 that reflect the NAS signalling connectivity of the UE with the AMF:

- CM-IDLE

- CM-CONNECTED

##### 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 and PLMN selection.

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

In the CM-IDLE state, the UE shall, unless otherwise specified in sub-clause 5.3.4.1:

- if not in MO-only mode, respond to paging, if received, by performing a service request procedure (see TS 23.502 [3] clause 4.2.3.2);

- 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).

- enter CM-CONNECTED state whenever an AN signalling connection is established between the UE and the AN (e.g. entering RRC Connected state over 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.

In the CM-IDLE state, the AMF shall:

- if a UE is not in MO-only mode, perform a network triggered service request procedure when it has signaling or mobile-terminated data to be sent to this UE, by sending a Paging Request to this UE (see TS 23.502 [3] clause 4.2.3.3).

- enter CM-CONNECTED whenever an N2 connection is established for this UE between the AN and the AMF.

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 sub-clause 5.4.1.3).

Editor's note: The CM states for the UE that successfully registered via non-3GPP access is FFS.

Editor's note: The definition of AN signaling connection is FFS: over 3GPP access, an AN signaling connection is an RRC connection. Over N3GPP access, an AN signaling connection is FFS

##### 5.3.3.2.3 CM-CONNECTED state

A UE in CM-CONNECTED state has a NAS signalling connection with the AMF over N1.

Editor's note: Whether a N2 connection for the UE in CM-CONNECTED state always exists or not depends on the conclusion on "stickiness" feature.

Editor's note: Whether an RRC connection for the UE in CM-CONNECTED state always exists or not depends on the conclusion on "RAN level paging" feature.

In the CM-CONNECTED state, the UE shall:

- enter CM-IDLE state whenever the AN signaling connection is released (e.g. entering RRC Idle state over 3GPP access), see TS 37.nnn.

In the CM-CONNECTED state, the AMF shall:

- enter CM-IDLE state whenever the N2 signaling connection for this UE is released.

Upon completion of a NAS signalling procedure, the AMF may decide to release the NAS signalling connection with the UE, after which the state at both the UE and the AMF is changed to CM-IDLE.

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

Editor's note: The CM states for the UE that successfully registered via non-3GPP access is FFS.

##### 5.3.3.2.4 5GS Connection Management State models



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 gets CM-IDLE over an access, the UP connection of the PDU sessions that were active on this access gets inactive.

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

#### 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.

When the UE in CM-IDLE state needs to transmit an NAS message, the UE shall initiate a Service Request or a registration procedure to establish a signalling connection to the AMF as specified in TS 23.502 [3] clause 4.1.2 and TS 23.502 [3] clause 4.1.1.

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 5G (R)AN node or the AMF.

The UE considers the NAS signalling connection is released if it detects the RRC connection is released. After the NAS signalling connection is released, the UE and the AMF enters CM-IDLE state.

#### 5.3.3.4 Support of an 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. A maximum of one N2 interface can serve the UE for 3GPP access and a maximum of one N2 interface can serve the UE for Non 3GPP access. An UE may be in any combination of the CM states between 3GPP and Non 3GPP access, e.g. an 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.

Connection Management over Non 3GPP access is further defined in clause 5.5.3.

### 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 in CM-IDLE state are executed by the UE based on information received from the core network. Mobility Restrictions in CM-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 with a Handover Restriction List.

Mobility restrictions consists of RAT restriction, forbidden area, and service area restrictions as follows:

- RAT restriction:  
Defines the 3GPP Radio Access Technology(ies), a UE is not allowed to access. In a restricted RAT a UE is based on subscription not permitted to initiate any communication with the network.

- 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.

- 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 is not allowed to initiate UE triggered Service Request or SM signalling to obtain UE initiated user services (both in CM-IDLE and in CM-CONNECTED states). The UE shall perform periodic and mobility registration updates, and if the UE is not already registered, it may also perform initial registration to attach to network in Non-allowed area due to mobility. The UE in a Non-allowed area shall respond to core network paging with Service Request.

Editor's note: Whether a network initiated Service Request in a Non-allowed area can be used also for normal user services or is limited to the purpose of mobility restriction update, is FFS.

For a given UE, the core network determines the service area restrictions based on UE subscription information. Optionally the allowed area may in addition be fine-tuned by the PCF e.g. based on UE location, and network policies. Service area restrictions can be changed due to, e.g. subscription, location, and/or policy change. Service area restrictions may be updated during a Registration procedure.

If the UE has overlapping areas between RAT restrictions, forbidden areas, allowed areas and non-allowed areas, 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;

- The evaluation of forbidden areas shall take precedence over the evaluation of allowed areas and non-allowed areas; and

- The evaluation of non-allowed area shall take precedence over the evaluation of allowed areas.

A UE shall override any forbidden area and non-allowed area restrictions whenever access to the network is required 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 may contain either allowed or non-allowed areas using explicit tracking area identities, 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.

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 signaling 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. If the UE has been assigned a limited allowed area, any visited tracking area that is not yet in the UE's allowed area is added to the allowed area until the maximum allowed number of tracking areas is reached. If the UE has been assigned a limited allowed area 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 Mobility restrictions, and comply with them in the area that is identified in the Mobility restrictions.

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 in a Non-allowed area to update service area restrictions.

Editor's note: The detailed procedure for the network-initiated update (i.e, whether Registration or a new procedure will be used) is FFS.

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 5G system core network to characterise and optimise the UE mobility. The 5G system core network determines Mobility Pattern of the UE based on subscription of the UE, statistics of the UE mobility, network local policy, and the UE assisted information. The statistics of the UE mobility can be historical or expected UE moving trajectory.

Editor's note: The details of subscription of the UE, network local policy, and the UE assisted information are FFS

Editor's note: The optimized mobility support based on Mobility Pattern is FFS.

Editor's note: It is FFS to figure out appropriate name of the concept.

## 5.4 3GPP access specific aspects

Editor's note: 3GPP access specific aspects - e.g. handover, reachability, paging.

### 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 5G-RAN (in case of CM-CONNECTED state).

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

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

1. UE reachability allowing Mobile Terminated data while the UE is CM-IDLE mode.

- 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 mode.

2. Mobile Initiated Connection Only (MICO) mode:

- Mobile originated data applies in this category for both CM-CONNECTED and CM-IDLE mode.

- Mobile terminated data is only supported when the UE is in CM-CONNECTED mode.

#### 5.4.1.2 UE reachability allowing MICO data while the UE is CM-IDLE

##### 5.4.1.2.1 General characteristics

For this category, the UE reachability is determined by the following aspects:

- The UE reachable time window: when the UE is reachable for paging in CM-IDLE. In the absence of any negotiation of UE reachable time window, the UE is assumed always reachable for paging while in CM-IDLE.

Editor's note: How to negotiate when the UE becomes reachable is FFS and has dependency on RAN procedures for paging.

- UE reachable area: This area is equal to the registration area provided by the AMF during initial registration or registration update procedures.

- High latency communication: the handling of the mobile terminated data in the core network when the UE is unreachable for extended periods of time.

Editor's note: high latency communication handling for 5G system is FFS.

#### 5.4.1.3 Mobile Initiated Connection only (MICO) mode

A UE may indicate preference for MICO mode during initial registration or registration update. The AMF, based on local configuration, 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.

The UE and core network re-initiates or exits the MICO mode at subsequent registration signalling. If MICO mode is not indicated explicitly in Registration, then both the UE and the AMF shall not use the MICO mode.

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. The network, based on local policy, and subscription information, may decide to provide an "all PLMN" registration area indication to the UE. In that case, re-registration to the same PLMN due to mobility does not apply.

Editor's note: It is FFS whether AMF should provide a registration area to UE in MICO mode. If the registration area is provided, the registration area size may be bound to Mobility restrictions (i.e. the registration may be contained by the allowed area) and by requirements to perform tracking for the UE.

When the AMF indicates MICO mode to a UE, the AMF considers the UE always unreachable while in CM-IDLE. The CN rejects any request for downlink data delivery for an MICO UE in idle mode. The CN also defers downlink transport over NAS for SMS, location services, etc. The UE in MICO mode is only reachable for mobile terminated data or signalling when the UE is in CM-CONNECTED mode for the PDU sessions that are resumed.

Editor's note: When the UE is in CM-CONNECTED after it has sent MO Data it is FFS how long the network needs to maintain the UE in CM-CONNECTED to enable delivery of MT Data from an application server and/or DL over NAS of SMS, location services etc.

A UE in MICO mode performs periodic registration at the expiration of periodic registration timer.

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 CM-IDLE to CM-CONNECTED mode procedures due to one of the following triggers:

- A change in the UE (e.g. change in configuration) requires an update its registration with the network.

- Periodic registration timer expires.

- MO data pending.

- MO signalling pending (e.g. SM procedure initiated).

Editor's note: It is FFS whether the AMF indicates to the RAN that the UE is in MICO mode.

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.

#### 5.4.1.4 Mobile Deregistration at the End of Communication

Editor's note: It is FFS to define the name of this functionality.

A UE can perform deregistration at the end of communication without additional NAS signalling. The UE may indicate preference for the deregistration at the end of communication during registration procedure. The AMF determines whether it is supported for the UE, and indicates during the registration signalling. When the AMF applies the deregistration at the end of communication to the UE, the AMF considers the UE enters RM-DEREGISTERED at the release of N2 connection for the UE, and the UE moves to RM-DEREGISTERED when leaving CM-CONNECTED.

### 5.4.2 UE reachability in CM-CONNECTED

For a UE in CM-CONNECTED state:

- the AMF knows the UE location is on a serving (R)AN node granularity.

- when the UE reachability is managed by the 5G RAN, the AMF may provide the UE reachability management policy information to the 5G RAN.

Editor's note: Related content of the UE reachability management policy are FFS.

- the 5G RAN notifies the AMF when UE becomes unreachable from RAN point of view.

Editor's note: The other case of UE reachability detection is FFS. Editor's note: how the AMF is notified is FFS.

NOTE 1: How to do the RAN level reachability detection is to be decided by the RAN WG.

## 5.5 Non-3GPP access specific aspects

### 5.5.1 General

When the UE is successfully registered to an access (e.g. a 3GPP access or a non-3GPP access respectively) and the UE registers to a second access:

- if the second access is located in the same PLMN (e.g. the UE is registered to a 3GPP access and selects a N3IWF located in the same PLMN), the UE shall use for the registration to the new access the Temporary UE identifier that the UE was provided at the first registration.

- if the second access is located in a PLMN different from the PLMN of the first access (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 not use for the registration to the new access the Temporary UE identifier that the UE was provided at the first registration.

### 5.5.2 Registration Management

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

Editor's note: It is FFS whether the UE needs to support periodic registration update procedures over Non 3GPP access

### 5.5.3 Connection Management

In case of Untrusted Non 3GPP access to 5G Core the release of the Nwu signalling connection between the UE and the N3IWF is interpreted

- By the UE as a criteria to go to CM-IDLE state for the Non 3GPP access.

- By the N3IWF as a criteria to release the N2 connection.

In case of Untrusted Non 3GPP access to the 5G Core, 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. When the N2 signalling connection is released, the UE state in the AMF for the non-3GPP access is CM-IDLE.

An UE cannot be paged on non 3GPP access.

## 5.6 Session Management

Editor's note: This should include session management etc.

Editor's note: Handling ATSSS is FFS.

### 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.

Editor's note: It is FFS whether "DNN" or "APN" is to be used.

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 (where the type of PDU exchanged between the UE and DN is totally transparent to the 5G system).

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 the UE to establish a PDU session to a specific DNN.

The SMF is responsible of checking whether the UE requests are compliant with the user subscription. For this purpose it retrieves SMF level subscription data from the UDM. Such data may indicate per DNN:

- The allowed PDU session Type.

- Whether in case of Home Routed the VPLMN is allowed to insert an UL CL or a Branching Point for a PDU session towards this DNN..

This information is provided to the SMF in VPLMN by the SMF in HPLMN.

- The allowed SSC modes.

Editor's note: The exact list of subscription data mentioned above will be refined. This will take into account the output of other key issues (slicing, QoS, etc.).

Editor's note: It is FFS whether SMF level subscription data is defined per slice

An UE that is registered over multiple accesses chooses over which access to establish a PDU session.

Editor's note: The choice of the access to use for a PDU session is based at least on network policy, service requirements and user subscription. The definition of policy for selecting the access to route the PDU Sessions (e.g. service requirements, user subscription, etc.) and how it is used are FFS.

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 Id as defined in clause 5.3.2. The UE may also provide:

- A PDU session Type.

- Slicing information.

Editor's note: slicing related information is to be further clarified. An S-NSSAI information is meant.

- The DNN (Data Network Name).

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

Editor's note: It is FFS Whether the UE may also provide and information indicating its willingness to move a PDU session between 3GPP and Non 3GPP access.

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 |
| Slicing information | No | (Note 1)(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) may correspond to different default SSC modes and different default PDU session Types  NOTE 2: Slicing information and DNN are used by AMF to select a SMF to handle a new session. Refer to clause 5.2. | | |

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 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.

### 5.6.2 Interaction between AMF and SMF

The AMF and SMF are separate Network Functions.

N1 related interaction is as follows:

- A 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 single N1 termination point is located in AMF. The AMF forwards SM related NAS information to the SMF.

- 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. In that case the serving PLMN ensures that for N1 NAS signalling received by the AMF over an access (e.g. 3GPP access or non-3GPP access) further SM NAS exchanges (e.g. SM NAS message responses) are transported over the same access.

- AMF handles the Registration Management and Connection Management part of NAS signalling exchanged with the UE. SMF handles the Session management part of NAS signalling exchanged with the UE.

- RM/CM NAS messages and SM NAS messages and the corresponding procedures are decoupled, so that the NAS routing capabilities inside AMF can easily know if one NAS message should be routed to a SMF, or locally processed in the AMF. It is possible to transmit an SM NAS message together with an RM/CM NAS message.

NOTE: Whether this implies encapsulating the SM NAS message in an RM/CM NAS message or not is FFS and should be defined at stage 3.

- AMF can decide whether to accept the RM/CM part of a NAS request without being aware of the possibly concatenated SM part of the same NAS signalling contents.

- When a SMF has been selected to serve a specific PDU session, AMF has to ensure that all NAS signaling related with this PDU session is handled by the same SMF instance.

- 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.

Editor's note: this text may have to be revisited when further progress has been made on the non stickyness topic.

N2 related interaction is as follows:

- N2 signalling related with UE is terminated in the AMF i.e. there is a unique N2 termination for a given UE regardless of the number of PDU sessions (possibly zero) of a UE.

- 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.

N3 related interaction is as follows:

- In case of UE having multiple established PDU sessions using multiple UPFs, the SMF supports the independent activation of UE-CN user plane connection per PDU session.

N4 related interaction is as follows:

- The SMF(s) supports the end-to-end control functions on PDU sessions (including any N4 interface to control the UPF(s)).

- 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. If the UE is in CM\_IDLE state the AMF may trigger UE paging from the AN (depending on the type of AN).

Editor's note: Precise details of the interaction for paging depend on the definition of paging mechanisms for the NextGen system. Interaction with power saving states is also FFS.

### 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.

NOTE1: 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 shall be able to control (via subscription data) per DNN 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 permanent user identity 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 regards 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 is able to control whether the VPLMN is allowed to route traffic locally. The SMF in VPLMN may activate mechanisms of local offload described in clause 5.6.4 only if it has explicitly received the corresponding authorization from the SMF in HPLMN.

- The SMF in VPLMN may, when local traffic offloading is allowed by the SMF in HPLMN for the PDU session, generate related SM signalling towards the UE.

- The SMF in HPLMN may send QoS requirements associated with a PDU session to the SMF in VPLMN. This may happen at PDU session activation and later on while the PDU session is already 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.

Information within NAS SM messages is split up between information that any SMF needs to understand and information that an SMF in VPLMN serving a PDU session in HR mode is not meant to understand but to relay transparently to the SMF in HPLMN.

NOTE2: The UE does not know whether the SMF in VPLMN can understand some information or not, and whether a PDU session will be in HR or LBO. The UE simply provides the two sets of information separately, then whether the SMF in VPLMN can process them or not depends on the SMF, not on the UE.

### 5.6.4 Single PDU session with multiple PDU session anchors

#### 5.6.4.1 General

In order to support traffic offloading 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 an PDU session anchor functionality. Each PDU session anchor supporting a PDU session provides a different access to the same DN.

Editor's note: The terminology "PDU session anchor" is to be revisited.

Editor's note: Proper terminology improvement is needed to distinguish Local Break Out (when referring to roaming) and offload for local traffic

This may correspond to

- The Usage of an 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 or to remove from the data path of a PDU session a UPF supporting the UL CL functionality either during or 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 insertion of an UL CL in the data path of a PDU session and of the traffic diversion by the UL CL. In case of a PDU session of IP type, the UE associates the PDU session with either a single IPv4 address or a single IPv6 Prefix allocated by the network.

Editor's note: The normative phase will determine whether it is needed to make the UE aware that access to local services is possible and if yes how.

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.

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 2: 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.

The insertion of an UPF 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 3: The same UPF may support both the UL CL and the PDU session anchor functionalities

In Home Routed case the visited operator is only allowed to use local access to a DN in case the home operator has explicitly allowed it.

Editor's note: The Relationship between SSC mode 1and Uplink Classifier is FFS.

#### 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 PDU Session provides access to the Data Network via more than one PDU (IPv6) anchor. The different user plane paths leading to the IP 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 IP anchors and merge of DL traffic to the UE i.e. merging the traffic from the different IPv6 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 or to remove from the data path of a PDU session a UPF supporting the Branching Point functionality either during or after the PDU session establishment.

Multi homing of a PDU session applies only for PDU sessions of IPv6 type.

The use of multiple IPv6 prefixes in a PDU session relies on:

- 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 (selected by the UE based on rules received from the network).

- IETF RFC 4191 [8] is used to configure rules 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 Multihoming 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.



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

NOTE 2: The same UPF may support both the Branching Point and the PDU session anchor functionalities



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

NOTE 3: The same UPF may support both the Branching Point and the PDU session anchor functionalities

Editor's note: Further clarification is needed to highlight in the figures the difference between figure 5.6.4.3-1 that addresses a mobility case and figure 5.6.4.3-2 that addresses local offload i.e. that refers to one of the PDU session anchors being deployed topologically near the AN

In case of HR roaming, the visited operator is allowed to use an IP anchor in the VPLMN only in case the home operator has explicitly allowed it.

Editor's note: The Relationship between SSC mode 1and multi-homing is FFS.

### 5.6.5 Support for connecting to a local area data network

5G System shall provide support for the UEs to connect to a local area Data Network reachable within certain area.

Editor's note: The granularity and type of location information and data network identification related information are FFS.

The 5G core network notifies the UE of the information for the specific local area Data Network which are available to the UE, based on the operator's policy and subscription information.

Editor's note: It is FFS how the 5G core network notifies the UE, e.g. whether the AMF notifies the UE of information or whether the direct interface between the UE and the PCF.

Based on the local area Data Network information received in the notification, the UE may request a PDU session establishment for the notified local area Data Network while the UE is located in the area.

### 5.6.6 DN authorization of the establishment of a PDU session

At the establishment of a PDU Session to a DN:

- The UE/user may be authenticated/authorized by the DN.

- If the UE/user provides authentication/authorization information during the establishment of the PDU session, and the SMF determines that authentication/authorization of the PDU session establishment is required based on on the DN policy, the SMF passes the authentication/authorization information of the UE to the DN via the UPF. 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.

Editor's note: the definition of the user is FFS

- The DN may authenticate/authorize the PDU session establishment.

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 with regard to subscription data retrieved from UDM enforced by SMF.

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

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

NOTE 1: The way for the UE to acquire such information is not defined.

Editor's note: The details of the NAS SM information provided by the UE for authentication/authorization of the PDU session are for FFS and depend on SA3 security design.

Editor's note: The extent of specification work in 3GPP to enable such authorization/authentication depends on SA WG3 work and is FFS.

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.

At any time, a DN may revoke the authorization for a PDU session.

### 5.6.7 Application Function influence on traffic routing

Editor's note: Roaming case is FFS.

An Application Function may send requests to influence SMF routeing decisions for traffic of PDU session. This may influence UPF selection and allow routeing user traffic to a local access to a Data Network

Such requests may contain at least:

- Information to identify the traffic to be routed. The traffic can be identified by the DNN, and an application identifier or traffic filtering information.

Editor's note: Mapping between the information provided by the Application Function and the information used in the Core Network, if needed, is FFS.

- Information on where to route the traffic. Individual UEs identified using either External Identifer or MSISDN, all UEs, or groups of UEs.

- Potential locations of the Application Functions to where the traffic routing should apply. The potential locations of the AFs may e.g. by used for UPF selection.

Editor's note: The normative phase will determine the nature of the Location Information exchanged with the application environment.

- Information on the UE(s) whose traffic is to be routed.

Editor's note: It is FFS How a group of UEs can be identified in the request

- Information on when (time indication) the traffic routing is to apply.

The Application Function issuing such requests is assumed to belong to the PLMN serving the UE. The Application Function may issue requests on behalf of other Application Functions not owned by the PLMN serving the UE.

SMF may, based on local policies, take this information into account to:

- (re)select UPF(s) for PDU sessions.

- activate mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL). Such mechanisms are defined in clause 5.3.5. This may include providing the UPF with traffic forwarding (e.g. break-out) rules.

- inform the Application Function of the (re)selection of the UP path.

Editor's note: The normative phase will determine how the application function request is routed to SMF e.g. whether the SMF receives it from the NEF or the PCF.

An Application Function may request to get notified about the Location Information of UE(s).

Editor's note: The nature of the Location Information exchanged with the application environment will be determined during the normative phase.

### 5.6.8 Selective activation of UP connection of existing PDU session

This clause applies to the case when a UE has multiple established PDU sessions. The activation of UP connection of existing PDU session causes UE-CN User Plane connection (i.e. data radio bearer and N3 tunnel) for the PDU session to be activated. The UP connection of different PDU sessions can be activated independently.

For the UE in the CM-IDLE state, either UE or network-triggered Service Request procedure may support independent activation of UP connection of existing PDU session.

An UE in the CM-CONNECTED state invokes a Connection Management (i.e. handled by AMF) procedure to request the independent activation of the UP connection of existing PDU sessions.

Editor's note: Which CM procedure is to be described in TS 23.502 [3] but it is expected to be similar to a Service Request procedure.

Editor's note: Whether CN-initiated PDU session deactivation is necessary or not is FFS.

### 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) modesdefined in this clause. The SSC mode associated with a PDU session anchor does not change during the lifetime of a PDU session.

#### 5.6.9.2 SSC mode

#### 5.6.9.2.1 SSC Mode 1

For 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 IP type, IP continuity is supported regardless of UE mobility events.

In this release, for a multi-homed PDU session the SSC mode 1 applies only to the first Prefix of the PDU session: for such sessions, if the network decides (based on local policies) to allocate additional PDU session anchors / Prefixes to a PDU session established in SSC mode 1, SSC mode 3 applies to these additional Prefixes.

In this release, when UL CL applies to a PDU session the SSC mode 1 applies only to the Prefix/address sent to the UE, If the network decides (based on local policies) to allocate additional PDU session anchors to such a PDU session, SSC mode 2 applies to these additional PDU session anchors.

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

#### 5.6.9.2.2 SSC Mode 2

For PDU session of SSC mode 2, 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. At establishment of the new PDU Session, a new UPF acting as PDU session anchor can be selected.

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

In case of multi-homed PDU sessions or in case UL CL applies to a PDU session SSC mode 2 applies to all PDU session anchors of the PDU session.

NOTE: In UL CL mode 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 case of a PDU session of IP Type, during the procedure of change of PDU session anchor,

- the new IP prefix anchored on the new PDU session anchor may be allocated within the same PDU session (relying on IPv6 multi-homing defined specified in clause 5.6.4) or

- This may apply to the case of a PDU session set up in SSC mode 3 or to the additional PDU session anchors of a PDU session established in SSC mode 1

- the new IP address/prefix may be allocated within a new PDU session that the UE is triggered to establish.

- This may only apply to the case of a PDU session set up in SSC mode 3

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.

#### 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; and:

a) If the UE has already an active 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 as part of the subscription information.

Editor's note: Whether SSC mode related subscription is related with slicing is FFS.

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 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.

The SMF shall inform the UE of the selected SSC mode for a PDU session.

## 5.7 QoS model

### 5.7.1 General Overview

The 5G QoS model supports QoS flow based framework. The 5G QoS model supports both QoS flows that require guaranteed flow bit rate and QoS flows that do not require guaranteed flow bit rate. 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 value within a PDU session receives the same traffic forwarding treatment. The QFI is carried in an encapsulation header on N3 i.e. without any changes to the e2e packet header. It can be applied to PDUs with different types of payload, i.e. IP packets, non-IP PDUs and Ethernet frames. The QFI shall be unique within a PDU session.

NOTE 0: A certain range of QoS Flow IDs (QFIs) is reserved for A-type QoS flows where the "full" QoS profile will not be used. These QFIs will map directly to standardized 5QIs and a default ARP value.

Each QoS flow (GBR and Non-GBR) is associated with the following QoS parameters (details are described in clause 5.7.2):

- 5G QoS Indicator (5QI),

- Allocation and Retention Priority (ARP).

Each GBR QoS flow is in addition associated with the following QoS parameters (details are described in clause 5.7.2):

- Guaranteed Flow Bit Rate (GFBR) - UL and DL;

- Maximum Flow Bit Rate (MFBR) - UL and DL;

- Notification control.

The QoS parameters of a QoS flow are provided to the (R)AN over N2 at PDU Session or at QoS flow establishment and when 5G-RAN is used at every time the User Plane is activated. QoS parameters may also be pre-configured in the (R)AN for non-GBR QoS flows (i.e. without the need to be signalled over N2).

The network provides QoS rules to the UE for the classification and marking of UL traffic, i.e. the association of uplink traffic to QoS flows. These rules can be explicitly signaled over N1, pre-configured in the UE or implicitly derived by UE from reflective QoS. A QoS rule contains the QFI of the QoS flow, packet filter**s** and corresponding precedence values. A default QoS rule is provided to the UE at PDU Session establishment, i.e. the default QoS rule shall include a packet filter which may be a match-all packet filter and an evaluation precedence value with highest possible value. In addition, pre-authorized QoS rules may be provided to the UE. QoS rules can be also provided at QoS flow establishment.

The principle for classification and marking of User Plane traffic to QoS Flows and mapping to AN resources is illustrated in Figure 5.7.1-1.



Figure 5.7.1-1: The principle for classification and User Plane marking for QoS Flows and mapping to AN Resources

In DL incoming data packets are classified based on SDF filters. The CN conveys the classification of the User Plane traffic belonging to a QoS flow through an N3 User Plane marking using a QFI. All A-type QoS flows are allocated a standardized or pre-defined QFI value, and the standardized or pre-defined QFI value is associated with a specific 5QI value and default ARP. The AN binds QoS flows to AN resources (i.e. Data Radio Bearers in case 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 to map the QoS flows to DRBs so that the UE receives the QFI (and reflective QoS (see clause 5.7.5) can be applied).

In UL, the UE classifies packets based on the uplink packet filters in the QoS rules and conveys the classification of the User Plane traffic belonging to a QoS flow through a User Plane marking using the QFI in the corresponding QoS rule. The UE binds QoS flows to AN resources.

The UE evaluates for a match, first the uplink packet filter amongst all packet filters in the QoS rules that has the lowest evaluation precedence index and, if no match is found, proceeds with the evaluation of uplink packet filters in increasing order of their evaluation precedence value. This procedure shall be executed until a match is found or all uplink packet filters have been evaluated. If a match is found, the uplink data packet is with the QFI that is associated with the matching packet filter. If no match is found and the default QoS rule contains one or more uplink packet filters, the UE shall discard the uplink data packet.

Two ways to control QoS flows are supported:

1) For A-type QoS flows, all the necessary QoS profile(s) (i.e. QoS Parameters) are either sent to (R)AN via N2 at time of PDU Session establishment or when the user plane of the PDU session is activated and no additional signaling is required at the time traffic for the corresponding QoS flows start, or the QoS profiles are pre provisioned or standardized and no N2 signaling is required.

2) For B-type QoS flows, all the necessary QoS profile(s) (i.e. 5G QoS characteristics using either 5QI or individual provided and QoS Parameters) are sent to (R)AN with N2, N7, N11 signaling. B-Type QoS Flows can be added or removed dynamically via signaling during the PDU session.

Editor's note: It is FFS whether to re-name A- and B-type QoS flows.

NOTE 1: A-type and B-type QoS flows must use a different value range for the QFI. There can be multiple A-type and/or B-type 5G QoS Flows with unique QoS profile per each QoS flow within a PDU session.

NOTE 2: For A-type QoS flows, the AN derives the 5G QoS characteristics from the 5QI value the QFI is referring to.

NOTE 3: In a 3GPP access, it is not prevented to use A-type GBR 5G QoS Flows, but since admission control in (R)AN will be performed at time of PDU Session establishment this could lead to resource waste until the traffic of the SDFs mapped to this 5G QoS Flow starts.

The following characteristics apply for processing of Downlink traffic:

- UPF maps Service data flow (SDF) to QoS flows

- UPF performs Session AMBR enforcement and also performs PDU counting for support of charging.

- UPF transmits the PDUs of the PDU session in a single tunnel between 5GC and (R)AN, the UPF includes User Plane marking (including the 5QI for non3GPP accesses) 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 downlink, e.g. setting the DiffServ Code point in outer IP header. Transport level packet marking can 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 QFIand the associated 5G QoS characteristics and parameters, also taking into account the N3 tunnel associated with the downlink packet.

NOTE 4: Packet filters are not used for binding 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 in the derived QoS rule is derived from the (i.e. the header of the) DL packet, and the User Plane marking of the derived QoS rule is given the User Plane marking of the DL packet.

Following characteristics apply for processing of uplink traffic:

- UE uses the stored QoS rules to determine mapping between SDFs and QoS flow. UE 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 determines the QFI value, which is included in the encapsulation header of the UL PDU, and selects the N3 tunnel.

- (R)AN performs transport level packet marking in the uplink, transport level packet marking can be based on the 5QI and ARP of the associated QoS Flow.

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

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

For UL Classifier PDU sessions, UL and DL Session AMBR shall be enforced in the UPF that supports the UL Classifier functionality. For multi-homed PDU sessions, UL and DL Session-AMBR is enforced separately per UPF that terminates the N6 interface (i.e. without requiring interaction between the UPFs) (see clause 5.6.4). The (R)AN shall enforce Max BitRate (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 PDU 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 5G QoS flows. The MBR is enforced in the UPF.

### 5.7.2 5G QoS Parameters

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.).

The 5QI in the standardized value range have one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in Table 5.7.5-1.

For non-standardized combinations of 5G QoS characteristics, a 5QI value from the non-standardized value range together with the 5G QoS characteristics are signalled over N2, N11 and N7 at the time of PDU session or QoS flow establishment.

NOTE 1: 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. The same applies to the N9 interfaces. 5QI in standardized and non-standardized value range can be used for B-Type 5G QoS flows based on PCC decisions. Only 5QIs in standardized value range can be used for B-Type 5G QoS flows.

Editor's note: It is FFS whether the ARP is included within the 5G QoS Profile sent to the UE.

Editor's note: It is FFS how the ARP for QoS Flows with A-type flows is determined.

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 can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). It can 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 can 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 can 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 can 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 X: 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.

In addition, the QoS flow may be associated with the parameter:

- Notification control.

The Notification control may be provided for GBR QoS flows. The Notification control indicates whether notification should be made by the RAN if the QoS targets cannot be fulfilled for a QoS flow during the lifetime of the QoS flow. If it is set and QoS targets cannot be fulfilled, RAN sends a notification towards SMF.

Editor's note: It is FFS whether the Notification control is needed for non GBR QoS flows.

For GBR QoS flows, the 5G QoS profile additionally include the following QoS parameters:

- Guaranteed Flow Bit Rate (GFBR) - UL and DL;

- Maximum Bit Rate (MFBR) -- UL and DL.

The GFBR denotes the bit rate that can be expected to be provided by a GBR QoS flow. The MFBR limits the bit rate that can 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, N11, and N7 for each of the GBR 5G QoS Flows for setting up the 5G QoS profile.

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 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. 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.

Editor's note: The above definition needs to be discussed for multi-homing PDU sessions.

Each UE is associated with the following aggregate rate limit QoS parameter:

- per UE Aggregate Maximum Bit Rate (UE-AMBR).

The subscribed UE-AMBR is a subscription parameter which is retrieved from UDM. The UE-AMBR is set to the sum of the Session-AMBR of all PDU Sessions with active user plane up to the value of the subscribed 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.

Editor's note: It is FFS which network entity is responsible for determining the value of UE-AMBR.

### 5.7.3 5G QoS characteristics

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 or Non-GBR);

2 Priority level;

3 Packet Delay Budget;

4 Packet Error Rate.

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.

The 5G QoS characteristics for 5QI in the standardized value range are not signalled on any interface.

The 5G QoS characteristics for 5QI in the non-standardized value range, are signalled over N2, N11 and N7 at the time of the PDU Session or QoS flow establishment.

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.

The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the PCEF. For a certain 5QI the value of the PDB is the same in uplink and downlink. 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).

NOTE 1: The PDB denotes an end-to-end "soft upper bound".

Editor's note: What will be the PDB confidence level e.g. whether 98 percent is enough or a more aggressive confidence level e.g. 99 percent is needed for 5G is FFS.

The Packet Error Rate (PER) defines an upper bound for the rate of SDUs (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 a certain 5QI the value of the PER is the same in uplink and downlink.

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.

### 5.7.4 Standardized 5QI to QoS characteristics mapping

The one-to-one mapping of standardized 5QI values to 5G QoS characteristics is specified in table 5.7.5-1.

Table 5.7.5-1: Standardized 5QI to QoS characteristics mapping

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5QI  value | Resource Type | Priority Level | Packet Delay Budget | Packet Error  Rate | Example Services |
| 1 |  |  |  |  |  |
| 2 | GBR |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 65 |  |  |  |  |  |
| 66 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 | Non-GBR |  |  |  |  |
| 69 |  |  |  |  |  |
| 70 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | | | | | |

Editor's note: A table showing QFI value mapping to 5QI values is to be added, i.e. a range of QFI values are one-to-one mapped to non.GBR 5QI values, and the rest of the QFI values are associated to QoS characteristics/parameters which are either signalled or pre-configured.

### 5.7.5 Reflective QoS

#### 5.7.5.1 General

The support for reflective QoS over AN is under control of the 5GC. The reflective QoS is achieved by creating a derived QoS rule in the UE based on the received downlink traffic. It shall be possible to apply reflective QoS and non-reflective QoS concurrently within the same PDU session. For traffic that is subject to reflective QoS, the UL packet gets the same QoS marking as the reflected DL packet.

#### 5.7.5.2 UE Reflective QoS Procedures

##### 5.7.5.2.1 General

For a UE supporting reflective QoS function, and if reflective QoS function is enabled by the 5GC for some traffic flows, the UE shall create a derived QoS rule for the uplink traffic based on the received downlink traffic. The UE shall use the derived QoS rules to determine mapping between uplink traffic and QoS flow.

##### 5.7.5.2.2 UE Derived QoS Rule

The UE derived QoS rule contains following parameters:

- Packet Filter

- QFI

- precedence value.

The UL packet filter is derived based on the received DL packet.

When Reflective QoS is activated via User Plane the precedence value for all derived QoS rules is set to a standardised value.

Editor's note: When Reflective QoS is activated via User Plane it is FFS whether and how the standardised value is overridden by a new value on per-PDU Session basis.

When Reflective QoS is activated via Control Plane the precedence value for a derived QoS rule within the scope of the Control Plane activation (i.e. QoS Flow, PDU Session) is set to a value that is signalled via the Control Plane.

#### 5.7.5.3 UPF Procedures for Supporting Reflective QoS

When the User Plane reflective QoS is enabled by the 5GC, the UPF shall include the Reflective QoS Indication (RQI) in the encapsulation header on N3 reference point together with the QFI.

#### 5.7.5.4 Enabling Reflective QoS

##### 5.7.5.4.1 General

Reflective QoS can be activated via User Plane and Control Plane. The 5GC determines whether to enable the reflective QoS function via Control Plane or User Plane based on policies and type of access.

##### 5.7.5.4.2 Reflective QoS Activation via User Plane

When the 5GC determines to activate reflective QoS via U-plane, the SMF shall include a QoS rule including an indication to the UPF to activate User Plane with user plane reflective. When the UPF receives a DL packet matching the QoS rule that contains an indication to activate reflective QoS, the UPF shall include the RQI in the encapsulation header on N3 reference point. The UE creates a UE derived QoS rule when the UE receives a DL packet with a RQI.

NOTE: The Reflective QoS activation via User Plane is used to avoid out-of-band signalling (e.g. for some non 3GPP accesses).

##### 5.7.5.4.3 Reflective QoS Activation via Control Plane

When the 5GC determines to activate reflective QoS via Control Plane, the SMF shall include the RQI in the QoS rule which is sent to the UE via N1 interface. When the UE receives a DL packet matching the QoS rule that contains the RQI the UE creates a UE derived QoS rule.

NOTE: The Reflective QoS activation via ControlPlane is used for coarse-grained (e.g. per QoS flow or per PDU Session).

#### 5.7.5.5 Disabling Reflective QoS

#### 5.7.5.5.1 General

The 5GC supports disabling reflective QoS.

Editor's note: How and when the S5GC disable the reflective QoS function is FFS.

## 5.8 User plane Management

Editor's note: this should include IP address management.

### 5.8.1 IP address management

#### 5.8.1.1 General

This clause applies to UE establishing a PDU session of PDU type IPv4, IPv6.

SMF shall perform IP address allocation to the UE based on the selected IP version. That is, if IPv4 PDU type is selected, an IPv4 address is allocated to the UE. If IPv6 PDU type is selected, an IPv6 prefix is allocated to the UE. For Roaming case, the SMF in this section 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.

For IPv4 PDU type, NGC and UE support the following IP address configuration:

a. During PDU session setup procedure, the SMF sends the IP address and IPv4 parameter configuration (e.g. DNS server address) to the UE via SM NAS signalling.

b. Alternatively, if DHCPv4 is used according to RFC 2131 [9], the SMF sends the IPv4 address and related IPv4 configuration information to the UE via DHCPv4. For this purpose the SMF configures the UPF acting as an IP anchor to forward all the DHCPv4 messages between the UE and the SMF.

For IPv6 PDU type, NGC and UE use SLAAC for IP prefix configuration:

The SMF sends a Router Advertisement message (solicited or unsolicited) to the UE via the UPF along with IPv6 parameter configuration via Stateless DHCPv6 according to RFC 4862 [10] and RFC 3736 [14]. For this purpose it configures the UPF acting as an IP anchor to forward all the RS/RA and DHCPv6 messages between the UE and the SMF.

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].

Editor's note: Static IP address/prefix allocation based on subscription data is FFS.

#### 5.8.1.2 Routing rules configuration

When the UE has multiple IPv6 PDU sessions to the same Data Network Name (DNN) with multiple IP prefixes, the UE selects the IP prefix according to routing rules pre-configured in the UE or received from network.

For IPv6 multi-homed PDU session the SMF can send routing rules along with IP prefixes to the UE to influence the source IP prefix selection in IPv6 Router Advertisement (RA) messages according to RFC 4191 [8]. Such messages are sent via the UPF.

Further, NGC supports the delivery of routing rules together with IP prefix allocation to the UE any time after the PDU session setup procedure is completed.

Editor's note: It is FFS whether the SMF provides routing rules to the UE in case of IPv4 PDU type.

### 5.8.2 User Plane Function(s)

User Plane Function(s) (UPF(s)) handle the user plane path of PDU sessions. An UPF that provides the interface to a Data Network supports the functionality of a PDU session anchor.

The number of UPFs for a PDU Session is not restricted by the3GPP specifications but specifications support deployments with a single UPF or multiple UPFs for a given PDU session.

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 sub-clause 5.6.4.

UPF traffic detection capabilities may be used by the SMF in order to control at least following features of the UPF:

- Traffic reporting (e.g. allowing SMF support for charging)

- QoS enforcement

- traffic routing (e.g.as defined in clause 5.6.4. for UL CL or IPv6 multi-homing)

The UPF traffic detection capabilities may detect traffic based on traffic pattern for mapping at least any combination of:

- PDU session.

- 5QI.

- 802.1q header (in case of PDU session Type Ethernet).

- Source/destination IP address or IPv6 network prefix.

- Source / destination port.

- Application Identifier: The Application ID is an index to a set of application detection rules configured in UPF.

- protocol ID of the protocol above IP.

- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.

In the pattern:

- a value left unspecified in a filter matches any value of the corresponding information in a packet.

- an IP address or Prefix may be combined with a prefix mask.

- port numbers may be specified as port ranges.

UPF selection is described in clause 6.2.

## 5.9 Identities

Editor's note: This could include describe different types of identities - permanent and temporary identities.

### 5.9.1 Subscriber Permanent Identity

A globally unique 5G Subscriber Permanent Identity (SUPI) shall be allocated to each subscriber in the 5G system.

The following have been identified as valid SUPI types for this Release:

- IMSI for UEs supporting at least one 3GPP Access Technology

Editor's note: Whether other SUPI types need to be defined depending on the use cases is FFS until SA WG1 and SA WG3 work is completed.

In order to enable roaming scenarios, the SUPI shall contains the address of the home network (e.g. the IMSI MCC and MNC).

For interworking with the EPC, the 3GPP UE shall always be allocated SUPI in the IMSI format to enable the UE to present an IMSI to the EPC.

### 5.9.2 Permanent Equipment Identifier

A Permanent Equipment Identifier (PEI) is defined for the physical device accessing the 5G system.

The PEI can assume different formats for different device 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.

## 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 protection.

- Control Plane signalling confidentiality and integrity protection.

Editor's note: Whether User identity confidentiality protection is part of security function is FFS.

Editor's note: Detailed description for the security functions will be addressed after the corresponding SA WG3 work is concluded.

## 5.11 Support for Dual connectivity, Multi-connectivity

Editor's note: This could include functional description for architecture impact due to 3GPP RAN dual connectivity, 3GPP RAN multi connectivity. Support for 3GPP RAN multi-connectivity is dependent on support for multi-connectivity in RAN, when it is supported, this section will be used to capture the architecture impact due to 3GPP RAN multi-connectivity.

## 5.12 Charging

Editor's note: Charging description - level of detail as in TS 23.401 - details to be specified by SA WG5.

## 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.

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, location, 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.X for details).

The functionality supporting for edge computing includes:

- Local Routing: the 5G core network selects UPF to route the user traffic to the local Data Network.

- Traffic Steering: the 5G core network selects the traffic to be routed to the Application Functions in the local Data Network.

- Session and service continuity to enable UE and Application Function mobility.

- User plane selection and reselection ,e.g. based on input from Application Function.

- Network capability exposure: 5G core network and Application Function to provide information to each other via NEF as described in clause 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.

## 5.14 Policy Control

Editor's note: Policy description. Delta over EPS PCC framework can be specified here.

## 5.15 Network slicing

### 5.15.1 General

Editor's note: It is FFS for the following definitions ...

The network slice is a complete logical network that comprises of a set of network functions and corresponding resources necessary to provide certain network capabilities and network characteristics. It includes both 5G-AN and 5G CN. A Network Slice Instance (NSI) is the Instantiation of a Network Slice, i.e. a deployed set of network functions delivering the intended Network Slice Services according to a Network Slice Template.

A network slice comprises all the resources required to fulfil the service and may include:

- the Core Network control plane and user plane Network Functions, as described in clause 4.2, as well as their resources (in terms of compute, storage and network resources, including the transport resources between the Network Functions),

- the 5G Radio Access Network described in TS 38.xxx [x],

- the N3IWF functions to the non-3GPP Access Network described in clause 4.2.7.2, and their respective resources in case the network slice is supporting a roaming service, the network slice encompasses the VPLMN part and the HPLMN part of the network slice.

Network slices may differ for supported features and network functions optimisations. The operator may 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 may be dedicated to a customer.

A single UE can simultaneously be served by one or more Network Slice instances via a 5G-AN. 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.

Editor's note: The following text is FFS ...

The AMF discovery and selection for the set of slices for a UE is triggered by the first contacted AMF in a registration procedure and it may lead to change of AMF. SMF discovery and selection is initiated by the AMF when a SM message to establish a PDU session is received from the UE. The NRF is used to assist the discovery and selection tasks.

A PDU session belongs to a specific Network Slice instance. Different Network Slice instances do not share a PDU session, though different slices may have slice-specific PDU sessions using the same DNN.

### 5.15.2 Identification and selection of a Network Slice: The S-NSSAI and the NSSAI

An S-NSSAI (Single Network Slice Selection Assistance information) 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 allow further differentiation for selecting an Network Slice instance from the potentially multiple Network Slice instances that all comply with the indicated Slice/Service type. This information is referred to as SD.

The S-NSSAI can have standard values or PLMN-specific values. S-NSSAIs with PLMN-specific values are associated to the PLMN ID of PLMN that assigns it. An S-NSSAI 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.

Editor's note: Whether a single value which is a representation of a collection of the S-NSSAIs could also be used as NSSAI is FFS.

The NSSAI is a collection of S-NSSAIs (Single Network Slice Selection Assistance Information). Each S-NSSAI assists the network in selecting a particular Network Slice Instance. The CN part of a Network Slice instance(s) serving a UE is selected by CN not by the RAN.

Editor's note: Whether NSSAI is used for selection for the RAN part of the slice, it is up to RAN WGs.

### 5.15.3 Subscription aspects

Subscription data include the S-NSSAI of the Network Slices that the UE subscribes to. One or more S-NSSAIs can be marked as default S-NSSAI. If an S-NSSAI is marked as default, then the network is expected to serve the UE with the related Network Slice even when the UE does not send any S-NSSAI to the network in a Registration request.

Editor's note: The following is FFS …

The UE subscription data may contain a default DNN value for a given S-NSSAI.

The NSSAI the UE provides in the Registration Request is verified against the user's subscription data.

### 5.15.4 UE NSSAI configuration and NSSAI storage aspects

A UE can be configured by the HPLMN with NSSAI. This is defined as Configured-NSSAI. A Configured NSSAI is PLMN-specific unless it is solely comprised of Standard S-NSSAI values, in which case the PLMN ID in the Configured NSSAI needs not be specified if it applies to all PLMNs a UE could roam to. A UE can be configured with NSSAI for several PLMNs.

Upon successful completion of a UE's Registration procedure, the UE may obtain from the AMF an NSSAI, which may include one or more S-NSSAIs that shall be used by the UE for subsequent slice selection related procedures. This is known as Accepted NSSAI.

The UE shall store the Accepted NSSAI for each PLMN. The UE shall use the Accepted NSSAI when returning to the PLMN.

### 5.15.5 Detailed Operation Overview

When a UE Registers with a PLMN. the UE shall provide to the network in RRC and NAS layer either the Configured-NSSAI, the Accepted NSSAI or sub-set of those, if stored in the UE.

Editor's note: Whether NSSAI in RRC and NAS are exactly the same, is to be determined. The NSSAI is used to select the AMF, whereas, the S-NSSAI is used to assist the selection of a Network Slice instance.

The UE shall store a Configured and/or Accepted NSSAI per PLMN.

- The Configured NSSAI is configured in a UE by the HPLMN to be used in a PLMN when no PLMN-specific Accepted NSSAI is stored in the UE.

- The Accepted NSSAI is the NSSAI provided by the PLMN to the UE in registration procedures and the UE shall use this in that PLMN until the next registration from that PLMN. The Registration Accept message may include the Accepted NSSAI. The accepted NSSAI may be updated by a subsequent Registration Procedure.

If the UE has been provided a Configured or Accepted NSSAI for the selected PLMN, the UE shall include this NSSAI in RRC Connection Establishment and in NAS. The RAN routes the initial access to an AMF using the provided NSSAI.

If the UE has not yet received any Accepted NSSAI for the selected PLMN, but the UE has been provided with a Configured NSSAI for the selected PLMN, the UE may provide the Configured NSSAI or sub-set in RRC Connection Establishment and in NAS. The RAN uses the NSSAI for routing the initial access to an AMF.

If the UE does not provide any NSSAI (Accepted or Configured) for the selected PLMN in RRC Connection Establishment and in NAS, the RAN sends NAS signalling to a default AMF.

Upon successful Registration, the UE is provided with a globally unique Temporary ID by its serving AMF. The UE includes the locally unique Temporary ID in the RRC Connection Establishment during subsequent initial accesses to enable the RAN to route the NAS message to the appropriate AMF, as long as the Temp ID is valid. In addition, the serving PLMN may return the latest Accepted NSSAI of the slices permitted by the serving PLMN for the UE. The Accepted NSSAI includes the S-NSSAI values of the slices permitted by the UE's serving PLMN.

When receiving the NSSAI and a complete locally unique Temporary ID in RRC, if the RAN can reach to the AMF corresponding with the locally unique Temporary ID, then RAN forwards the request to this AMF. Otherwise, the RAN selects a suitable AMF based on the 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 provided NSSAI, then the request is sent to a default AMF.

The network operator may provision the UE with network slice selection policy (NSSP). The NSSP includes one or more NSSP rules each one associating an application with a certain S-NSSAI. A default rule which matches all applications to a S-NSSAI may also be included. When a UE application associated with a specific S-NSSAI requests data transmission, then:

- If the UE has one or more PDU sessions established with this 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.

If the UE does not have a PDU session established with this specific S-NSSAI, the UE requests a new PDU session with 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.

Editor's note: how the RAN is made aware of the network slices used by the UE is FFS.

The network, based on local policies, subscription changes and/or UE mobility, can change the set of Network Slices that is being used by a UE by providing the UE a notification of Accepted NSSAI change indicating a new value of NSSAI. This then triggers a UE initiated re-Registration procedure including in RRC and NAS Signalling the value of the new NSSAI the network has provided.

Change of set of slices used by a UE (whether UE or Network initiated) may lead to AMF change subject to operator policy.

NOTE 1: Changing the set of network slices accessible by the UE will result in termination ongoing PDU sessions with the original set of network slices if these slices are no longer used (Some slices are still retained, potentially).

Editor's note: The condition is under which the UE is able to request the change of the network slices, and what it is able to request is FFS.

During the initial Registration procedure, in case the network decides that the UE should be served by a different AMF, then the AMF that first receives the initial Registration Request shall redirect the initial 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 about the 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.

- Operator policy determines whether redirection between AMFs is allowed.

- If the network decides to redirect the UE due to NSSAI change, the network send the updated/new NSSAI to the UE using an RM procedure and an indication for the UE to initiate an Registration Update procedure with the updated/new NSSAI. The UE then initiates the Registration Update procedure with the updated/new NSSAI.

The AMF selects an SMF in a network slice instance based on S-NSSAI, DNN and other information e.g. UE subscription and local operator policies. The selected SMF establishes a PDU session based on S-NSSAI and DNN.

### 5.15.6 Network Slicing Support for Roaming

For roaming scenarios, the network slice specific network functions in VPLMN and HPLMN are selected based on the S-NSSAI provided by the UE during PDU connection establishment as following.

- If a standardized S-NSSAI is used, then selections of slice specific NF instances are done by each PLMN based on the provided S-NSSAI.

- Otherwise, the VPLMN maps the S-NSSAI of HPLMN to a S-NSSAI of VPLMN based on roaming agreement (including mapping to a default S-NSSAI of VPLMN). The selection of slice specific NF instance in VPLMN are done based on the S-NSSAI of VPLMN, and the selection of any slice specific NF instance in HPLMN are based on the S-NSSAI of HPLMN.

Editor's note: The case where the HPLMN (based on roaming agreements) configured non-standard S-NSSAI values of the VPLMN in the Configured NSSAI for that PLMN is FFS

## 5.16 Support for specific services

### 5.16.1 Public Warning System

Editor's note: This include functional description for supporting Public Warning System in 5G system.

### 5.16.2 SMS over NAS

#### 5.16.2.1 General

This section 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

- 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.

#### 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. If the core network supports SMS functionality, the AMF includes "SMS supported" indication to the UE.

SMS is transported over NAS without the need to establish data radio bearers, via NAS transport message, which can carry SMS messages as payload.

Editor's note: How to transport SMS payload between UE and AMF depends on the overall NAS transport protocol stack and that is FFS.

### 5.16.3 IMS support

Editor's note: This could include functional description for supporting IMS based services such as voice.

#### 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].

#### 5.16.3.2 IMS voice over PS Session Supported Indication

The serving PLMN AMF shall send an indication toward the UE during the Registration procedure if an IMS voice over PS session is supported. The serving PLMN AMF uses this indicator to indicate to the UE whether it can expect a successful IMS voice over PS session with a 5G QoS Flow that supports voice as specified in clause 5.7. A UE with "IMS voice over PS" voice capability should take this indication into account when establishing voice over PS sessions.

The serving PLMN provides this indication based e.g. on local policy, HPLMN and how extended 5G-RAN coverage is. The serving PLMN shall indicate to the UE that the UE can expect a successful IMS voice over PS session only if the AMF has the knowledge that the serving PLMN has a roaming agreement for IMS voice with the HPLMN of the UE. This indication is per Registration Area list.

Editor's note: Interactions between the AMF and UDM for T-ADS, if required, including, support for "homogenous support for IMS voice over PS Session supported indication" are FFS.

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.

#### 5.16.3.3 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".

### 5.16.4 Emergency services

Editor's note: This could include functional description for supporting emergency services in 5G system, including support for unauthenticated emergency services.

- IMS emergency service is supported with emergency PDU session service by establishing a PDU session with an Emergency APN (or DNN).

- UE determines whether the serving network support IMS emergency service support for UE in limited service state, as specified in TS 23.122 [17], is based on Access Stratum broadcast indication.

- A serving network shall provide an Access Stratum broadcast indication to UEs as to whether eCall Over IMS is supported.

### 5.16.5 Multimedia Priority Services

Editor's note: This include functional description for supporting Multimedia Priority Services.

## 5.17 Interworking and Migration

Editor's note: This could include functional description for interworking with EPS, 2G, 3G and support for migration towards 5G system.

### 5.17.1 Support for Migration from EPC to 5GC

#### 5.17.1.1 General

This section 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 24.201 [x]) 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 UDM in case of 5GC.

Editor's note: The functionality of the common subscriber database will be defined based on the interworking procedures.



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 NGC or NR towards NGC;

- 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: A UE supporting EPC NAS 5GC NAS initiates NGC NAS procedures when 5GC is supported by the serving PLMN.

Editor's note: The final names for "E-UTRAN that connects to NGC" and NR are FFS and depend on the discussion in RAN.

Editor's note: The final names for 5GC is FFS.

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.xxx [xx] 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: 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

### 5.17.2 Interworking with EPC

#### 5.17.2.1 General

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). Similarly, the network maintains one state either in the AMF or in the MME. UE maintains a single coordinated registrationfor 5GC and EPC.

- In dual-registration mode, UE can handle independent registrations for 5GC and EPC. In this mode, the UE may be registered to 5GC only, EPC only, or to both 5GC and EPC.

Editor's note: It is FFS which mode is mandatory for the UE and the network, and how to converge on one mode.

UE during initial NGC registration procedures provides its support of single-registration and/or dual-registration mode. The network selects one of the two modes, based on UE capabilities, network capabilities and operator policies, and provides the selected mode to the UE in the registration response message. This mode is valid in the UE's 5GC registration area and maybe updated by the network during subsequent registration procedure.

Editor's note: It is FFS if such an indication is also needed in EPC/E-UTRAN.

#### 5.17.2.2 Mobility in single-registration mode

To support mobility in single-registration mode, the Nx interface between AMF in 5GC and MME is optional, but it is required if seamless session continuity for voice is needed.

If Nx is supported:

- For idle-mode mobility from 5GC to EPC, the UE performs TAU procedure with 4G-GUTI mapped from 5G-GUTI and the MME retrieves the UE's MM and SM context from 5GC. For connected-mode mobility from 5GC to EPC, inter-system handover is performed.

- For idle-mode mobility from EPC to 5GC, the UE performs registration procedure with 5G-GUTI mapped from 4G-GUTI and the AMF and SMF retrieve the UE's MM and SM context from EPC. For connected-mode mobility from EPC to 5GC, inter-system handover is performed.

Editor's note: Description for single registration mode based interworking with no Nx support is FFS.

#### 5.17.2.3 Mobility in dual-registration mode

To support mobility in dual-registration mode, the support of Nx interface between AMF in 5GC and MME in EPC is not required.

Editor's note: It is FFS if dual-registration mode can be used for IMS voice.

During inter-system mobility from 5GC to EPC, the UE performs Attach in EPC with "handover" indication in PDN Connection Request message (TS 23.401, clause 5.3.2.1) and it subsequently moves all its other PDU session using the UE initiated PDN connection establishment procedure with "handover" flag (TS 23.401 clause 5.10.2). The UE does not continue to perform registrations in NGC and remains registered without PDU sessions in 5GC till its registrations in 5GC times out and the network performs implicit detach.

During inter-system mobility from EPC to NGC, the UE performs Registration in 5GC and it subsequently moves all its PDN connections from EPC using the UE initiated PDU session establishment procedure with "handover" flag (TS 23.502 [3], clause 4.3.2.2.1). The UE does not continue to perform TAU in EPC and remains attached without PDN connections in EPC till the network performs implicit detach. If the UE does not support attach without PDN connections in EPC, the UE is detached in EPC when the last PDN Connection is moved to 5GC

Editor's note: Support of "handover" flag in TS 23.502 [3] is not yet defined.

## 5.18 Network Sharing

Editor's note: Place holder for Network sharing. Relation between network slicing could network sharing should be clarified.

## 5.19 Control Plane Congestion and Overload Control

Editor's note: Description for congestion and overload control in 5G System.

## 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.

Editor's note: Additional network capability categories can be defined during the normative work.

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 is comprised of means that allow the identification of the 5G network function responsible for adopting the provisioning information from the external party, receive the provisioning information, and use the provisioning information for the UE. Provisioning capability can be used for the mobility management and session management of the UE. For the mobility management of the UE, Mobility Pattern can be provisioned. For the session management of the UE, communication pattern can be provisioned such as periodic communication time, communication duration time, and scheduled communication time.

Editor's note: It is FFS to provision how long response time from an application server can be supported when a UE is in MICO mode.

Editor's note: It is FFS to provision information in order to support routing change (e.g., Break-out) of selected traffic to application(s) in a local data network, based on clause 8.4 in the TR 23.799 .

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.

Editor's note: The external exposure functionality needs to inherit from the service and capability exposure functionality defined in TS 23.682 .

## 5.21 xxxx

Editor's note: Place holder for features that are not covered in the sections above.

# 6 Network Functions

Editor's note: This should include Network functions, functionalities and NF selection functionality, etc.

## 6.1 General

## 6.2 Network Function Functional description

Editor's note: This should include various network functions in the architecture, features and functionalities supported.

### 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 a 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).

- Transparent proxy for routing SM messages.

- Access Authentication.

- Access Authorization.

- Security Anchor Function (SEA). 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 SEA that it uses to derive access-network specific keys.

NOTE: 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.

Editor's note: When there is an update to security architecture defined by SA WG3, security functionality mapping to the overall architecture will be updated.

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.

Editor's note: The definition which 3GPP information and procedures are not applicable to N3GPP-access and those N3GPP access specific information and procedure needs to be considered are FFS.

- 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.

Editor's note: The definition which NAS signalling procedures are not applicable to N3GPP-access and those N3GPP access specific information and procedure needs to be considered are FFS.

- Support of authentication of UEs connected over N3IWF.

- Management of mobility and authentication/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: Not all of the functionalities are required to be supported in an instance of a network slice.

### 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 (incl optional Authorization).

- Selection and control of UP function.

- Configures traffic steering at UPF to route traffic to proper destination.

- Termination of interfaces towards Policy control functions.

- Control part of policy enforcement and QoS.

- Lawful intercept (for SM events and interface to LI System).

- 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 (for IP type PDU 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.

Editor's note: when there is an update to security architecture defined by SA WG3, security functionality mapping to the overall architecture will be updated.

### 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.

- Packet inspection and User plane part of Policy rule enforcement.

- Lawful intercept (UP collection).

- Traffic usage reporting.

- Uplink classifier to support routing traffic flows to a data network.

- Branching point to support multi-homed PDU session.

- QoS handling for user plane, e.g. packet filtering, gating, UL/DL rate enforcement

- 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.

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 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.

- Implements a Front End to access subscription information relevant for policy decisions in a User Data Repository (UDR).

### 6.2.5 NEF

The Network Exposure Function (NEF) supports the following functionality:

- It provides a means to securely expose the services and capabilities provided by 3GPP network functions for e.g 3rd party, internal exposure/re-exposure, Application Functions, Edge Computing as described in section 5.13.

- The Network Exposure Function receives information from other network functions (based on exposed capabilities of other network functions). It may store the received information as structured data using a standardized interface to a data storage network function (interface to be defined by 3GPP). The stored information can be "re-exposed" by the NEF to other network functions and Application Functions, and used for other purposes such as analytics.

Editor's note: Bullet above needs to be reflected in the figure.

### 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.

NOTE: Whether NRF is an enhancement of DNS server is to be determined during Stage 3.

Editor's note: Whether NRF is used only for NF instance discovery or both NF discovery and selection is FFS.

Editor's note: Whether Network repository function (NRF) is an enhancement of DNS server will be determined by CT WGs.

### 6.2.7 UDM

The Unified Data Management (UDM) supports the following functionality:

- Supports Authentication Credential Repository and Processing Function (ARPF). This function stores the long-term security credentials used in authentication for AKA.

- Stores Subscription information.

NOTE 1: UDR (User data repository) could be present within the UDM.

NOTE 2: The interaction between UDM and HSS is implementation specific.

### 6.2.8 AUSF

The AUSF supports the following functionality:

- Supports Authentication Server Function (AUSF) as specified by SA WG3.

Editor's note: when there is an update to security architecture defined by SA WG3, security functionality mapping to the overall architecture will be updated.

### 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.

Editor's note: How and whether N3IWF allocates N3IWF IP address(es) and/or UE IP address(es) for control-plane and/or user-plane IPSec tunnels is FFS.

- 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.

- Supporting AMF selection.

Editor's note: How QoS is supported via N3IWF and over untrusted non-3GPP accesses is FFS.

Editor's note: Whether ePDG selection procedure defined in TS 23.402 is applicable as N3IWF discovery procedure is FFS.

### 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 section 5.6.7),

- Accessing Network Capability Exposure (see section 5.13),

- Interact with the Policy framework for policy control (see section 5.14),

Editor's note: Other functions to be added are FFS.

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 SDSF

The SDSF is an optional function that supports the following functionality:

- Storage and retrieval of information as structured data by the NEF.

NOTE 1: Deployments can choose to collocate SDSF with other NFs (e.g. UDR, 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 1: Deployments can choose to collocate UDSF with other NFs (e.g. SDSF).

## 6.3 Network function discovery and selection

### 6.3.1 General

The NF discovery enables one NF discover a specific target NF type.

Unless the expected NF information is locally configured on requester NF, e.g. the expected NF is in the same PLMN the NF discovery is implemented via the NRF. The NF repository function (NRF) is the logical function that is used to supports the functionality of NF discovery.

Editor's note: It is FFS how to identify the NRF in remote PLMN.

In order to access to a requested type NF and no associated NF(s) stored on the requester NF, the requester NF initiates the NF discovery by providing the type of the NF (e.g. SMF, PCF) and other service parameters e.g. slicing related information to discover the target NF. The detail service parameter(s) used for specific NF discovery refer to the related NF discovery and selection clause.

The NRF provides the IP address or the FQDN of NF instance(s) to the requester NF for target NF instance selection. Based on that information, the requester NF can select one NF instance.

For NF discovery across PLMNs, the requester NF provides the NRF the PLMN ID of the target NF. The Local PLMN interacts with the NRF in the target PLMN to retrieve the IP address or the FQDN of the target NF instance (s).

### 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.

Editor's note: Further detailing of the cases where SMF selection is not using NRF is FFS.

Editor's note: Whether the Network repository function (NRF) is an enhancement of DNS server will be determined by CT WGs. A proper reference will be added once this is available in stage 3.

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. whether local breakout may apply to the session.

- Local operator policies.

- Load conditions of the candidate SMFs.

Editor's note: It is FFS what other information may be considered for SMF selection. It is also FFS what parts of S-NSSAI is considered, e.g. whether both SST and ST is used or only SST.

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.

Editor's note: It is FFS if there are conditions under which the same SMF need to be selected for PDU Session to the same DNN and slice.

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 DN subscription context that allows for handling the PDU Session in the visited PLMN (i.e. using LBO) for this DNN 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 network slice, 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 is used to derive an SMF identity from the HPLMN.

Editor's note: Impact on SMF selection for handovers between 3GPP and non-3GPP access is FFS

Editor's note: Impact on SMF selection due to interworking with EPC is FFS

### 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.

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 non-IP Type).

- SSC mode selected for the PDU session.

- UE subscription profile in UDM.

- Routing destination of traffic (e.g. application location).

Editor's note: Aspects related to service area are FFS.

- Local operator policies.

- Network slicing related information.

### 6.3.4 AUSF selection function

The AMF performs AUSF selection to allocate an AUSF that performs authentication b/w 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

Editor's note: Further detailing of the cases where AUSF selection is not using NRF is FFS.

Editor's note: Whether the Network repository function (NRF) is an enhancement of DNS server will be determined by CT WGs. A proper reference will be added once this is available in stage 3.

Editor's note: How to handle AUSF selection in the roaming situation is FFS.

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.

Editor's note: when the security architecture is defined by SA WG3, the selection criteria will be updated.

## 6.3.x <NF name> selection

Editor's note: This should include individual network function selection.

# 7 Network Function Services and descriptions

## 7.1 Network Function Service Framework

## 7.1.1 General

Editor's note: General procedures that apply to all services provided network functions.

A NF service is one type of capability exposed by a NF (NF Service Producer) to other NF (NF Service Consumer) through a service-based interface.

There are two mechanisms that NFs provide their services through a service-based interface:

- "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 can include performing an action and/or providing information. NF\_B response provides NF service results based on the information provided by NF\_A in its request. 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 7.1.1-a: "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 from consumer may include notification request for periodic updates or notification triggered through certain events (e.g., the information requested gets changed, reaches certain threshold etc.). This mechanism also covers the case where NFs (NF\_B) are subscribed to certain notifications implicitly without explicit subscription request (e.g. due to successful registration procedure).

Editor's note: Whether Notify without Subscribe is treated as a separate mechanism is FFS.



Figure 7.1.1-b: "Subscribe-Notify" NF Service illustration

NF Service discovery, authorization and registration are framework mechanisms that enable the use of NF services.

### 7.1.2 Network Function Service discovery

The network function (NF) within the core network may expose its capability as service via its service based interface, which can be re-used by other CN NFs.

The NF service discovery enables the CN NF to discover a specific target NF instance which provides the expected NF service(s).The NF service discovery is implemented via the NF discovery. The NF discovery enables the service requester NF to discover the service provider NF instance and access the NF service provided by the service provider NF. For more detail NF discovery refer to clause 6.3.1.

### 7.1.3 Network Function Service authorization

NF service authorization ensures the service requester NF is authorized to access the NF service provided by the service provider NF, according to e.g. the policy of NF, the policy from the serving operator, the inter-operator agreement.

Service authorization information is one of the components in the profile of the NF. It includes the NF type (s) which is allowed to interconnect with this NF and the corresponding NF service (s) which can be accessed by those NF type(s).

The Service authorization entails two steps:

- Check whether the requester NF is permitted to discover the requested NF instance during the NF service discovery procedure. This is per NF granularity.

Editor's note: It is FFS whether this function on NRF is needed.

- Check whether the requester NF is permitted to access the requested NF for consuming the NF service. This is either be per NF or per UE granularity. NF Service authorization per UE granularity is embedded in the related NF service logic.

NOTE: The security of the connection between service request and service provider is specified in SA WG3.

### 7.1.4 Network Function Service registration and de-registration

NF Service Registration and NF Service de-registration is defined in TS ab.cde.

Editor's note: This is to be confirmed with SA5.

## 7.2 Network Function Services

Editor's note: This should include common services that can be supported, exposed by control plane network functions with service based interface.

### 7.2.1 General

Editor's note: The NF services introduced in this section is non-exhaustive and will be added with more services are identified during the normative phase.

This section provides 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
| UE location reporting | UE location is reported by the AMF |  | NEF | Subscribe-Notify |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

### 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] | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

## 7.3 Network Internal Exposure

Editor's note: This should include description on how network internal exposure is supported (with or without NEF) using the necessary service framework function (s). This is meant to show how service framework functions in 7.1 and 7.2 are used for network internal exposure but avoid duplication with 7.1 and 7.2. This is not meant to describe on a per NF basis (for the list as in 7.2) rather meant as a general description.

## 7.4 External Exposure

Editor's note: This should include description on how external exposure is supported with NEF using the necessary service framework function(s). This is meant to show how service framework functions in 7.1 and 7.2 are used for external exposure but avoid duplication with 7.1 and 7.2. This is not meant to describe on a per NF basis (for the list as in 7.2) rather meant as a general description.

# 8 Control and User plane Protocol Stacks

Editor's note: This is a place holder to include control and user plane protocol stacks if there is a need to capture the same in stage 2 specification (similar content as TS 23.401 clause 5.1 expected). Need for this section is FFS.

## 8.1 General

## 8.2 Control plane Protocol stacks

### 8.2.x Control Plane for untrusted non 3GPP Access



**Legend:**

- N2 Application Protocol (N2-AP): Application Layer Protocol between the N3IWF and the AMF.

- N12 Application Protocol (N12-AP): Application Layer Protocol between the AMF and the AUSF.

- The N3IWF creates a NAS Attach Request message on behalf of the UE and send this message over N2 to AMF

Figure 8.2.x-1: Control Plane for initial part of attach procedure via N3IWF

Editor's note: The need for NAS layer between N3IWF and AMF is FFS.



**Legend:**

- N2 Application Protocol (N2-AP): Application Layer Protocol between the N3IWF and the AMF.

- IPsec transport mode and GRE is used to encapsulate NAS payload between UE and N3IWF.

Figure 8.2.x-2: Control Plane for NAS when CP IPsec SA is established

Editor's note: It is FFS whether GRE encapsulation of NAS is needed or not.



**Legend:**

- N2 Application Protocol (N2-AP): Application Layer Protocol between the N3IWF and the AMF.

- IKEv2 is used to establish the Child SA between UE and N3IWF for each PDU session.

Figure 8.2.x-3: Control Plane for user plane establishment via N3IWF

Editor's note: The name of N2-AP and the protocol stack for N2 should be confirmed with RAN3.

Editor's note: The name of N12-AP and the protocol stack for N12 is FFS.

## 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.



Figure 8.3.1-1: User Plane Protocol Stack

**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….

- **5G Encapsulation**: This layer supports multiplexing traffic of different PDU sessions (possibly corresponding to different PDU session Types) over N3 (i.e. between AN and 5G Core) or over N9 (i.e. between different UPF of the 5G Core). 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

Editor's note: The details of encapsulation header should be updated according to the protocol chose/defined in stage 3.

- **AN protocol stack**: This set of protocols/layers depends on the AN

- When the AN is a 3GPP RAN, these protocols/layers are defined by the 3GPP RAN

Editor's note: The details of RAN protocol stacks depend on the decision of RAN WG and will be updated later.

- 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 AN protocol stack is defined in clause 8.3.3.

- **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.. For the IP type PDU session, the UPF acting as PDU session anchor is the IP anchor point of the IP address/prefix allocated to the UE.

NOTE 2: The "non PDU anchor session" 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



**Legend:**

- PDU Layer: As defined in Figure 8.3.1-1

- 5G UP Encapsulation: This protocol tunnels user data between N3IWF and the UPF. This tunnel is per PDU session.

- The N3IWF relays the user data between per PDU session IPsec tunnel over NWu and corresponding N3 tunnel.

-

Figure 8.3.2-1: User plane via N3IWF

Editor's note: The protocol stack for N3 is FFS and should be confirmed with RAN WG3.

Annex A (informative):  
Policy framework

Editor's note: This annex is being used to develop the technical content and then moved as and where appropriate to TS 23.501 , TS 23.502 [3] and TS 23.203 [4]. The Annex will not be maintained and voided when normative content has been prepared and efforts to be made to do so before the specification reaches version 2.0.0 to avoid having VOID Annex.

# A.1 High level architectural requirements

The policy framework shall provide the relevant parts of the PCC framework as specified in TS 23.203 [4], including:

a. Policy Control Function (PCF) shall support interfaces to the Policy and Charging Enforcement Function (PCEF), Network Exposure Function (NEF), the Application Function (AF), and the Online Charging System (OCS).

b. The PCF shall be able to evaluate operator policies that are triggered by events received from the PCEF, NEF, the AF, and the OCS.

c. The PCF shall provide Rules for application and service data flow detection, gating, QoS and flow based charging to the PCEF.

d. The Policy Framework shall be able to manage the Packet Filter Descriptions (PFDs) in the PCEF by the 3rd party AS via the NEF and PFDF.

e. The Policy Framework shall support to negotiate the background data transfer policy with the 3rd party AS via the NEF.

f. The PCF shall implement a Front End to access subscription information relevant for policy decisions in a User Data Repository (UDR) including dynamic profile updates pushed by the UDR.

g. Traffic Steering Control for steering traffic for the services on the DN side of the N6 reference point,

h. The PCF shall be able to take input from Network Data Analytics (NWDA) into consideration for policies on assignment of network resources and for traffic steering policies.

NOTE 1: The existing PCC framework is applicable to PDU sessions of IP Type only.

Editor's note: How the PCC framework applies to PDU sessions other than IP Type is FFS. Also, where IP-CAN is used, may need to update per 5G terminology.

Additionally, the policy framework shall provide following functionality for the access and mobility enforcement:

a. Policy Control Function (PCF) shall support the interface to the Access and Mobility Policy Enforcement Function (AMPEF).

b. The PCF shall be able to provide Access and Mobility Management related policies to the AMPEF.

c. The PCF shall be able to evaluate operator policies that are triggered by events received from the AMPEF.

Editor's note: How to enforce the access and mobility policy when interfacing with PCF is FFS.

Editor's note: The list above covers the high level requirements that are addressed in the document so far. Additional requirements are to be added when the related information is agreed. Mapping of PCEF and AMPEF into 5G CN entities are FFS.

# A.2 Architecture model and reference points

## A.2.1 Reference architecture

The policy framework functionality is comprised by the functions of the Policy Control Function (PCF), the Policy Control Enforcement Function (PCEF), the Access and Mobility Policy Enforcement Function (AMPEF), the Online Charging System (OCS) and the Application Function (AF).

Figure A.2.1-1 shows the policy framework architecture (non-roaming) in 5G:



Figure A.2.1-1: Overall non-roaming 5G Policy framework architecture

Editor's note: The reference point PUd and PSy are not yet defined in the baseline 5G architecture and the actual name is expected to change.

Editor's note: Implications from multiple Slices and its relation to PCF are FFS.

Figure A.2.1-2 shows the roaming policy framework architecture (local breakout scenario with AF in VPLMN) in 5G:



Figure A.2.1-2: Overall roaming policy framework architecture - local breakout scenario with AF in VPLMN

Figure A.2.1-3 shows the roaming policy framework architecture (local breakout scenario with AF in HPLMN) in 5G:



Figure A.2.1-3: Overall roaming policy framework architecture - local breakout scenario with AF in HPLMN

Editor's note: The need for this roaming scenario with local breakout and AF in HPLMN is FFS. Resolution of this editor's note also depends on feedback from GSMA.

Figure A.2.1-4 shows the roaming policy framework architecture (home routed scenario) in 5G:



Figure A.2.1-4: Overall roaming policy framework architecture - home routed scenario

## A.2.2 Reference points

### A.2.2.1 N5 reference point

The N5 reference point resides between the AF and the PCF.

The N5 reference point enables transport of application level session information from AF to PCF.

The N5 reference point enables the AF to get information about IP-CAN session events.

### A.2.2.2 N7 reference point

The N7 reference point resides between the PCEF and the PCF.

The N7 reference point enables the PCF to have dynamic policy and charging control at a PCEF.

The N7 reference point enables the signalling of policy and charging decision and it supports the following functions:

- Establishment of IP-CAN session by the PCEF;

- Request for policy and charging control decision from the PCEF to the PCF;

- Provision of policy and charging control decision from the PCF to the PCEF;

- Delivery of network events and IP-CAN session parameters from the PCEF to the PCF;

- Termination of IP-CAN session by the PCEF or the PCF.

### A.2.2.3 N15 reference point

The N15 reference point resides between the AMPEF and the PCF.

The N15 reference point enables the PCF to provide Access and Mobility Management related policies to the AMPEF and it supports the following functions:

- Handling of UE Context Establishment request sent by the AMPEF to the PCF as part of UE Registration procedure(s);

- Provision of access and mobility management decision from the PCF to the AMPEF;

- Delivery of network events from the AMPEF to the PCF;

- Handling of UE Context Termination request sent by the AMPEF to the PCF as part of UE De-Registration procedure.

### A.2.2.4 N7r reference point

The N7r reference point resides between a PCF in the HPLMN (H-PCF) and a PCF in the VPLMN (V-PCF).

For roaming scenario, the N7r enables the H-PCF to:

- Provision mobility policy rules to V-PCF in the VPLMN;

- Handling of UE Context Establishment request sent by the V-PCF as part of UE Registration procedure(s);

- Receipt of network events from the V-PCF;

- Handling of UE Context Termination request sent by V-PCF as part of UE De-Registration procedure.

### A.2.2.5 PUd reference point

The PUd reference point resides between the UDR and the PCF, acting as an Application Front End in a layered architecture as defined in TS 23.335 on User Data Convergence.

The PUd reference point enables the PCF to access policy control related subscription data stored in the UDR. The PUd interface supports the following functions:

- Request for policy control related subscription information from the UDR

- Provisioning of policy control related information to the UDR

- Notifications from the UDR on changes in the subscription information

Editor's note: The difference between Ud in TS 23.335 and PUd are FFS.

### A.2.2.6 N23 reference point

The N23 reference point resides between the Network Data Analytics (NWDA) and the PCF. The N23 reference point, enables the PCF to subscribe to and be notified on network status analytics e.g. congestion information for a specific slice. NWDA provides slice specific network data analytics. The subscription to NWDA by PCF therefore is on a network slice level and the NWDA is not required to know about the current subscribers using the slice. NWDA notifies / publishes slice specific network status analytic information to the PCF(s) that are subscribed to it. This information is not subscriber specific. PCF uses that data in its policy decisions. The PCF, the slice and NWDA in question are always in the serving network.

NOTE: NWDA functionality beyond its support for N23 is out of scope of 3GPP.

Editor's note: The actual parameter notified to the PCF is FFS.

Editor's note: Applicability of slicing in PCF architecture is FFS.

# A.3 Functional description

## A.3.1 Overall description

The Policy framework architecture provides the functions for:

- application and service data flow detection,

- QoS and gating control,

- Credit management,

- Flow based charging,

- Background data transfer policy negotiation,

- Management of the PFDs in the PCEF by the 3rd party AS,

- Traffic Steering Control for steering traffic for the services on the DN side of the N6 reference point,

- Provide a Front End to subscription information relevant for policy decisions in a User Data Repository,

- Provide Network selection and Mobility Management related policies (e.g. RFSP index) to the Access and Mobility Management,

Editor's note: Further work is required to include the different aspects of the Policy framework architecture.

The PCF evaluates operator policies that are triggered by events received from the Application Function, the Session Management, Mobility Management and the Online Charging System as well as Changes in User Profile.

For policy control, the AF interacts with the PCF and the PCF interacts with the PCEF as instructed by the AF as specified in TS 23.203 [4].

Editor's note: Further work would be required to cover details of these aspects.

NOTE 1: Credit management and reporting are defined in SA WG5 specification.

NOTE 2: The policy control framework for phase 1 does not preclude potential extensions in phase 2 for policy control in multiple administrative areas.

### A.3.1.1 UE Access and Mobility Management Control

UE Access and Mobility Management control comprises policy rules for the UE Access and Mobility Management e.g. the provisioning of information about allowed areas for the UE.

### A.3.1.2 Roaming impacts to Policy

For a subscriber roaming in a visited PLMN, the visited PLMN shall be able to receive the subscriber's policy rules, including (not exhaustive):

- Mobility policies e.g. RFSP index.

In the case of local breakout, an interface (N7r) is supported between the visited V-PCF and H-PCF for providing mobility policy rules from HPLMN to VPLMN.

Editor's note: It is FFS whether session management policy rules on the roaming interface is needed.

Editor's note: Whether other types of policy rules, apart from the above list need to be provided by PCF is FFS.

### A.3.1.3 UE Policy

#### A.3.1.3.1 General

The 5G core network shall be able to provide policy information from the PCF to the UE. Such policy information includes:

1) Access network discovery & selection policy: It is used by the UE for selecting non-3GPP accesses and for deciding how to route traffic between the selected 3GPP and non-3GPP accesses. The structure and the content of this policy are specified in clause A.3.1.3.2.

2) Route Selection Policies: These policies are used by the UE to determine how to route outgoing traffic. Traffic can be routed to an established PDU session, can be offloaded to non-3GPP access outside a PDU session, or can trigger the establishment of a new PDU session. The following policies are used for route selection:

2a) SSC Mode Selection Policy (SSCMSP): This policy is used by the UE to associate UE applications with SSC modes and to determine the PDU session which this traffic should be routed to. It is also used to determine when a new PDU session should be requested with a new SSC mode.

2b) Network Slice Selection Policy (NSSP): This policy is used by the UE to associate UE applications with SM-NSSAIs and to determine the PDU session which this traffic should be routed to. It is also used to determine when a new PDU session should be requested with a new SM-NSSAI..

2c) DNN Selection Policy: This policy is used by the UE to associate UE traffic with one or more DNNs and to determine the PDU session which this traffic should be routed to. It is also used to determine when a PDU session should be requested to a new DNN. It may also indicate the access type (3GPP or non-3GPP) on which a PDU session to a certain DNN should be requested.

2d) Non-seamless Offload Policy: This policy is used by the UE to determine which traffic should be non-seamlessly offloaded to non-3GPP access (i.e. outside of a PDU session).

Editor's note: It is FFS if the Route Selection Policies will be defined separately or if they could be grouped into a single policy. Clause A.3.1.3.3 shows an example of how these policies could be grouped.

The SSCMSP and NSSP shall be provided from the PCF to the UE via the N1 interface.

Editor's note: It is FFS regarding PCF interactions and if the SSCMSP and the NSSP policies are transported via SMF and AMF or AMF only.

Editor's note: It is FFS if the size of the policy rules to be transferred and frequency of the rules update from the PCF to the UE would require additional transport options.

Editor's note: It is FFS if part of the policies can be transferred via UDM.

Editor's note: Whether the information for Local Area Data Network described in clause 5.6.5 is included as UE Policy Provisioning or not is FFS.

#### A.3.1.3.2 Access network discovery & selection policy

Editor's note: The details of the access network discovery & selection policy if FFS. It is also FFS if any of the access network discovery & selection policies specified in TS 23.402 clause 4.8 can be reused.

#### A.3.1.3.3 Grouping the Route Selection Policies

This clause shows an example of how the Route Selection Policies (defined in clause A.3.1.3.1) could be grouped into a single policy called UE Route Selection Policy (URSP). The URSP includes a prioritized list of URSP rules, each one composed of the following components:

- Traffic filter: Information that can be compared against data traffic and determine if the rule is applicable to this data traffic or not. It may include application identifiers and other information, if needed. The traffic that matches the traffic filter of a URSP rule is referred to as the "matching traffic" for this URSP rule.

- Non-seamless offload: Indicates if the matching traffic is Prohibited, Preferred or Permitted (i.e. allowed but not preferred) to be offloaded to non-3GPP access outside of a PDU session. It may also indicate a specific non-3GPP access type (e.g. WLAN, SSID-x) on which the matching traffic is Prohibited, Preferred or Permitted.

- Slice Info: This includes the S-NSSAI (see clause 5.15) required for the matching traffic. It may also include multiple S-NSSAIs in priority order if the matching traffic may be transferred over a PDU session supporting any of these S-NSSAIs. It is used to associate the matching traffic with one or more S-NSSAIs.

- Continuity Types: This includes the SSC Mode (see clause 5.6.9.2) required for the matching traffic. It may also include multiple SSC Modes in priority order if the matching traffic may be transferred over a PDU session supporting any of these SSC Modes. It is used to associate the matching traffic with one or more SSC modes.

- DNNs: This includes the DNN required for the matching traffic. It may also include multiple DNNs in priority order if the matching traffic may be transferred over a PDU session to any of these DNNs. It is used to associate the matching traffic with one or more DNNs.

- Access Type: If the UE needs to establish a PDU session for the matching traffic, this indicates the type of access (3GPP or non-3GPP) on which the PDU session should be established. It may also indicate a prioritized list of accesses on which the PDU session establishment should be attempted.

Each URSP rule shall include a traffic filter and one or more of the other components, which specify how the matching traffic should be routed.

As an example, the URSP provisioned in the UE may include the following rules:

Table A.3.1.3.3-1: Example of URSP rules

|  |  |
| --- | --- |
| Example URSP rule | Comments |
| Traffic filter: App=DummyApp  Direct offload: Prohibited  Slice Info: S-NSSAI-a  Continuity Types: SSC Mode 3  DNNs: internet  Access Type: 3GPP access | This URSP rule associates the traffic of application "DummyApp" with S-NSSAI-a, SSC Mode 3 and the "internet" DNN.  It enforces the following routing policy:  Traffic of application "DummyApp" should not be directly offloaded to non-3GPP. It should be transferred on a PDU session supporting S-NSSAI-a, SSC Mode 3 and DNN=internet. If this PDU session is not established, the UE shall attempt to establish the PDU session over Access Type=3GPP access. If the PDU session cannot be established, the traffic of this application cannot be transferred. |
| Traffic filter: App=App1, App2  Direct offload: Permitted  Slice Info: S-NSSAI-a  Access Type: Non-3GPP access | This URSP rule associates the traffic of applications "App1" and "App2" with S-NSSAI-a.  It enforces the following routing policy:  The traffic of application App1 and the traffic of application App2 should be transferred on a PDU session supporting S-NSSAI-a. If this PDU session is not established, the UE shall attempt to establish the PDU session over Access Type=non-3GPP access. If the PDU session cannot be established, the traffic of these applications can be directly offloaded to non-3GPP access. |
| Traffic filter: App=DummyApp  Direct offload: Permitted (WLAN SSID-a)  Continuity Types: SSC Mode 3 | This URSP rule associates the traffic of application "DummyApp" with SSC Mode 3.  It enforces the following routing policy:  The traffic of application "DummyApp" should be transferred on a PDU session supporting SSC Mode 3. If this PDU session is not established, the UE shall attempt to establish the PDU session over any access type. If the PDU session cannot be established, the traffic can be directly offloaded if the UE is connected to WLAN with SSID-a. |
| Traffic filter: \*  Direct offload: Preferred  Slice Info: S-NSSAI-a, S-NSSAI-b  Continuity type: Type-3  DNN: internet | This (default) URSP rule associates all traffic not matching any prior rule with S-NSSAI-a (first priority), S-NSSAI-b (second priority), SSC Mode 3 and the "internet" DNN.  It enforces the following routing policy:  All traffic not matching any prior rule should preferably be offloaded directly to any non-3GPP access. If it cannot be directly offloaded to non-3GPP access, it should be transferred on a PDU session supporting S-NSSAI-a, SSC Mode 3 and DNN=internet. Alternatively, it can be transferred on a PDU session supporting S-NSSAI-b, SSC Mode 3 and DNN=internet. The PDU sessions can be established over any access type. |

If a UE application requests a specific SSC Mode, S-NSSAI and/or DNN, the traffic of this application shall be routed to a PDU session that supports the requested SSC Mode, S-NSSAI and DNN. The SSC Mode, S-NSSAI and DNN requested by the UE application shall take precedence over the corresponding values in the URSP rules.

Editor's note: It is FFS if a VPLMN can provide its own URSP rules to a roaming UE. It is also FFS how the UE selects the URSP rules to apply if it is provisioned with VPLMN URSP and HPLMN URSP.

Editor's note: It is FFS if/how the URSP can be applied in case of multi-homed PDU sessions and in case of multiple PDU sessions to the same DNN.

Editor's note: It is FFS if/how a UE application can be prevented from using a specific PDU session.

### A.3.1.4 Policy Control Subscription information management

The PCF may request subscription information from the UDR at establishment, modification, or termination of a PDU-CAN session, and at UE Context Establishment or termination.

The PCF may provision policy control related information to the UDR.

The PCF may receive notifications from the UDR on changes in the subscription information. Upon reception of a notification, the PCF shall make the policy control decisions necessary to accommodate the change in the subscription and shall update the PCEF and/or the AMPEF if needed.

The UDR may provide the following subscription profile information:

- Subscriber's allowed services;

- Information on subscriber's allowed QoS;

- Subscriber's charging related information;

- Subscriber category;

- Subscriber's usage monitoring related information;

- MPS EPS Priority, MPS Priority Level, and IMS Signalling Priority;

- Subscriber's profile configuration indicating whether application detection and control can be enabled.

- Spending limits profile information;

- Sponsored data connectivity profiles;

- Service area restrictions;

- RAT Frequency Selection Priority (RFSP) information.

Editor's note: The list above covers subscription profile information for policy control functionality that is addressed in the document so far. Additional policy-related subscription data is to be added when the related functionality is agreed.

Annex B (informative):  
Location Services temporary placeholder

Editor's note: This is placeholder for changes to Location Service for 5G System It is expected that eventually the Location Service Architecture for 5G will be defined in TS 23.271 .

# B.1 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].

GMLC Gateway Mobile Location Centre

HGMLC Home GMLC

LMF Location Management Function

LRF Location Retrieval Function

VGMLC Visited GMLC

# B.2 Non-Roaming Reference Architecture

Figure Y.2-1 shows architectural support for location services for non-roaming scenarios using a point to point (P2P) reference point representation.

Editor's note: The architecture for the service based representation is FFS.

Only entities directly relevant to location services are shown.



Figure B.2-1: Non-roaming reference architecture for Location Services

Editor's note: It is FFS whether the NGLs reference point includes the GMLC or AMF

# B.3 Roaming Reference Architecture

Figures B.3-1 shows the architectural support for location services for roaming scenarios using a point to point (P2P) reference point representation.

Editor's note: The architecture for the service based representation is FFS.

Only entities directly relevant to location services are shown.



Figure B.3-1: Roaming reference architecture for Location Services

Editor's note: It is FFS whether the NGLs reference point includes the GMLC or AMF.

# B.4 Reference Points

The following reference points are defined for location services.

**NGLh:** Reference point between a GMLC and the HSS.

**NGLg:** Reference point between a GMLC and either an AMF or LMF or both (see note).

**NGLs:** Reference point between an AMF and LMF and between the VGMLC and LMF.

NOTE: It is FFS whether the NGLg interface includes an AMF or LMF or both.

# B.5 LMF Functions

The LMF includes the following functionality (see note):

- 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.

NOTE: Additional functions of the LMF are FFS.

Annex C (informative):  
Multimedia Priority Services temporary placeholder

Editor's note: This annex is being used as a placeholder to develop the technical content for Multimedia Priority Services for 5G System. It is planned to be moved as and where appropriate to TS 23.501, TS 23.502 [3], and TS 23.203 [4]. The Annex will not be maintained and will be voided when normative content has been prepared.

# C.1 References

Editor's note: This material highlights new documents referenced in this annex, as extensions to References in TS 23.501.

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*.

…

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

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

…

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

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

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

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

# C.2 General MPS Functionality

Editor's note: This material is targeted against TS 23.501 , sub-clause 5.16.5, "Multimedia Priority Services."

Multimedia Priority Service (MPS) allows certain subscribers (i.e. Service Users as per TS 22.153 [w]) 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 obtains priority access to the Radio Access Network by using the Access Class Barring mechanism according to TS 36.331 [x] and TS 22.011 [y]. This mechanism provides preferential access to UEs based on its assigned Access Class. If a Service User belongs to one of the special access-classes as defined in TS 22.011 [y], the UE has preferential access to the network compared to ordinary users in periods of congestion.

Editor's note: Whether NR in Rel.15 supports Access Class Barring mechanism according to TS 36.331 , or based on extensions and/or other specifications, depends on the decision of TSG RAN.

Editor's note: For this release of the specification, particular 5G-RAN support for MPS (e.g. E-UTRAN access only, or E-UTRAN + NR) depends on the decision of TSG RAN.

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 23.502 [3], TS 23.203 [4] and TS 23.228 [z].

Editor's note: 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 sub-clause 4.3.18.3 of TS 23.401 .

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 PDU session for a DNN. When not On Demand, MPS service does not require invocation, and provides priority treatment for all QoS Flows within the PDU session that is configured to have priority for a given Service User after attachment to the 5G network.

NOTE 2: According to regional/national regulatory requirements and operator policy, On-Demand MPS Service Users can be assigned the highest priority.

Editor's note: Further details of 5G priority processing (e.g. based on Establishment Cause in RRC connection request, as specified for MPS in sub-clause 4.3.18.1 of TS 23.401 ) are excluded from TS 23.501 , based on the anticipated inclusion of such details in corresponding procedure descriptions within TS 23.502 [3].

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).

Priority treatment for MPS includes priority message handling, including priority treatment during authentication, security, and location 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 3: Use of B-type QoS Flows for MPS 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.

Priority treatment is applicable to IMS based multimedia services and priority PDU connectivity service.

Annex D (informative):  
IMS specific placeholder for TS 23.228 [15]

Editor's note: This is placeholder for changes to IMS Service for 5G System. This annex will be moved to TS 23.228 [15] and will be deleted from TS 23.501 before TS 23.501 is sent to SA for approval. It is FFS if 5GS contents can be merged into existing Annex E for EPS/GPRS.

# D. IP-Connectivity Access Network specific concepts when using 5GS to access IMS

## D.0 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over 5GS.

HSS is used to store IMS related subscription and context as shown in the Figure 4.0 "Reference Architecture". For 5GS, HSS functionality for IMS shall continue to be as standalone regardless it is co-located or implemented as part of the UDM. A single IMS subscription profile is used regardless of UE accessing IMS via different IP-CANs.





Figure X.0-1: UDM and HSS collocated or HSS as part of UDM

NOTE: The HSS shown in Figure X.0-1 is only considering the functionality required for IMS.

Editor's note: It is FFS how to describe / retain legacy interface toward IP-CAN (i.e. Rx) and other IMS elements (e.g, Mw, Gm, etc.). So there is one set of interfaces from P-CSCF perspective when UE moves between different IP-CANs.

Editor's note: Details on the N5 reference point are further defined in the PCC Annex A – it is FFS to ensure that the N5 supports all the IMS capabilities defined in TS 23.228 [15].

## D.1 Mobility related concepts

To support IMS Multimedia Telephony Service as specified in TS 22.173 [16], SSC mode 1 is used for the corresponding APN/DDN.

If the UE changes its IP address due to changes triggered by the 5GS procedures, then the UE shall re- register in the IMS.

Editor's note: To capture SSC mode issue and other possible 5GS specific issue.

## D.2 QoS related concepts

Editor's note: For details on 5G QoS mode aspect with IMS.

Annex <Z> (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#118BIS | - | - | - | - | 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 |